

2. Der Einsatz von RFID-Systemen als ein Auto-ID-Verfahren

2.1 Bedeutung des Einsatzes von RFID-Systemen als Auto-ID-Verfahren in der Wirtschaft

In diesem Kapitel wird in einem Überblick aufgezeigt, welche konkreten RFID-Anwendungen angedacht sind oder eingesetzt werden. Anhand von Anwendungsbeispielen ausgewählter Einsatzfelder soll der Einsatz von RFID-Systemen illustriert werden. Zuvor aber gilt es der Frage nachzugehen, welches Ziel mit dem Einsatz von RFID-Systemen als ein Auto-ID-Verfahren in der Wirtschaft verfolgt und welche Idee mit dieser Technik verbunden wird.

2.1.1 Kennzeichnung und Identifikation

2.1.1.1 Aufgabe und Ziel von Auto-ID-Verfahren

Im organisierten Leben des Menschen bestand stets, sei es für Dokumente, Güter oder für Wareneinheiten, im Archiv, Registratur, Lagerhaltung oder Frachtwesen, das Bedürfnis, Gegenstände zu identifizieren, um sie zu ordnen oder wieder finden zu können. „Identifikation“ ist das Feststellen der Identität des Untersuchungsgegenstandes.⁶⁹ Dies kann anhand von Merkmalen erfolgen, die den betreffenden Gegenstand auszeichnen oder ihm angeheftet sind. Wenn zu identifizierende Gegenständen kein Unterscheidungsmerkmal zu Eigen ist oder sie im gewählten Identifikationsvorgang kein wahrnehmbares oder erfassbares Merkmal besitzen, können Gegenstände zur Identifizierung vorbereitet werden, indem man sie mit charakteristischen Merkmalen kennzeichnet. Kennzeichnung ist also das Unterscheidbarmachen von Objekten, wo hingegen Identifikation das Wiedererkennen von solchen Objekten bedeutet.

2.1.1.2 Historische Kennzeichnungs- und Identifikationssysteme

Bereits von der Antike bis ins Mittelalter wurden Zeichen oder Symbole zum Markieren von Waren, Gegenstände und Personen verwendet. Für Handelsware aller Art war die Verwendung von Kennzeichen seit der Antike verbreitet.

Griechische Händler kennzeichneten ihre Waren, die in Amphoren verschickt wurden, durch Einstemplung, Aufmalung oder Anhängung eines Etikettes.⁷⁰ Die Römer übernahmen von den Griechen das Urheberrechtzeichen, ergänzten ihre Handelsware aber noch durch Fabrik- und Herstellungsmarke.⁷¹ Mit dieser Kennzeichnung waren Erwartungen an die Herkunft und Qualität verbunden.

⁶⁹ Fischer 2002, 222.

⁷⁰ Der kleine Pauly 1979, 318.

⁷¹ Busseman/Pietzcker/Kleine 1962, 5 f.

Für den mittelalterlichen Warenverkehr war der wichtigste Transportbehälter das Holzfass. Die meisten auf den Fassdeckeln festzustellenden Marken oder Zeichen sind Eigentumsmarken, die den Inhalt betrafen. Die Kaufleute mussten ihre Handelsgüter kennzeichnen, um den Nachweis zu erbringen, dass es sich um ihr Eigentum handelte. Einerseits musste beim Transport zusammen mit Gütern anderer Kaufleute das unterschiedliche Eigentum erkennbar sein. Andererseits musste der Kaufmann bei Zoll- und Einfuhrformalitäten seine Ware vorweisen können. Weiterhin war auch bei Verkauf an Zwischenhändler oder auch an Endabnehmer an die Marke des Kaufmanns eine Art Garantie für die richtige Menge und die Güte des Inhalts der Behälter gebunden. Und letztlich war bei Verlust der Handelswaren durch Schiffbruch oder Raub mit der Markierung die Möglichkeit gegeben, das verlorene Handelsgut wieder zurückzubekommen.⁷²

Haus- und Hofmarken gab es in Deutschland seit dem 16. Jahrhundert. Mit dieser Marke wurde das Eigentum des Markeninhabers gekennzeichnet, sei es als Grenzzeichen oder als ein dem Tier aufgedrucktes Zeichen. Sie diente zur Unterstützung des Besitzererbs.⁷³

Das Militärwesen kannte schon früh Feldzeichen, Fahnen oder Standarten zur Kennzeichnung. Im Gegensatz zu den Griechen, bei denen sich nur selten Feldzeichen nachweisen lassen, waren im römischen Heer Feldzeichen von Anfang an vorhanden. Das Feldzeichen einer römischen Legion war die silberne oder versilberte „aquila“, der Adler mit ausgebreiteten, zum Aufzug erhobenen Flügeln, der auf einer silberbeschlagenen Stange befestigt war. Ihn trug in der ersten Kohorte der „aquilifer“.⁷⁴ Seit dem Mittelalter dienten Wappen im Schild und Helmzier im Ritterheer der Kennzeichnung von Einzelkriegern, welche erst von farbigen Schärpen und Leibbinden (16./17. Jhdt.), dann von Kokarden (18.Jhdt.) und Rangabzeichen (19.Jhdt.) abgelöst wurden. Seit dem ersten Weltkrieg tragen die Soldaten metallene Erkennungsmarken um den Hals mit eingepprägter Personal- und Truppenkennziffer zur Identifizierung.

Um Nachahmungen und Verwechselungen zu verhindern, bot das römische Namensrecht, die *Lex Cornelia de fabris*, strafrechtlichen Schutz des Namens. Im Mittelalter legte eine Kleiderordnung fest, was der Bürger zu tragen hatte. Die Kleidung gab Auskunft über Stand, Berufsgruppe und Konfession des Einzelnen. Bei Nichtbeachtung dieser Ordnung drohten Strafen. Sklaven wurden mit Brandzeichen oder Tätowierungen ihres Besitzers markiert.⁷⁵ Die Steinmetze im Mittelalter kennzeichneten die bearbeiteten Steine mit monogrammartigen oder geometrischen Steinmetzzeichen. Sie waren nicht nur Erkennungszeichen, sondern dienten auch zur Lohnabrechnung.

⁷² Falk 2002, 426.

⁷³ Bussemann/Pietzcker/Kleine 1962, 5 f.

⁷⁴ S. <http://www.jfrs.de/theologie/tattoosTText.htm>.

⁷⁵ S. <http://www.jfrs.de/theologie/tattoosTText.htm>.

2.1.1.3 Moderne Kennzeichnungs- und Identifikationssysteme

In der sich entwickelnden Industriegesellschaft, die einmal durch die Produktion von Massengütern gleicher Art und Güte sowie zum anderen durch zunehmende Arbeitsteiligkeit und Automation der Produktions- und Logistikprozesse gekennzeichnet ist, wuchs die Notwendigkeit, Gegenstände eindeutig zu kennzeichnen und identifizieren zu können. Wichtig war und ist, Prozesse möglichst maschinell abzuwickeln. Durch die zunehmende Automatisierung gilt es Daten zu Personen, Tieren, Gütern oder zu Waren klar definiert und strukturiert so zur Verfügung zu stellen, dass diese maschinell erfasst und weiterverarbeitet werden können. Hierzu werden Systeme zur automatischen Identifikation benötigt.⁷⁶ Dabei beschreibt ein Identifikationssystem ein technisches System, das die automatisierte Erkennung von Objekten ermöglicht, die mit Trägern von Informationen gekennzeichnet sind.

- **Strichcode-Systeme:**
Als einer der bekanntesten und mit Abstand verbreitesten Vertreter moderner Kennzeichnungssysteme kann der Strichcode (Barcode), früher Balkencode, gelten.⁷⁷ Ein Strichcode ist ein maschinell lesbares Muster in einem Sichtformat von einer Hell- und Dunkelabfolge, in der Informationen kodiert sind.⁷⁸
- **Zeichenerkennungssysteme:**
Abhängig von den Einsatzanforderungen finden in der Praxis neben dem Strichcode weitere automatische Kennzeichnungssysteme Verwendung. Hierzu gehören unter anderem Zeichen- oder Schrifterkennungssysteme – Klerschriftleser, die auch als System der Optical Character Recognition (OCR-Systeme) bezeichnet werden. Sie ist die einfachste Form Schwarzschrift mittels elektro-optischer Abtaster in maschinenlesbare Zeichen umzusetzen. Im ersten Schritt werden die Zeichen auf dem Kennzeichnungsträger als digitales Bild erfasst und mittels Mustererkennung, die im erfassten Muster abgebildeten Zeichen für die Weiterverarbeitung erschlossen.⁷⁹
- **Speicherkarten-Systeme:**
Eine andere Technik sind Speicherkartensysteme, bei denen das Auslesen der Daten von einem Magnetstreifen oder einem Mikroprozessorchip mit Datenspeicher, allerdings nur kontaktgebunden, erfolgt. Anders als bei den Strichcodes besteht bei den auf Magnetstreifen oder Mikroprozessor basierten Kennzeichnungssystemen bereits die Möglichkeit, die Daten auf Kennzeichnungsträgern zu verändern.⁸⁰

⁷⁶ Finkenzeller 2002, 1 f.; Hansen, in: ident Jahrbuch 2012, 136 f.; Mattern/Flörkemeier, Informatik-Spektrum 2010, 108 ff.

⁷⁷ Fischer 2002, 456.

⁷⁸ Wiesner 1990, 325.

⁷⁹ Wiesner 1990, 20.

⁸⁰ Finkenzeller 2002, 5.

- **RFID-Systeme:**
In den letzten Jahren hat sich die Technik der Funketiketten oder Radio-Frequency-Identifikation (RFID – Identifikation durch Radiowellen) so entwickelt, dass RFID-Systeme als neueres, automatisches Identifikationssystem weiter in vielen Einsatzfeldern Einzug halten werden. Bei RFID-Systemen werden RFID-Marken als Kennzeichnungsträger verwendet, von denen Daten mittels Funkkommunikation ausgelesen, aber auch auf ihnen gespeichert werden können.⁸¹
- **Biometrische Identifikationsverfahren:**
Biometrie ist die zahlenmäßige Erfassung und Bearbeitung von Mess- und Zahlenwerten in allen Bereichen der Biologie, Medizin und Landwirtschaft. Das Biometrische Verfahren bedient sich der unverwechselbaren Kennzeichnungsmerkmale, die den Personen oder Tieren naturgegeben anhaften. In der Praxis sind dies Sprachidentifizierung, Handabdruck- und Fingerabdruckverfahren (Daktyloskopie) oder auch die Augen-Netzhaut- (bzw. auch Iris-) Identifikation.⁸²

2.1.2 Einführung von Auto-ID-Verfahren als ökonomisch gebotener Entwicklungsschritt

Das Interesse Auto-ID-Techniken in verschiedenen Bereichen der Wirtschaft einzuführen, entsteht durch Effizienzdruck. Dieser wird vornehmlich durch den herrschenden Wettbewerb hervorgerufen, der sich in vielen Branchen durch die Globalisierung der Märkte verschärft hat. Dadurch ergibt sich für die einzelnen Unternehmen das Erfordernis ihre Produktion oder die Erbringung von Dienstleistungen zu optimieren.⁸³

2.1.2.1 Auto-Identifikation als Ansatzpunkt in der Wirtschaft zur Effizienzsteigerung

Mikroökonomisch stellt sich für Unternehmen daher die Frage, wo und wodurch können sie ihre Effizienz steigern. Dabei haben die Unternehmen grundsätzlich die Möglichkeit, mit den Maßnahmen, die sie zur Optimierung ergreifen, entweder ihren Aufwand zu senken oder die Qualität zu verbessern.

Als Ansatzpunkte für Maßnahmen kommen verschiedene Faktoren in Betracht, die Effizienz innerhalb des Unternehmens zu steigern. Zu den wichtigen Produktionsfaktoren gehören die natürlichen Ressourcen, Kapital, vor allem in Form von Roh- und Werkstoffen, Waren, Maschinen oder die Betriebsausstattung und die menschliche Arbeitskraft einschließlich technischen Wissens. Hier lassen sich etwa durch Optimierung von Arbeitsabläufen bei der Produktion, durch Optimierung des Verschnitts, der Lagerhaltung oder des Einkaufs, beim

⁸¹ Finkenzeller 2002, 6.

⁸² Finkenzeller 2012, 570 f.; ausführlich dazu Eckert 2013, 496 ff.

⁸³ Töpfer 2007, 74; Straub 2012, 211.

Materialeinsatz oder durch Qualifikation und Motivation des Personals Verbesserungen erzielen.⁸⁴

Aber auch hinsichtlich der im Unternehmen benötigten Informationen können Produktivitätsreserven gehoben werden, wenn es gelingt, Daten besser zu beschaffen, aufzubereiten und in den jeweiligen Prozessschritten besser zu verwenden. Eine bessere Gewinnung und Nutzung von Informationen bedeutet, dass relevante Daten schneller, kostengünstiger, valider, feingranularer oder mit höherem Aussagegehalt weiterverarbeitbar zur Verfügung stehen.

Außerhalb des Unternehmens verspricht die Optimierung der Prozesse zwischen Lieferanten und Kunden Wettbewerbsvorteile. Diese müssen nicht nur in direkten Kosteneinsparungen bestehen, sondern können, wie zuvor dargestellt, immer auch die Qualität der zu erbringenden Leistung betreffen. Um die angesprochenen Faktoren zu optimieren und damit Effizienzsteigerungen zu erzielen, bieten sich für Unternehmen verschiedene Maßnahmen an. Die richtigen Ansatzpunkte und deren konkrete Ausgestaltung sind stark von der Branche, von der Einbindung der jeweiligen Unternehmung in die Wertschöpfungskette sowie von der spezifischen Unternehmenssituation abhängig.

Allgemein kommen Maßnahmen für einen effizienten Einkauf, zur Prozessoptimierung oder zur Produktverbesserung in Betracht. Dadurch lassen sich Einsparungen oder Verbesserungen hinsichtlich Zeit, Preis, Kosten, Qualität und Personaleinsatz erreichen. Hierfür ist es allerdings meist unabdingbar, schon um einen höheren Automatisierungsgrad realisieren zu können, relevante Informationen zeitnah und in benötigter Qualität zu erhalten und weiterverarbeiten zu können. Auch wird erst hierdurch die Entwicklung neuer Produkte oder Dienstleistungen möglich.

Wenn ein Unternehmen es schafft, das Silo des Kunden hinsichtlich Befüllung, Mischung der Stoffe sowie den Weiterverarbeitungsprozess im Silo direkt aus der eigenen Produktion vollständig zu steuern, dann helfen die ergriffenen Maßnahmen, nicht nur die Qualität zu verbessern und seine Kosten zu senken. Vielmehr entsteht für den Kunden darüber hinaus ein Mehrwert, der einen Wettbewerbsvorteil bedeutet.

Ebenso bedeutet in der Logistik oder im Groß- und Einzelhandel es einen Effizienzgewinn, wenn im Warenwirtschaftssystem Daten über die Handelsgüter schneller und mit geringerem Personaleinsatz zur Verfügung stehen. Dies ist der Fall, wenn Transportbehälter (z.B. Schiffscontainer, Paletten oder Werkstückkisten) oder gar einzelne Waren eindeutig gekennzeichnet sind und ohne direkten Sichtkontakt, automatisiert am Ladetor oder in Regalen der Lager registriert werden können, um Standort, Status im Prozess, Zielverwendung oder Füllstand von Lagern zu messen.

⁸⁴ Töpfer 2007, 78; Straub 2012, 210; Fehll/Oberender 2004, 174.

2.1.2.2 Einführung von Auto-ID-Verfahren als Maßnahme zur Effizienzsteigerung

Ökonomisch werden Maßnahmen nur in den Bereichen sinnvoll sein, die einer Steuerung zugänglich sind. Wesentlich für eine Steuerung von Prozessen ist, dass ein Unternehmen regelnd eingreifen kann und veränderte Prozessparameter in dem gewünschten Zeitraum zu ökonomisch optimaleren Ergebnissen führen. Für ein Unternehmen muss also in einem betrieblich relevanten Prozess (überhaupt) die Möglichkeit bestehen, durch technische Lösungen oder mittels Personaleinsatz auf Bedingungen des betreffenden Prozesses gezielt einzuwirken.⁸⁵

Voraussetzung für ein regelndes Eingreifen oder aktives Bewirtschaften ist aber, die Bedingungen und Zustände des jeweiligen Prozesses erfassen zu können und dadurch eine Rückkopplung zum Prozess herzustellen. „Unternehmen können nur managen, was sie auch messen können.“⁸⁶ Beim Management oder der Bewirtschaftung von Prozessen führen Defizite in ihrer Analyse zu Fehlern, die sich betriebswirtschaftlich in erhöhten Aufwendungen oder in verminderten Erträgen auswirken können. Im Fall des Einzelhändlers bedeutet dies, dass er seine Umsatzverluste wegen Angebotsengpässen trotz Vorrätigkeit im Lager (Out-of-Stock-Situationen) nur reduzieren kann, wenn sich der Füllstand seiner Regale hinreichend genau messen lässt, um die Verfügbarkeit seiner Handelsware in der Filiale entsprechend erhöhen zu können.⁸⁷

Ein Schlüssel, um ertragsmindernde oder kostenerzeugende Fehler zu vermeiden, stellt der Einsatz von neuen Technologien und Techniksystemen dar. Diese müssen eine Integration der realen betrieblichen Umgebung in die im Unternehmen eingesetzten Datenbanken und Anwendungen leisten. Dabei sind Daten der Umwelt mit einzubeziehen, um den Prozess im Unternehmen besser zu regeln oder überhaupt in ein Managementsystem⁸⁸ überführen zu können. Zudem haben diese Systeme den Medienbruch zwischen realer und virtueller Welt möglichst vollständig zu schließen, um Aufwände für (manuelle) Eingaben und Aufbereitung zu reduzieren. Auch müssen Daten ohne (prozessrelevante) Zeitverzögerung vom Ort ihrer Entstehung zu dem Ort ihrer Verwendung gelangen, um dem jeweiligen Managementsystem eine optimalere Prozesssteuerung zu ermöglichen.

⁸⁵ Töpfer 2007, 952.

⁸⁶ Fleisch/Michahelles, in: Matern 2007, 145.

⁸⁷ Fleisch/Michahelles, in: Matern 2007, 145.

⁸⁸ Mit Management können zu regelnde Prozesse abgebildet werden, in denen anhand von Ist-Daten und Soll-Daten Steuervorgänge ausgelöst werden, die über Aktuatoren (Mitarbeiter oder Robotersysteme) in der realen Welt gezielt eingreifen und Prozessparameter verändern. Unternehmensprozesse können als Regelkreismodelle abgebildet und entsprechend formalisiert beschrieben werden – näher hierzu Glattfelder/Schaußelberger 1997, 8 ff.; Fleisch/Christ/Dierkes, in: Matern 2005, 12 f.

Insbesondere, die im Zusammenhang mit „Ubiquitous Computing“ entwickelten Techniken und Technikkonzepte können helfen, Managementdefizite abzubauen, die entstehen, weil relevante Informationen überhaupt nicht oder nicht schnell, nicht feingranular oder nicht aussagekräftig genug zur Verfügung stehen. Techniksysteme im Kontext allgegenwärtiger Datenverarbeitung zeichnen sich dadurch aus, dass sich ihre Komponenten aufgrund der kleinen Baugrößen in vielfältige Gegenstände integrieren und solche Systeme sich an fast allen Orten realisieren lassen. Unterstützt durch Vernetzbarkeit und Sensorik vermitteln sie Informationen über Zustände der realen Welt, die medienbruchfrei und damit ohne Zeitverzug in den betrieblichen Informationssystemen zur Steuerung von Prozessen, etwa im Warenwirtschaftssystem des Unternehmens, genutzt werden können.⁸⁹

Eine herausragende Bedeutung kommt hier den Auto-ID-Verfahren und insbesondere der RFID-Technik zu. Die RFID-Technik ist heute schon verfügbar und bietet eine flexible, recht einfach zu handhabende und kostengünstige Möglichkeit, elektronische Identifikationssysteme zu realisieren.

2.1.2.3 Voraussetzungen für die Einführung von RFID-Systemen als Auto-ID-Verfahren

In der betrieblichen Informationsverarbeitung stellt die Einführung von Techniksystemen aus dem Kontext der allgegenwärtigen Datenverarbeitung, insbesondere der RFID-Technik, einen zwingenden nächsten Entwicklungsschritt dar.⁹⁰

Allerdings ist zu bedenken, dass Registrierung und Abbildung betrieblicher Realwelt-Vorgänge stets Aufwände generieren. Diese Aufwände für eine verbesserte Messgenauigkeit müssen unter einer betriebswirtschaftlichen Betrachtung im Verhältnis zu dem Nutzen stehen, der durch die Verwendung der Daten entsteht, die mittels der einzuführenden Registriervorgänge erhoben werden.

Beim Einsatz von RFID-Systemen in betrieblichen Umgebungen ergibt sich der zu schöpfende Nutzen aus den technischen Merkmalen der RFID-Technik.⁹¹ Bedingt dadurch lassen sich betriebliche Anwendungen effizienter managen und betriebliche Prozesse anders als bisher aufsetzen. Daher beschränkt sich der Nutzen von RFID-Systemen nicht nur auf eine Reduktion der Kosten gegenüber herkömmlichen Registrierverfahren (z.B. manuelles Zählen und Sortieren). Vielmehr kann der weitere Nutzen (abhängig von der konkreten Ausgestaltung der RFID-Anwendung) in der höheren Qualität der mit RFID-Systemen erzeugten Daten bestehen.

Mit den vier Dimensionen Zeitgranularität, Objektgranularität, Messstrecke und Semantik lässt sich der Nutzen, der über RFID-Systeme erzeugten Daten,

⁸⁹ S. Einführung

⁹⁰ *Fleisch/Christ/Dierkes*, in: *Mattern* 2005, 5; *Töpfer* 2007, 642.

⁹¹ Näher hierzu Abschnitt 2.4.2.

genauer beschreiben.⁹² Für die Auflösung in zeitlicher Hinsicht kommt es auf die Erhebungshäufigkeit von Daten und ihre Verfügbarkeitszeit an. Als Kriterium für den Nutzen ist nicht nur wichtig, wie oft gemessen wird, sondern auch mit welchem Zeitverzug die erhobenen Daten für eine Weiterverwendung zur Verfügung stehen, also ob etwa noch ein händischer Verarbeitungsschritt erfolgen muss.

Hinsichtlich des Objekts ist relevant, welche Typen von Objekten und wie viele Instanzen einer Objektklasse in das Identifikationsverfahren einbezogen werden können. Dabei steigt die Attraktivität eines Systems, wenn die Gegenstände, seien es Paletten oder seien es Bauteile, die im zu steuernden Prozess vorhanden sind, erfasst werden können. Ebenso spielt die Auflösung eine Rolle, mit der bestimmte Gegenstände (etwa Kotflügel einer Fertigungslinie) registriert werden können – als Stichproben- oder Vollerfassung.

Weiter bestimmt die Messstrecke, die mit einem Identifikationssystem eingerichtet werden kann, den Nutzen. Dieser erhöht sich, wenn die Grenzen der Anwendungsumgebung erweitert und in einer Anwendungsumgebung mehr Messpunkte bedient werden können. Schließlich ist bei den zu verarbeitenden Daten ihre Semantik ein wichtiges Kriterium. Der Informations- oder Bedeutungsgehalt, den das Identifikationssystem liefert, hat Einfluss auf die Verwertbarkeit der Daten.

Aus den Kriterien für die Datenqualität ergibt sich, dass der Informationswert, der sich aus erhobenen und verwendeten Daten ziehen lässt, nicht gleich bleibt. Trotz sich erhöhender Granularität der Daten nimmt in vielen Anwendungsfällen ihr Nutzen ab.⁹³ Im Fall des Einzelhändlers bedeutet dies, dass häufigere Bestandsanalysen, vielleicht stündlich anstatt nur täglich, zur Optimierung der Füllstände in den Regalen hilfreich sind. Ab einer bestimmten Auflösung der Erhebungszeiten, etwa einer sekundlichen gegenüber einer stündlichen Messung, haben die zusätzlich gewonnenen Daten geringen Wert, wenn dadurch in dem Prozess der Regalauffüllung kein verbessertes Management, zum Beispiel mangels Personal zum Auffüllen, erreicht werden kann.⁹⁴

Im Hinblick auf die dargestellten Gesichtspunkte sind RFID-Systeme den bisher eingesetzten Verfahren, wie das des manuellen Sortierens oder das des Strichcodes, überlegen.⁹⁵ Nachdem die Registriervorgänge in RFID-Systemen automatisiert ablaufen, lassen sich RFID-Marken – ihr Vorhandensein und ihre Daten – zeitlich wesentlich häufiger, nahezu permanent, abfragen. Als elektronisches System stellen RFID-Systeme der jeweiligen Anwendung die Daten der registrierten RFID-Marke informationstechnisch verarbeitbar bereit, sodass

⁹² *Fleisch/Christ/Dierkes*, in: *Mattern* 2005, 16; s. auch *Fleisch/Michahelles*, in: *Mattern* 2007, 149.

⁹³ Näher dazu *Fleisch/Michahelles*, in: *Mattern* 2007, 147.

⁹⁴ *Fleisch/Christ/Dierkes*, in: *Mattern* 2005, 13 f.; s. auch *Fleisch/Michahelles*, in: *Mattern* 2007, 152.

⁹⁵ Zu den folgenden Ausführungen näher Abschnitt 2.4.

aufwendiges manuelles Einpflegen der Daten entfällt und diese medienbruchfrei in angeschlossenen IuK-Systemen des Unternehmens oder anderen Stellen weiterverarbeitet werden können. Dadurch stehen die erhobenen Daten ohne größeren Zeitverzug zu Managementzwecken zur Verfügung. Echtzeit-Anwendungen lassen sich realisieren.

Ferner bieten RFID-Systeme eine wesentlich höhere Qualität der erzeugten Daten. Sie registrieren nicht nur das Vorhandensein einer RFID-Marke, sondern können diese über die Objektklasse hinausgehend, eindeutig identifizieren. Zudem lassen sich die Aussagekraft der erhobenen Daten um Zeit- und Ortsangaben des RFID-Lesegeräts sowie gegebenenfalls ergänzt um weitere Sensordaten anreichern.

Neben dem objektbezogenen Kennzeichnungsdatum, bringen RFID-Marken weitere auf ihr abgelegte Nutzdaten mit. Dadurch stehen in der jeweiligen Anwendung über das Identifikationsmerkmal hinaus zusätzliche anwendungsrelevante Informationen (z.B. Eigenschaften oder Transportziel der markierten Handelsware) zur Verfügung, ohne auf (externe) Datenbestände in einem Hintergrundinformationssystem zurückgreifen zu müssen. Damit lassen sich RFID-Anwendungen realisieren, die über Unternehmensgrenzen hinweg, ohne zentrale Datenhaltung funktionieren. Sind beschreibbare Speicherbausteine verbaut, können Anwendungen mit dynamischen Daten versorgt werden.

Die RFID-Technik zeichnet sich weiter dadurch aus, dass RFID-Marken extrem klein und damit an Gegenstände nahezu aller Art angeheftet oder sogar in diese eingebaut werden können, zumal sie in ihrer passiven Ausführung keine eigene Stromversorgung benötigen. Aber auch RFID-Lesegeräte lassen sich flexibel an vielen Orten, integriert in Umgebungselemente, aufstellen oder mobil einsetzen. Dadurch sind RFID-Anwendungen mit sehr vielen Objekttypen umsetzbar. Hinzukommt, dass die Identifikationstiefe bis zur Objektklasse möglich ist und bei der sich abzeichnenden Preisentwicklung jedes einzelne Objekt, auch niedrigpreisige, in die RFID-Markierung einbezogen werden kann.

Die flexiblen und breiten Einsatzmöglichkeiten, begünstigt durch die sichtkontaktlose Auslesbarkeit von RFID-Marken, erlauben, mehr Messpunkte als bisher einzurichten (z.B. nicht nur an Kassen, sondern an Ladetoren, Türen von Lagerräumen bis hin zu Lagerregalen). Zudem kann die Messstrecke über unternehmensinterne Prozesse hinaus ausgeweitet (z.B. über die interne Lagerhaltung auf die Logistikkette) und externe Partner können einbezogen werden (z.B. Lieferant, Groß- und Einzelhändler). Letztlich lässt sich der Informationsfluss entlang der gesamten Wertschöpfungskette organisieren. Im Rahmen ihrer technischen Möglichkeiten (z.B. begrenzt durch funktechnische Dämpfung oder Störung, Lesefehler- oder Ausfallwahrscheinlichkeit) liefern RFID-Systeme schließlich verlässlichere Daten als herkömmliche eingesetzte Identifikationssysteme.

Für den Einzelhandel bietet die Einführung eines RFID-Systems in der Handelsfiliale die Chance, nicht nur an der Kasse, sondern auch an den Toren zum Lager sowie in den Auslageregalen Registriermöglichkeiten für die dann RFID-markierte Handelsware einzubauen. Dadurch lässt sich häufiger, als mit manu-

eller Inventur, die tatsächliche Befüllung der Regale und der tatsächliche Lagerbestand ermitteln, ohne, wie bei seltener Bestandskontrolle, auf statistische Abschätzungen angewiesen zu sein, bei der Störgrößen, etwa unerwartete Absatzschwankungen, schwer zu berücksichtigen sind. Werden RFID-Marken mit Sensortechnik für Temperatur kombiniert, kann überdies bei einzelnen Produkten überwacht werden, ob ihre Lagerbedingungen über die gesamte Kühlkette eingehalten wurden.⁹⁶ Der Einsatz von RFID-Systemen verspricht zwar Effizienzgewinne in betrieblichen Prozessen sowie verbesserte und sogar neue Realisierungsmöglichkeiten von Anwendungen. Gleichwohl sind in der betriebswirtschaftlichen Abwägung auch die Aufwendungen in Ansatz zu bringen, die für die Einrichtung und den Betrieb von RFID-Systemen zusätzlich gegenüber bisher eingesetzten Verfahren zu leisten sind.

Im Einzelnen unterscheiden sich Einführungsbedingungen und Aufwände für RFID-Systeme nach jeweiliger Unternehmenssituation, Branche und Anwendungsfeld. Dabei spielt auch eine Rolle, ob das RFID-System unternehmensintern oder in geschlossenen Nutzergruppen eingesetzt wird (geschlossene RFID-Systeme) oder ob es für beliebige Nutzer geöffnet ist (offene RFID-Systeme).⁹⁷ Jedoch kann verallgemeinernd gesagt werden, dass RFID-Systemen in der Regel zunächst höhere Aufwendungen in der Anschaffung bedeuten, zumal herkömmliche Identifikationsverfahren, wie Strichcode, letztlich auch manuelle Verfahren, oft schon eingeführt sind.⁹⁸

Der Mehrwert von RFID-Systemen entsteht vor allem, wenn auf eine Infrastruktur zurückgegriffen werden kann. Dazu gehört, RFID-Lesegeräte mit einem Hintergrundinformationssystem zu vernetzen, dessen Schnittstellen, Datenbankanwendungen und seine Einbindung in die übrige betriebliche IuK-Infrastruktur entsprechend anzupassen oder zu entwickeln sind. Zudem müssen oft nicht nur ein RFID-Lesegerät, sondern eine Lesegeräteinfrastruktur, also eine Vielzahl von RFID-Lesegeräten installiert werden, um die benötigten Verfolgungs- und Überwachungsfunktionen zur Verfügung zu stellen.

Soll ein RFID-System effizient arbeiten, müssen eine genügend hohe Anzahl der zu identifizierenden Gegenstände mit RFID-Technik ausgestattet sein. Bei der Einführung bedarf es hier einer gewissen sogenannten „kritischen Masse“, wenn nicht die Anwendung ohnehin eine Vollerfassung verlangt. Unter betriebswirtschaftlichen Gesichtspunkten muss sich, wie oben gesagt, die Einführung eines RFID-Systems rechtfertigen. Das ist dann der Fall, wenn sich durch das RFID-System mit seinen vielfältigen Vorteilen die Effizienz betrieblicher Prozesse steigern lässt. Diese Effektivitätsgewinne müssen mindestens in dem Maß steigen, dass sich monetär gemessen die Aufwendungen für Beschaffung und Betrieb des RFID-Systems amortisieren.

⁹⁶ *Fleisch/Michahelles*, in: *Mattern* 2007, 154.

⁹⁷ Näher dazu *Fleisch/Christl/Dierkes*, in: *Mattern* 2005, 28 f.; *Polenz* 2008, 51 f.

⁹⁸ *Friedewald/Raabe* 2010, 153.

Wenn für die Anpassung und das Management von betrieblichen Prozessen eine verbesserte Datenlage und damit eine erhöhte Granularität der Daten benötigt wird, rechnet sich ein RFID-System. Seine Einrichtung verursacht zwar in der Regel höhere Aufwendungen, jedoch fallen die zusätzlich aufzubringenden Aufwendungen für einzelne Identifikationsabfragen gegenüber herkömmlichen Verfahren geringer aus. Allerdings ist es von den ökonomischen Rahmenbedingungen der jeweiligen Anwendung abhängig, inwieweit die technischen Möglichkeiten eines RFID-Systems tatsächlich ausgeschöpft werden. Ein Mehr an Granularität rechtfertigt sich nur bis zu dem Punkt, in dem der Nutzen für genauere Daten (z.B. in zeitlich oder objektbezogener Hinsicht) die Kosten zu ihrer Erzeugung zumindest nicht unterschreitet (optimale Messgenauigkeit).

In diesem Zusammenhang ist jedoch zu berücksichtigen, dass ein Unternehmen, wenn es verbesserte Daten für das Managementsystem generiert, auch die Möglichkeit (insbesondere der Ressourcen) haben muss, betriebliche Prozesse anzupassen und prozesslenkende Maßnahmen in der Realwelt umzusetzen. Letztlich kommt es auch darauf an, ob bereits eingeführte Verfahren die betreffende Aufgabe in gleicher Weise erfüllen, wie ein RFID-System, das zwar technisch überlegen ist, aber mit entsprechendem Aufwand noch installiert werden müsste.⁹⁹

Im Fall des Einzelhandels führt der Einsatz maschineller Messung der Regalbestände durch RFID-Systeme zu einer höheren Messgenauigkeit. Der ökonomisch optimale Wert, der sich an den Grenzkosten und den Grenznutzen orientiert, verschiebt sich zugunsten einer höheren Messgenauigkeit. Bei manueller Bestandsprüfung begrenzen die hohen Kosten jeder Einzelprüfung die Erhebungszyklen. Hingegen erlauben die geringeren Kosten für jede zusätzliche Bestandsprüfung bei einer maschinellen RFID-Abfrage höhere Messgenauigkeit und zwar in dem Maß, als dass weitere Erhebungen keinen ökonomischen Nutzen bringen.¹⁰⁰

Bei der Einführung von RFID-Systemen lassen sich die Effizienzschwelle oder die angesprochene sogenannte kritische Masse innerhalb eines Unternehmens oder bei einem definierten Nutzerkreis einfacher herstellen. Da RFID-Systeme ihre Vorzüge als Grundlage zur Steuerung und Kontrolle von betrieblichen Abläufen gerade auch über Grenzen unternehmensinterner Prozesse ausspielen, spielt in diesem Zusammenhang eine Rolle, wie sich die Aufwand-Nutzen-Struktur für die beteiligten Akteure darstellt. Insbesondere bei RFID-Systemen, die mehrere Wertschöpfungsstufen erfassen, sind die Aufwände und der Nutzen bei den verschiedenen, beteiligten Wertschöpfungspartnern oft nicht gleichmäßig verteilt. Zur Verfolgung von Gütern in der Logistikkette fallen beispielsweise Aufwände für die Integration von RFID-Marken in die Produkte eher in der Herstellungsstufe an. Hingegen müssen Spediteure oder der Handel

⁹⁹ Fleisch/Michahelles, in: *Mattern* 2007, 146 f.

¹⁰⁰ Fleisch/Michahelles, in: *Mattern* 2007, 151.

eher in die Einrichtung einer funktionierenden RFID-Lesegeräte-Infrastruktur investieren.¹⁰¹

Als weitere Faktoren, die die Einführung hemmen oder befördern, sind vor allem die Preisentwicklung für die RFID-Komponenten und der Stand der Standardisierung der RFID-Technik wichtig. Sinkende Preise, insbesondere für RFID-Marken, begünstigen entsprechende Investitionsentscheidungen.¹⁰² Wie bei anderen Investitionen auch, ist für ein Unternehmen hier ebenfalls ein Kriterium, ob der Amortisationszeitraum ihrer Investitionen überschaubar oder die Investitionsbeträge für das Unternehmen bezahlbar sind. Dabei spielt auch eine Rolle, ob die Vorteile des geplanten RFID-Systems sich in monetären Größen messen lassen. In kundennahen Anwendungsfeldern ist schließlich das Akzeptanzproblem beim Nutzer zu lösen, das als hemmender Faktor nicht zu vernachlässigen ist.¹⁰³

Soll sich eine Infrastruktur entwickeln, die RFID-Anwendungen im Sinne der Vision der allgegenwärtigen Datenverarbeitung ermöglicht, dann bedarf es einheitlicher Standards für die verschiedenen technischen Anforderungen an ein RFID-System (z.B. Sendefrequenz, Kommunikationsprotokolle, Authentisierungsverfahren).

Mit der RFID-Technik entstehen neue Einsatzmöglichkeiten, die nicht mit dem Verlust an informationeller Selbstbestimmung einhergehen dürfen. Gegen diese Gefahr wandten sich viele Nichtregierungsorganisationen, Datenschutzbehörden und Verbände.¹⁰⁴

Viele der Anwendungen im Kontext der allgegenwärtigen Datenverarbeitung gehen von einer flächendeckend ausgebauten RFID-Infrastruktur aus. Angesichts der für ihren Auf- und Ausbau zu leistenden Aufwände wird sich diese Infrastruktur erst allmählich entwickeln und zunächst erst in begrenzten Anwendungsumgebungen zur Verfügung stehen, wo sich eine Einführung für einzelne RFID-Anwendungen bereits ökonomisch rechtfertigt.

2.1.3 Anwendungsbeispiele für den Einsatz von RFID-Systemen

Für die RFID-Technologie bestehen bereits seit rund 25 Jahren vielfältige Einsatzmöglichkeiten. Ausgangspunkt des Einsatzes ist stets die Verbindung einer RFID-Marke mit einem Objekt. Anhand der Kennzeichnungsnummer dieser Marke wird das Objekt identifizierbar und durch eine Infrastruktur von RFID-

¹⁰¹ Polenz 2008, 55.

¹⁰² Die Preisentwicklung von RFID-Komponenten hängt stark von der Verbreitung von RFID-Systemen ab. Wegen Skaleneffekten (Abhängigkeit der Produktionsmenge von der Menge der eingesetzten Produktionsfaktoren) verbilligen sich RFID-Chips bei hoher Stückzahl signifikant und ihre Verwendung als RFID-Marke in immer mehr und neuen Gegenständen wird interessant. Investitionen in weitere RFID-Infrastruktur werden für weitere Unternehmen wirtschaftlich.

¹⁰³ Friedewald/Raabe 2010, 154; Berthold/Günther/Spiekermann 2005, 6.

¹⁰⁴ S. Abschnitt 2.5.

Lesegeräten, ergänzt gegebenenfalls um Sensoren, auch lokalisierbar. Objekte können dabei sowohl Gegenstände, Pflanzen, Tiere oder auch Menschen sein.

Durch Lesegeräte werden die Marken erfasst. Diese Lesegeräte wiederum können untereinander und mit einem im Hintergrund arbeitenden Datenverarbeitungssystem vernetzt werden, wodurch die Weiterverarbeitung der Daten in den verschiedensten Anwendungen möglich ist.

Bereits 2006 betrugen die Herstellungskosten für einen Chip in der Größe eines Reiskornes mit 500 kByte Speicher lediglich 10 Cent.¹⁰⁵ Überall dort wo automatisiert überwacht, transportiert, gelagert oder abgerechnet wird, werden RFID-Systeme eingesetzt. Die im Folgenden vorgestellten Beispiele stellen eine Auswahl aus einem breiten Spektrum von Anwendungen unterschiedlicher Anwendungsfelder für RFID-Technik dar. Auch sind die vorgestellten Anwendungen nicht auf eine Funktion festgelegt, sondern erfüllen zumeist mehrere Funktionen und Aufgaben.

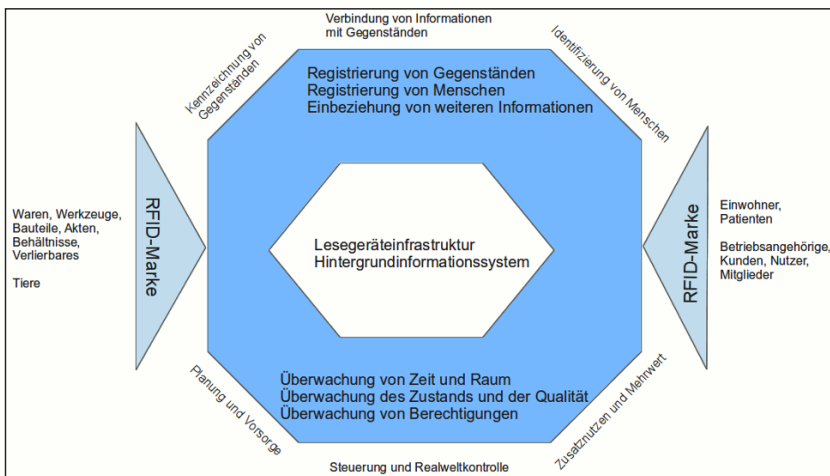


Abbildung 1: Funktionen und Anwendungsfelder von RFID-Systemen

Viele der in Unternehmen und zwischen Unternehmen eingesetzten RFID-Anwendungen dienen der Überwachung von Zeit und Raum sowie oft ergänzend der Überwachung des Zustandes oder der Qualität von oder in Gegenständen. Weiter interessieren Informationen zum Gegenstand, seien es seine aktuellen Umgebungsbedingungen, sein Status oder seien es Hintergrundinformationen zu seiner Geschichte. Aber auch die Überwachung von Berechtigungen ist ein wichtiges Anwendungsfeld. Viele gegenüber Kunden oder dem Bürger eingesetzte RFID-Anwendungen dienen, den Zutritt von Personen zu

¹⁰⁵ <http://www.heise.de/newsticker/meldung/75558>.

bestimmten Bereichen, zu kontrollieren oder die dazu Abrechnung von Leistungen zu ermöglichen.

2.1.3.1 Überwachung von Zeit und Raum

Der Einsatz von RFID-Technik bei der Verfolgung von Waren entlang der Wertschöpfungskette (Supply Chain Management)¹⁰⁶ wird vor allem vom Handel forciert. RFID beschleunigt in Echtzeit den Datenaustausch zwischen Zulieferern, Händlern und Endverbrauchern, damit können Herstellungs-, Liefer- und Personalkosten optimiert werden. Beispielsweise kann die Ware in der Bekleidungsindustrie wie auch im Lebensmitteleinzelhandel (Kartons und Paletten), versehen mit einer RFID-Marke, nicht nur effizient eingelagert werden, sondern auch vom Hersteller bis zum Verkaufsort (Point-of-Sale) verfolgt werden.¹⁰⁷ Die Daten des Warenausgangs eines Zulieferers werden automatisch an eine Datenbank weitergegeben, damit sie in Echtzeit der Lagerverwaltung oder der Warenwirtschaft zur Verfügung stehen.

Den Modernisierungs- und Rationalisierungsprozess voranzutreiben, verfolgen innerhalb der Handelsbranche z.B. die Metro Group Future Store Initiative wie auch Kaufhof Warenhaus GmbH in Zusammenarbeit mit dem Bekleidungshersteller Gerry Weber International AG. Dafür entwickeln und erproben die globalen Unternehmen gemeinsam innovative Handelstechnologien.¹⁰⁸

Der Future Store in Tönisvorst bietet seinen Kunden nicht nur ein umfangreiches Produktsortiment und flexible Öffnungszeiten, sondern die Möglichkeit des „Mobilen Einkaufs“. Mit seinem elektronischen Einkaufszettel, den der Kunde an den Einkaufswagen übermittelt, wird er zu den gewünschten Produkten geführt.¹⁰⁹ Direkt im Regal befindliche Lesegeräte erfassen automatisch den Warenbestand, die Entnahme, aber auch die Produkttemperatur oder die Überschreitung des Mindesthaltbarkeitsdatums von jedem einzelnen Produkt. So lässt sich die „Out-of-Stock-Rate“ deutlich reduzieren.¹¹⁰ Beispielsweise zeigt ein Regal im Textilhandel an, welche Produkte eines Herstellers noch in welcher Größe und Farbe verfügbar sind. Wie der Barcode wird die RFID-Marke aber nicht nur im Warenbereich genutzt, sondern auch an der Kasse zur Preis-erfassung. Hier wird die Ware dann durch Pulkerfassung schnell und unter

¹⁰⁶ Supply Chain Management (SCM) ist die Zusammenarbeit verschiedener Unternehmen zur Herstellung von Produkten bis zum Verkauf – s. *Töpfer* 2007, 887; *Oertel u.a.* 2004, 84.

¹⁰⁷ *Tellkamp/Quide*, in: *Fleisch/Mattern* 2005, 144.

¹⁰⁸ *Tellkamp/Quide*, in: *Fleisch/Mattern* 2005, 143; <http://www.future-store.org/fsi-internet/html/de/1124/index.html>; <http://www.gerryweber.com/ag-website/de/startseite/unternehmen/unternehmensprofil/rfid>; <http://www.gerryweber.com/ag-website/de/startseite/unternehmen/.../rfid>.

¹⁰⁹ *Friedewald/Raabe* 2010, 148. S. auch <http://www.future-store.org/fsi-internet/html/de/20147/inindex.html>.

¹¹⁰ *Schwindt*, in: *Hildebrand* 2004, 55; *Friedewald/Raabe* 2010, 151.

Ausschluss menschlicher Fehler erfasst und im gleichen Moment der Gesamtpreis errechnet.¹¹¹

Schon heute werden, durch eine am Einkaufswagen angebrachte Anzeige, Kunden individuell umworben. Diese Möglichkeit des Marketings fördert die persönliche Kundenansprache wie beispielsweise im Textilhandel intelligente Spiegel und Umkleidekabinen dem Kunden Informationen über Materialien und Pflegehinweise zu den Kleidungsstücken nennen.¹¹²

Ein weiterer Vorteil der RFID-Technik liegt in der Diebstahlsicherung. Sie dient zum einen der Identifikation der Ware und zum anderen der Warensicherung. Auf der RFID-Marke bleibt solange ein bestimmter Abschnitt aktiviert, bis dieser an der Kasse entwertet wird. Verlässt ein Kunde den Laden mit einem Produkt, an dem die Marke nicht deaktiviert wurde, lösen Scanner am Ausgang Alarm aus.

Im Bereich der Handelslogistik, Paketdienste, Bibliotheken und Gepäckkennzeichnung im Flugverkehr bestehen mannigfache Einsatzmöglichkeiten von kontaktloser Datenauslesung, Identifikation und Lokalisierung.¹¹³ Mit dem Ziel möglichst umfassender Objekterfassung überwachen RFID-Systeme mit einigen Metern Reichweite, wie oben beschrieben, Ein- und Ausgänge von Lagerhallen, registrieren Behälter auf den Paletten und dirigieren unbemannte Gabelstapler zum Einsatzort.¹¹⁴

Aber selbst große Gegenstände wie Container oder Fahrzeuge können bei entsprechender Versorgung und Verteilung von Lesegeräten lokalisiert werden, was für Mautsysteme auf den Autobahnen, für die Containersteuerung und -verfolgung wie auch für die Gepäckkennzeichnung im Flugverkehr unverzichtbar geworden ist. Container, wie auch Fluggepäck werden mit einer RFID-Marke ausgestattet, so dass jederzeit der aktuelle Standort, sei es im Hafen oder im Flughafen, auf dem Schiff oder auf der Autobahn festgestellt werden kann. Neben der Identifikationsnummer enthält jeder Container weltweit Angaben über Eigentümer, TÜV-Termin, Inhalt, Fülldruck und Volumen. Mehr Angaben speichern zu können ist ein Vorteil gegenüber dem herkömmlichen Strichcode, außerdem hält die RFID-Marke schwierigen Umweltbedingungen stand (z.B. Temperaturschwankungen, Strahlen, Säure).

Im industriellen Fertigungsprozess werden alle Einzelteile, die mit einer RFID-Marke versehen sind, automatisch erfasst und identifiziert. Damit lässt sich beispielsweise in der Automobilindustrie, die über eine Vielzahl von Fahrzeugvarianten verfügt, aus der Zusammenfügung sämtlicher Einzelteile zu einem – von dem Kunden bestellten Endprodukt – preisgünstig und fehlerfrei herstellen. Die zu verwendenden Baugruppen, die von Zulieferbetrieben gemäß

¹¹¹ Tellkamp/Quide, in: *Fleisch/Mattern* 2005, 148.

¹¹² Tellkamp/Quide, in: *Mattern* 2005, 158; Hähner, in: *Coroama u.a.* 2003, 30.

¹¹³ Krabs, in: *Jansen* 1999, 13 ff.

¹¹⁴ S. <http://www.heise.de/newsticker/meldung/68509>; SZ v. 3.11.2005, „Vom Einkaufskorb in die Europalette“.

dem Just-in-Time-Prinzip (Produzieren auf Abruf) direkt an das z.B. Montageband geliefert werden, machen eine sofortige und damit lagerlose Verwendung möglich.¹¹⁵ Heute ist dieses Prinzip weltweit umgesetzt.

RFID-Technik wird heute auch zunehmend zur Kontrolle überwachungsbedürftiger Personen, z.B. für ältere oder kranke Menschen oder Arbeitnehmer, die eine gefährliche Tätigkeit (Minen- und Bergarbeiter) ausüben, eingesetzt.¹¹⁶ So trägt jeder Minenarbeiter des schwedischen Staatsbetriebs Luossavaara-Kiirunavaara Aktiebolag eine aktive RFID-Marke an der Kleidung, die eine dynamische Ortung und Visualisierung von Personen ermöglicht.¹¹⁷ Die in der Demenzversorgung genutzten RFID-Marken dienen als Personenortungsanlage und geben dem Pflegepersonal Auskunft über den Aufenthalt von desorientierten Personen. Induktionsschleifen, die im Fußboden vor Türen verlegt sind, geben Alarm, wenn eine Person, versehen mit einer Funkmarke an Kleidung, im Schuh oder als Armband, den Wohnbereich oder die Einrichtung verlassen möchte. Vergleichbar werden RFID-Marken genutzt, um kranken Menschen das Öffnen von Türen unmöglich zu machen, die z.B. zu einem Gefahrenbereich führen. Der Einsatz der RFID-Technik soll hierbei eine Alternative zu einer geschlossenen Unterbringung bieten.¹¹⁸ Ebenfalls ist es im Maßregelvollzug möglich, dass Straftäter zum Zwecke ihrer Lokalisierung RFID-Marken tragen.¹¹⁹

2.1.3.2 Überwachung von Zustand und Qualität

Ausgehend von den derzeitigen Entwicklungen könnten RFID-Systeme, kombiniert mit drahtlosen Sensornetzen¹²⁰ (Wireless Sensor Networks [WSN]), den Zustand der Umwelt, die Schadstoffbelastung in der Luft, Herstellungsprozesse, die Kühlung von Lebensmitteln, Medikamenten und medizinischen Produkten beobachten und überwachen. Auch Infrastruktursysteme, Verkehrssysteme, Integrationsüberwachung von Logistikprozessen und Asset Management können vom Monitoring profitieren.¹²¹

RFID-Marken versehen mit Sensoren, die an den individuellen Paletten, Kisten oder an Gefahrgut angebracht werden, zeichnen kontinuierlich die Temperaturentwicklung und andere Umwelteinflüsse auf dem Weg zum Käufer auf und können damit gleichzeitig Auskunft geben über den Qualitätszustand und die Haltbarkeit der Ware. Die Berechnungsgrundlage wird der transportierten Ware beispielsweise bei Obst- und Gemüsesorten, aber auch bei Chemikalien

¹¹⁵ Sander/Stieler 2006, 26; Hansen, in: ident Jahrbuch 2012, 136.

¹¹⁶ Friedewald/Raabe 2010, 159.

¹¹⁷ <http://www.rfid-basis.de/article - 00149.html>

¹¹⁸ Friedewald/Raabe 2010, 157; Kreicker, NJW 2009, 890, 894.

¹¹⁹ <http://www.heise.de/newsticker/meldung/53789>.

<http://www.heise.de/newsticker/meldung/68879>.

¹²⁰ Sensornetzwerke sind ein Zusammenschluss aus einer Vielzahl von Sensorknoten, die miteinander kommunizieren können.

¹²¹ Roßnagel 2009, 4; ders. 2007b, 51; Münch/Hupp, in: ident Jahrbuch 2012, 115 ff.

angepasst. Fällt der festgelegte Grenzwert, lösen die Sensoren automatisch Alarm aus. Daneben können auch Lüftungssysteme in Industrieanlagen der Überwachung zugänglich gemacht werden. Gegenüber vernetzten Sensoren und auch Übertragungstechnologien wie WLAN und Bluetooth besitzt RFID den Vorteil der Passivität. Energie wird erst bei Abfrage erzeugt und verbraucht.

In Pilotprojekten werden beispielsweise in Brücken, Bauwerke und Straßen drahtlose Sensornetze eingebaut, die physikalische Größen wie Temperatur, Feuchtigkeit messen und dadurch Materialschäden frühzeitig erkennen.¹²²

Unternehmen können mit der RFID-Technik Einsatz und Zustand ihrer Investitionsgüter lückenlos und ständig erfassen. Beispielsweise können die gewonnenen Daten aus Wartungsarbeiten Mängel aufzeigen, um dann durch entsprechende Weiterentwicklung einen höheren Qualitätsstandard zu erreichen. Dies lohnt sich bei höherwertigen Investitionsgütern wie Werkzeugen, Hardware, Zubehör oder angemieteten Objekten. Der Autovermieter Sixt kann durch ein speziell für die Firma entwickeltes RFID-System in Echtzeit auf alle Verfügbarkeitsdaten seiner gesamten Mietwagen zugreifen. Eine integrierte RFID-Marke im Schlüsselanhänger ermöglicht dem Verleiher bei der Rückgabe des Wagens die Daten auszulesen und eine erneute Reservierung sofort vorzunehmen.¹²³ Der Smart-Carsharing-Service von Daimler in der Stadt Berlin bietet Mietern eines Autos, innerhalb des Stadtgebietes, die Möglichkeit an, nach einmaliger Registrierung im car2go Shop die zu mietenden Autos per RFID-Chip, auf dem Führerschein platziert oder in einer Kundenkarte verborgen, zu öffnen.¹²⁴

Elektronische Kennzeichnungssysteme werden schon seit vielen Jahren in der Nutztierhaltung (z.B. Rind, Schaf, Schwein) eingesetzt. Die RFID-Marke kann am Ohr des Tieres angebracht oder in das Tier injiziert werden. Im Oktober 1996 wurden die notwendigen Normen für die Tierkennzeichnung durch die International Organization for Standardization (ISO) verabschiedet.¹²⁵ Damit soll die Betrugssicherung, aber auch die betriebsübergreifende, lückenlose Verfolgung der Tiere (von Geburt bis zum Verkauf des Fleisches) gewährleistet werden.¹²⁶ Ein weiteres Einsatzgebiet für die RFID-Technik seit 2011 ist die Kennzeichnungspflicht mit RFID-Marken bei der Mitnahme von Hunden, Katzen und Frettchen in andere EU-Länder.¹²⁷

¹²² Oertel u.a. 2004, 83; Hähner/Becker/Marrón/Rothermel, in: Mattern 2007, 42.

¹²³ Sander/Stieler 2006, 26.

¹²⁴ <http://www.rfid-im-blick.de/Nachrichten/Personenidentifikation>.

¹²⁵ Für die Identifizierung von Tieren gelten die ISO-Normen 11784, 11785 und 14223, näher Oertel u.a. 2004, 67; Finkenzeller 2002, 233; Artmann, ZAI 1998, 55 ff., abrufbar unter: http://www.gil.de/dokumente/berichte/DDD/R9_20000057.pdf

¹²⁶ Von 1998 bis 2002 liefen in der EU Erprobungen zur elektronischen Kennzeichnung von Tieren (Electronic Identification of Animals [IDEA]).

¹²⁷ Entsprechend der EU-Verordnung Nr. 438/2010, (EU-ABl. L 132 v. 19.5.2010).

Um die „Richtlinie zur Überprüfung der Verkehrssicherheit von Bäumen“, herausgegeben von der Forschungsgesellschaft Landschaftsentwicklung Landschaftsbau e.V., erfüllen zu können, hat die Gemeinde Borsdorf bei Leipzig ein digitales Baumkataster mit Anbindung an ein Geoinformationssystem (GIS) angelegt. Alleeebäume wurden mit einer RFID-Marke versehen, die jeden Baum eindeutig identifiziert. Der Baumkontrolleur trägt vor Ort Schädigungen und mögliche Pflegemaßnahmen in das mobile RFID-Lesegerät (PDA) ein. Im Büro werden diese gesammelten Daten an einen Server übertragen, die vom gemeindlichen Bauhof abgefragt werden.¹²⁸

Im Gesundheitswesen und in der Pharmaindustrie wird zunehmend die RFID-Technik eingesetzt. Die Kennzeichnung von Blutkonserven, Gewebeproben schließen Fehlerquellen und Missbrauch aus. Die angebrachten aktiven RFID-Marken melden Temperaturabweichungen an Blutbeuteln wie auch das Verfallsdatum. Damit wird verhindert, dem Patienten abgelaufene Blutkonserven zu verabreichen. Die Inventarisierung von Geräten und Materialien erfolgt über die Ausstattung mit Marken zuverlässig und zeitsparend. Medikamente, die mit einem Chip ausgestattet sind, garantieren die richtige Dosierung für den richtigen Patienten. RFID-Systeme unterstützen eine schnelle, zielgerichtete Behandlung von Patienten, wenn auf der Marke Daten des Patienten hinterlegt sind, die der Arzt am Krankenbett oder vor einer Operation abrufen kann.¹²⁹

2.1.3.3 Überwachung von Berechtigungen

Touristische Regionen haben schon vor vielen Jahren den Vorteil der RFID-Technik erkannt. So erhalten Kurgäste beispielsweise eine Karte oder ein Armband – versehen mit einer RFID-Marke – die es erlaubt, je nach gebuchten Leistungen, Skilifte, Skiverleih oder Wellness-Bereiche zu nutzen. Der Zutritt erfolgt über Schleusen, die mit Lesegeräten ausgestattet sind. Bezahlvorgänge in Restaurants oder in Bars erfolgen bargeldlos durch Erfassungsgeräte.¹³⁰

Breites öffentliches Interesse weckte der Einsatz von RFID-Systemen im Zuge der Fußball-Weltmeisterschaft (WM) 2006 in Deutschland.¹³¹ Auch hier wurden die Eintrittskarten mit RFID-Marken ausgestattet und die Eintrittsschleusen mit Lesegeräten, die die Daten auf der Eintrittskarte mit dem elektronischen Einlasssystem abglich. Ausgelesen wurde bei der Eintrittskartenkontrolle die gespeicherte Seriennummern (UID) einer Person. Namen oder sonstige Identitätsdaten enthielt der Chip nicht.¹³² Fußballvereine und auch Großveranstalter haben dieses Konzept übernommen. Ein weiteres RFID-Einsatzfeld bilden Berechtigungsprüfungen in Sicherheitsbereichen wie Räume mit beschränktem Zutritt, Industrieanlagen, aber auch öffentliches Gelände.

¹²⁸ <http://www.rfid-basis.de/rfid-anwendungen.html>.

¹²⁹ Oertel u.a. 2004, 72; näher dazu Friedewald/Raabe 2010, 155 ff.

¹³⁰ Oertel u.a. 2004, 77.

¹³¹ S. zu der gesellschaftlichen Diskussion Abschnitt 2.5.

¹³² Conrad, CR 2005, 537, 538; Oertel u.a. 2004, 78.

Für Arbeitgeber bietet die RFID-Technik die Möglichkeit, Mitarbeiter durch eine eingebaute Marke im Firmenausweis zu kontrollieren. Der Arbeitgeber kann beispielsweise dadurch feststellen, ob der Mitarbeiter zur vorgegebenen Zeit am Arbeitsplatz ist oder in welcher Zeit er die vorgegebene Arbeit erledigt hat.¹³³

Menschen selbst können unmittelbar mit Marken versehen werden, wie dies beispielsweise in einem Club in Barcelona Besuchern angeboten wird. Über eine RFID-Marke, die sich unter der Haut befindet, weisen sich die Gäste aus und können gleichzeitig ihre Forderungen für Eintritt und Verzehr über den Chip abbuchen lassen.¹³⁴ Wie Spiegel-Online 2006 berichtete, lassen sich weltweit junge Menschen einen funktionierenden RFID-Chip unter die Haut implantieren, dies gehört zum höchsten Hipness-Faktor.¹³⁵

Steigende Entsorgungskosten und damit hohe Müllgebühren für den Bürger haben die Kommunen veranlasst, die pauschalisierten Gebührenmodelle zu verändern. Als Maß kommt das Abfallgewicht mit der Häufigkeit der Inanspruchnahme der Müllabfuhr in Betracht. Voraussetzung hierfür ist die Ausstattung aller Behälter mit RFID-Marken, die vor Ort bei allen Bürgern aufgestellt werden. Die Müllfahrzeuge sind mit Lesegeräten ausgestattet, die die Daten der RFID-Marke bei der Müllentsorgung erfassen und speichert.¹³⁶ Ziel ist die Erstellung einer individuellen Abrechnung, was bereits seit 2004 in einigen Landkreisen Bayerns schon praktiziert wird.¹³⁷

Weltweit werden in Reisepässe und Personalausweise RFID-Marken integriert, um erweiterte Echtheitsprüfungen zu ermöglichen und weitere biometrische Merkmale wie das Gesichtsfeld und Fingerabdrücke zu speichern. Dies soll eine Fälschung unmöglich machen.¹³⁸

Die Bundesrepublik Deutschland erfüllte mit der Einführung des elektronischen Reisepasses 2005 die Forderung der europäischen Union, das „digitalisierte Gesichtsfeld“ in Ausweispapiere zu integrieren.¹³⁹ Neu ausgestellte Ausweispapiere werden mit einer RFID-Marke versehen, die kontaktlos ausgelesen werden kann. Der RFID-Chip speichert beim „E-Reisepass“ (ePass) das biometrische Passfoto, die Fingerabdrücke, die Bezeichnung der erfassten Finger, die Angaben zur Qualität der Abdrücke sowie die Angaben der maschinenlesbaren Zone.¹⁴⁰ Diese Angaben sind zwingend.¹⁴¹ Seit August 2010 wird der

¹³³ Steinkühler/Raif, Arbeit und Arbeitsrecht 2009, 215.

¹³⁴ Börse unter der Haut – s. *Der Spiegel* v. 29.5.2004, 156, abrufbar unter: <http://www.spiegel.de/spiegel/print/d-31031494.html>.

¹³⁵ <http://www.spiegel.de/netzwelt/tech/implantierte-chips-das-geht-unter-die-haut-a-394217.html>

¹³⁶ Tuminski, in: Jansen 1999, 88 ff.

¹³⁷ Oertel u.a. 2004, 71.

¹³⁸ Oertel u.a. 2004, 72; Eckert 2013, 496 f.

¹³⁹ Entsprechend der Verordnung (EG) Nr. 2252/2004 v. 13.12.2004, (EG-ABl. L 385 v. 29.12.2004).

¹⁴⁰ Zilkens, RDV 2010, 15.

„E-Personalausweis (eID) ausgegeben. Der E-Personalausweis soll als biometrischer Identitätsausweis der Authentisierung im Internet sowie der Speicherung einer elektronischen Signatur dienen.“¹⁴²

2.2 Technische Grundlagen der RFID-Systeme

In diesem Abschnitt werden zum besseren Verständnis wichtige technische Begriffe erläutert. Es werden der Aufbau der einzelnen Komponenten von RFID-Systemen und die prinzipielle Funktionsweise einer RFID-Kommunikation beschrieben sowie die Unterschiede, der sich aus der technischen Bauweise ergebenden Arten von RFID-Systemen dargestellt. Zudem wird auf verschiedene Produktionsweisen und auf die für RFID-Systeme maßgeblichen Standardisierungen eingegangen. Abschließend erfolgt eine Betrachtung der Vorzüge und Nachteile der verschiedenen Systeme aus technischer Sicht, die auf die Gestaltungsmöglichkeiten und Verletzungspotentiale von RFID-Systemen Einfluss haben.

Ein RFID-System besteht aus einem Lesegerät¹⁴³ und mindestens einer RFID-Marke.¹⁴⁴ Im Regelfall ist das RFID-Lesegerät mit einem Hintergrundinformationssystem verbunden, um die vom Lesegerät erfassten Daten anwendungsadäquat weiterverwenden zu können.

In der vorliegenden Untersuchung wird unter RFID-System eine Infrastruktur verstanden, deren wesentliche Bestandteile RFID-Vordergrundsysteme mit RFID-Marken und RFID-Lesegeräte sind sowie einem RFID-Hintergrundsystem, dessen „Herz“ mit dem Lesegerät verbundene Hintergrundinformationssysteme bilden.¹⁴⁵ Da die Leistungsmerkmale eines RFID-Systems durch die technischen Möglichkeiten der RFID-Technik bestimmt werden, hat die Beschreibung der RFID-Technik vor allem die Komponenten und Funktionsweise des Vordergrundsystems zum Gegenstand.

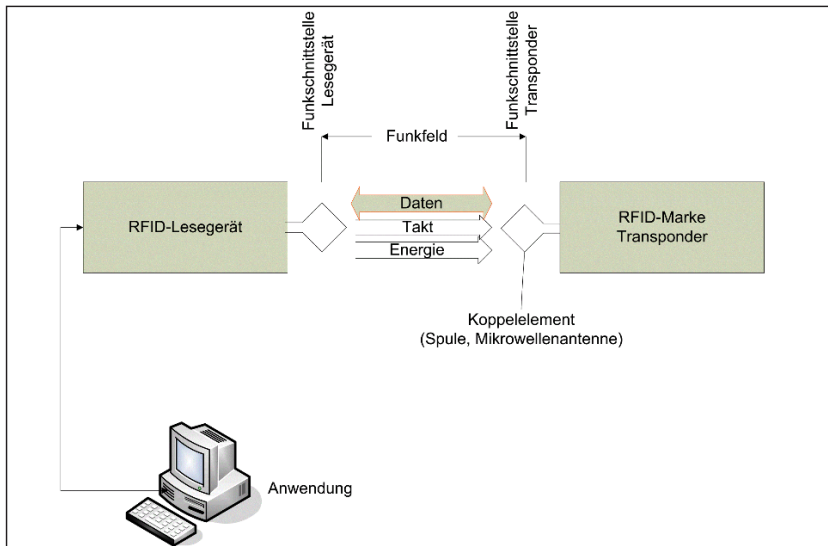
¹⁴¹ S. § 4 Abs. 3 PassG.

¹⁴² Zilkens, RDV 2010, 14.

¹⁴³ Das als „Lesegerät“ bezeichnete Erfassungsgerät kann Lese- und u. U. auch Schreibfunktionen erfüllen.

¹⁴⁴ Finkenzeller 2006, 7; Oertel u.a. 2004, 15; abweichend davon drei Bestandteile verlangend, nämlich zusätzlich einen hinter das Lesegerät geschalteten Rechner – s. Lampel/Flörkemeier/Haller 2005, 70 f.

¹⁴⁵ Somit wie Lampel/Flörkemeier/Haller 2005, 70 f.; vgl. Fn. 2.

Abbildung 2: Aufbau eines RFID-Systems¹⁴⁶

2.2.1 Grundlegender Aufbau eines RFID-Systems

Der Aufbau von RFID-Systemen ist vom Kommunikationsverfahren abhängig. Eine RFID-Marke ist ein mikroelektronischer Schaltkreis, der aus einer Funk-Einheit mit einer Sende- und Empfangsantenne, meist in Form einer Spule oder eines Dipols, sowie aus einer Steuerlogik, meist aus einem Datenspeicher und teilweise aus einer zusätzlichen Energiequelle, besteht.¹⁴⁷

Die Funk-Einheit bildet, vergleichbar zu einem klassischen analogen Datenmodem¹⁴⁸, die Schnittstelle zwischen dem analogen Übertragungskanal vom Lesegerät zur RFID-Marke und ihren digitalen Schaltungselementen.¹⁴⁹ Durch Demodulation wird aus dem modulierten HF-Signal des Lesegerätes ein serieller, digitaler Datenstrom erzeugt.¹⁵⁰ Der dazu erforderliche Takt wird aus dem Übertragungssignal gewonnen. Um Daten an das Lesegerät zurückzusenden, verfügt die Funk-Einheit der RFID-Marke, je nach Bauart, über einen Last- oder Backscattermodulator (oder andere Verfahren z.B. Frequenzteiler), der durch die digitalen Sendedaten angesteuert wird.¹⁵¹

¹⁴⁶ Nach Finkenzeller 2006, 7.

¹⁴⁷ Sottriffer 2003, 25; Finkenzeller 2006, 7 f., 317 ff.; Rietzler/Wagner, in: Jansen 1999, 44.

¹⁴⁸ Datenmodem (Modulator - Demodulator) – s. Fischer 2002, 303.

¹⁴⁹ Finkenzeller 2006, 317.

¹⁵⁰ Schoblick 2005, 82.

¹⁵¹ Finkenzeller 2006, 318; Schoblick 2005, 138.

Die Steuerungslogik ist das Kernelement einer RFID-Marke und steuert als Adress- und Sicherheitslogik alle Operationen auf der Marke.¹⁵² Sie kann in Form eines fest codierten Zustandsautomaten¹⁵³ (State-Machine) oder mittels eines Mikroprozessors ausgeführt sein. Aufwendigere RFID-Marken besitzen Datenspeicher mit höherer Speicherkapazität, die aus irreversiblen oder reversiblen Festwertspeichern (Read Only Memory [ROM]) und aus wiederbeschreibbaren Datenspeichern (Random Access Memory [RAM]) bestehen können.¹⁵⁴ Teilweise verfügen RFID-Marken über eine eigene Energiequelle,¹⁵⁵ in Form eines Stützkondensators oder einer Batterie, um Funktionen der Marke zu unterstützen.¹⁵⁶

Das Lesegerät besteht aus einem Sender und einem Empfänger als NF- oder HF-Schnittstelle, einer Steuerungseinheit sowie einer Antenneneinheit als Luftschnittstelle zur RFID-Marke.¹⁵⁷ Die Steuerungseinheit kodiert in Abfrage-richtung das abfragende Sendesignal und dekodiert in Empfangsrichtung das von der RFID-Marke empfangene Antwortsignal.¹⁵⁸ Der Sender bereitet in Senderichtung das in der Steuerungseinheit kodierte Signal mit Hilfe eines Trägersignals für die Funkschnittstelle auf, während der Empfänger, das von der RFID-Marke empfangene Antwortsignal vom Trägersignal befreit und für die Übergabe an die Steuerungseinheit aufbereitet, die das Empfangssignal dekodiert, auswertet und protokolliert. Das Lesegerät ist meist auch mit einer Datenschnittstelle ausgestattet, über die das von der Steuerungseinheit ausgewertete Signal an einen Rechner oder ein umfassenderes Hintergrundinformationssystem weiter gereicht wird.¹⁵⁹

Ein solches Hintergrundinformationssystem ist eine zentrale Datenverarbeitungsanlage oder mehrere dezentrale, miteinander verbundene Anlagen, an die die von einem oder mehreren Lesegeräten erfassten Daten übermittelt werden. Auf diesem an ein Lesegerät angeschlossenen Hintergrundinformationssystem laufen Anwendungsprogramme, mit Hilfe derer erfasste RFID-Marken registriert, gespeichert, mit weiteren Daten verknüpft oder Daten der RFID-Marken anderweitig aufbereitet und ausgewertet werden können.

¹⁵² Finkenzeller 2006, 322.

¹⁵³ Ein Zustandsautomat oder State-Machine ist ein Schaltwerk (Mealy-Machine), mit dem logische Verknüpfungen durchgeführt werden können mit der zusätzlichen Fähigkeit zu speichern – s. Finkenzeller 2006, 323; Heinrich 2005, 84.

¹⁵⁴ Sottriffer 2003, 27 f.; Finkenzeller 2006, 12.

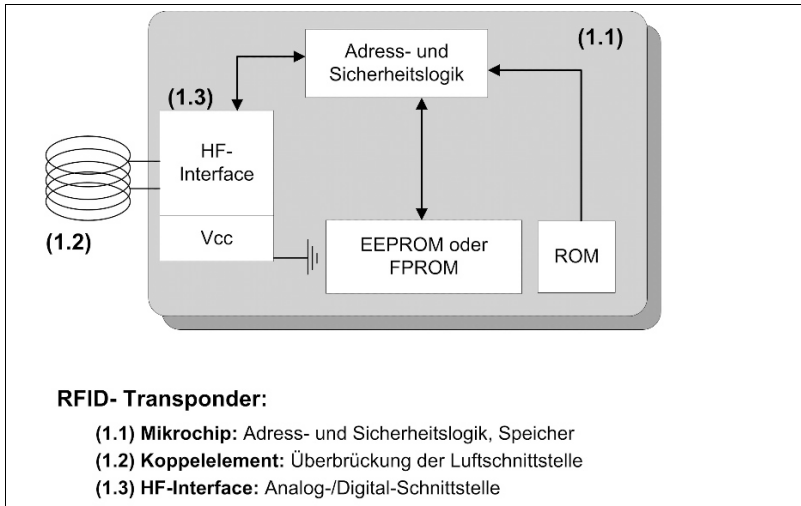
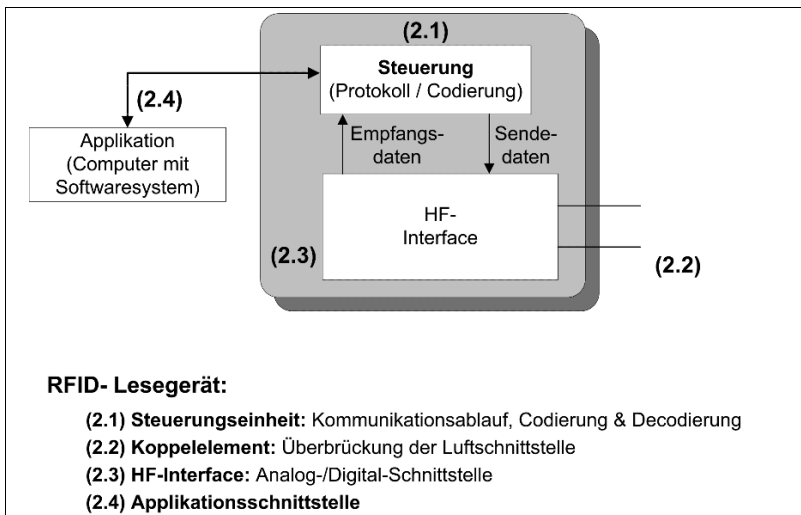
¹⁵⁵ Lampel/Flörkemeier/Haller 2005, 73; Schoblick 2005, 121; Sottriffer 2003, 26.

¹⁵⁶ Schoblick 2005, 118.

¹⁵⁷ Finkenzeller 2006, 7, 356 f.

¹⁵⁸ Sottriffer 2003, 31; Finkenzeller 2006, 362 f.

¹⁵⁹ Finkenzeller 2006, 362.

Abbildung 3: Aufbau einer RFID-Marke oder eines Transponders¹⁶⁰Abbildung 4: Aufbau eines RFID-Lesegeräts¹⁶¹¹⁶⁰ Nach Finkenzeller 2002, 281.¹⁶¹ Nach Finkenzeller 2002, 362.

2.2.2 Unterscheidungsmerkmale

RFID-Systeme insbesondere die Komponenten des RFID-Vordergrundsystems lassen sich anhand ihrer technischen Merkmale unterscheiden. Dabei ergeben die einzelnen, sich teilweise gegenseitig bedingenden Technikmerkmale ein Gesamtbild eines RFID-Systems, das die Leistungsfähigkeit und Eignung für spezifische Anwendungen bestimmt.¹⁶² Danach können RFID-Systeme in niedrige, mittlere und hohe Leistungsklassen und damit in entsprechende Preissegmente eingeteilt werden, da der für eine großflächige RFID-Infrastruktur maßgebliche Kostenfaktor vom Produktionsaufwand der eingesetzten RFID-Marken bestimmt wird.¹⁶³ Technisch können sie nach ihrer Reichweite in Kurz- und Weitdistanz-Systeme eingruppiert werden, was stark von der Kommunikationsfrequenz, dem Kommunikationsverfahren und von der Art der Energieversorgung für die RFID-Marke beeinflusst wird.¹⁶⁴ Weitere wichtige technische Merkmale sind Betriebsart, eingesetzte Speichertechnologien und Rechenleistung auf der RFID-Marke.

2.2.2.1 Energieversorgung der RFID-Marke

Ein zentraler Punkt bei RFID-Marken, wie bei allen mobil eingesetzten Techniken des „Ubiquitous Computing“, die in miniaturisierter Baugröße Rechenleistung und Kommunikationsmöglichkeit anbieten sollen, ist die Versorgung mit Energie. Um die RFID-Marken mit elektrischem Strom zu speisen, kommen hauptsächlich drei Varianten zur Anwendung. Die Energieaufnahme kann markenseitig entweder passiv, aktiv oder semi-passiv erfolgen.¹⁶⁵

Eine passive RFID-Marke besitzt keine eigene Energiequelle. Sie erhält die für ihren Betrieb erforderliche Energie aus dem vom RFID-Lesegerät empfangenen Signal.¹⁶⁶ Dagegen sind aktive RFID-Marken mit einer eigenen Energiequelle ausgestattet.¹⁶⁷ Dies kann eine Stützbatterie in Form einer Folienbatterie¹⁶⁸ oder Miniaturknopfzelle sein. Sie versorgt jedoch meist nur die inneren Schaltkreise oder implementierte Sensorbausteine auf der RFID-Marke.¹⁶⁹ Die Energie für die Datenübertragung wird weiterhin aus dem vom Lesegerät empfangenen Signal gewonnen. Um für den Betrieb der aktiven RFID-Marke den Energieverbrauch zu optimieren, wird diese in einen stromsparenden Bereitschaftsmodus versetzt. Sobald die Marke in den Ansprechbereich eines Lesegeräts gelangt und ein Aktivierungssignal erhält, baut sich die Kommunikation

¹⁶² Oertel u.a. 2004, 39; Lampe/Flörkemeier/Haller 2005, 77 ff.

¹⁶³ Oertel u.a. 2004, 39; zu den Transponderkosten – s. Lampe/Flörkemeier/Haller 2005, 82.

¹⁶⁴ Finkenzeller 2006, 22 f.; Schoblick 2005, 122 f.

¹⁶⁵ Lampe/Flörkemeier/Haller 2005, 73; Finkenzeller 2006, 24, 318; Oertel u.a. 2004, 31.

¹⁶⁶ Sotriffer 2003, 26; Finkenzeller 2006, 13; Schoblick 2005, 121.

¹⁶⁷ Oertel u.a. 2004, 31; Schoblick 2005, 122; Finkenzeller 2006, 23, 149.

¹⁶⁸ Schoblick 2005, 122; Folienbatterien auf Lithium-Polymer Basis sind wieder aufladbar. Ihre Größe beträgt ca. ein Zehntel Millimeter – s. <http://www.smart-power.fhg.de>.

¹⁶⁹ Sotriffer 2003, 28; Finkenzeller 2006, 52.

mit dem RFID-Lesegerät, unterstützt von der eigenen Energiequelle, auf.¹⁷⁰ Die Energiequelle auf der RFID-Marke kann einerseits dazu dienen, außerhalb des Ansprechbereichs des Lesegeräts die Betriebsfähigkeit zu erhalten und andererseits die Kommunikationsreichweite zu erhöhen.¹⁷¹

Form der Energieversorgung	Eigene Energiequelle	Energiegewinnung für Schaltkreise	Energiegewinnung für Datenübertragung
Passiv	keine	über Lesegerät	über Lesegerät
Aktiv	Stützbatterie	Eigenversorgung	über Lesegerät
Semiaktiv	Stützbatterie	nur teilweise	über Lesegerät

Tabelle 1: Energieversorgung der RFID-Marken

2.2.2.2 Reichweite und Kommunikationsfrequenzen von RFID-Systemen

Ebenso können RFID-Systeme nach ihrer Kommunikationsreichweite eingeteilt werden. Diese ist von der verwendeten Kommunikationsfrequenz und dem verwendeten Kopplungsverfahren abhängig.¹⁷² Maßgeblich für die Unterscheidung ist die Reichweite, in der noch eine fehlerfreie¹⁷³ Kommunikation erfolgt.

Grundsätzlich gibt es Systeme für kurze und lange Distanzen, wobei Kurzstanzsysteme eng oder fern gekoppelt sein können und im elektromagnetischen Nahfeld des Lesegerätes arbeiten.¹⁷⁴ Eng gekoppelte RFID-Systeme (Close-Coupling-Systeme) können in Frequenzbändern von einem Hertz bis dreißig Megahertz betrieben werden und überbrücken eine Entfernung bis zu einem Zentimeter.¹⁷⁵ Bei ihnen erfolgt die Datenübertragung entweder durch induktive oder bei sehr kurzen Funkstrecken durch kapazitive Kopplung.¹⁷⁶ Diese eng gekoppelten Systeme finden aufgrund ihrer sehr geringen Reichweite von weniger als einem Zentimeter und der Verfügbarkeit großer Energiemengen häufig in Anwendungen mit hohen Sicherheitsanforderungen, wie elektronische Türschließanlagen oder Karten mit Zahlungsfunktion, Verwendung.¹⁷⁷

¹⁷⁰ Finkenzeller 2006, 52.

¹⁷¹ Sottriffer 2003, 28; Finkenzeller 2006, 24, 52.

¹⁷² Finkenzeller 2006, 13; Sottriffer 2003, 27.

¹⁷³ Dabei darf ein bestimmter Schwellenwert der Übertragungsfehlerhäufigkeit nicht überschritten werden, der eine ordnungsgemäße Kommunikation auch unter Zuhilfenahme von Fehlerkorrekturmechanismen sicherstellt.

¹⁷⁴ RFID-Systeme werden oft auch im englischen als Systeme mit „Close Coupling“ und „Remote Coupling“ sowie „Long Range“ bezeichnet – s. Schoblick 2005, 123; Finkenzeller 2006, 13.

¹⁷⁵ Oertel u.a. 2004, 39; Finkenzeller 2006, 22, 53; Lampel/Flörkemeier/Haller 2005, 77 f.

¹⁷⁶ Finkenzeller 2006, 22, 54; Oertel u.a. 2004, 31, 40.

¹⁷⁷ Oertel, u.a. 2004, 40; Finkenzeller 2006, 22.

Ferngekoppelte RFID-Systeme des Nahfeldes (Remote-Coupling-Systeme) arbeiten typischerweise in Frequenzbereichen unterhalb 135 KHz und bei 13,56 MHz. Ihre Reichweite beträgt bis zu einem Meter.¹⁷⁸ Für die Datenübertragung findet überwiegend das Kommunikationsverfahren der induktiven Kopplung Verwendung.¹⁷⁹ Sie werden meist für Anwendungen in kontaktlosen Chipkarten eingesetzt, bei denen in der Regel nach ihrer Kommunikationsreichweite zwischen „Proximity Cards“ und „Vicinity Cards“ unterschieden wird. Der Abstand von der RFID-Marke und dem Lesegerät beträgt bei den sogenannten „Proximity-Coupling-Systemen“ (ISO/IEC 14443) höchstens 20 cm und bei den „Vicinity-Coupling-Systemen“ (ISO/IEC 15693) bis zu ungefähr einem Meter.¹⁸⁰

Die theoretische Maximalreichweite ist abhängig von der Frequenz oder Länge der elektromagnetischen Welle λ . Im Nahfeld übersteigt diese nicht das Verhältnis Wellenlänge λ zum zweifachen von π . Ist dieses Verhältnis größer als $\lambda / 2 \pi$, spricht man von Fernfeld (Long-Range-System).¹⁸¹ Allerdings wird dieser theoretisch mögliche Ansprechbereich eines Lesegeräts nie erreicht, da vielfältige Faktoren, wie Antennengestalt oder zu durchdringendes Material, die Sendeeigenschaften dämpfend beeinflussen.

Dagegen können RFID-Systeme des Langdistanz-Bereiches (Long-Range-Systeme), die im elektromagnetischen Fernfeld arbeiten, eine Funkstrecke von mehr als einem Meter abdecken.¹⁸² Sie nutzen typischerweise die Frequenzen im Ultrahochfrequenz- und Mikrowellenbereich bei 868 und 915 MHz sowie bei 2,45 GHz.¹⁸³ Meist verfügen sie über eine Reichweite von 1,5 bis zu 10 Metern, in Ausnahmefällen können aber auch größere Distanzen von ungefähr 100 Metern überwunden werden.¹⁸⁴ Dabei dürften sogar im Frequenzband von 5,8 GHz, dessen technische Nutzung sich noch in einem Entwicklungsstadium befindet, Entfernungen von einem Kilometer überbrückbar sein.¹⁸⁵ Anders als bei RFID-Systemen des Nahfeldes findet die Kommunikation bei Langdistanz-Systemen im Fernfeld überwiegend mittels eines Rückstreuverfahrens (Backscatter-Verfahren) statt,¹⁸⁶ bei dem das von der RFID-Marke zurück gesandte Echosignal ausgewertet wird. Teilweise kommen zusätzliche Energiequellen auf

¹⁷⁸ *Lampel/Flörkemeier/Haller* 2005, 77 f.; *Finkenzeller* 2006, 22; *Oertel u.a.* 2004, 40.

¹⁷⁹ *Finkenzeller* 2006, 22; *Schoblick* 2005, 123.

¹⁸⁰ *Oertel u.a.* 2004, 40; *Finkenzeller* 2006, 22; *Schoblick* 2005, 144.

¹⁸¹ Reichweite im Nahfeld $< \lambda / 2 \pi$ – s. *Schoblick* 2005, 113; *Finkenzeller* 2006, 121.

¹⁸² *Finkenzeller* 2006, 23, 50; *Oertel u.a.* 2004, 40.

¹⁸³ So *Oertel u.a.* 2004, 40; abweichend dazu *Finkenzeller* 2006, 23, 50, der als Arbeitsfrequenz 2,5 GHz angibt.

¹⁸⁴ *Finkenzeller* 2006, 23, 50; *Lampel/Flörkemeier/Haller* 2005, 79; *Schoblick* 2005, 125.

¹⁸⁵ *Oertel u.a.* 2004, 40.

¹⁸⁶ *Finkenzeller* 2006, 23; *Oertel u.a.* 2004, 40. Daneben gibt es auch RFID-Marken, die mit Oberflächenwellen arbeiten – s. näher *Finkenzeller* 2006, 23, 361 f., 157 ff.

der RFID-Marke zum Einsatz, die aber ausschließlich der Versorgung ihrer Schaltkreise und Speicherbausteine dienen.¹⁸⁷

Kommunikationsdistanz	Bezeichnung	Reichweite (in Metern)	Typische Arbeitsfrequenzen	Kommunikationsverfahren
Kurzstanzbereich	Eng gekoppelte Systeme (Close Coupling)	0,001 bis 0,01	0 bis 30 MHz	Induktive / kapazitive Kopplung
	Ferngekoppelte Systeme (Remote-Coupling)	< 1	< 135 kHz und 13,56 MHz	Induktive Kopplung
Langstanzbereich	Fernfeld-Systeme (Long Range)	> 1	Europa: 868 MHz USA: 915 MHz und 2,45 GHz; In Diskussion: 5,8 GHz	Rückstreuverfahren (Backscatter-Verfahren)

Tabelle 2: Reichweite und Arbeitsfrequenzen von RFID-Systemen

2.2.2.3 Rechenkapazität und Speichertechnologien

Wichtig für die Auswahl von RFID-Systemen ist die auf einer RFID-Marke verfügbare Rechenkapazität.¹⁸⁸ Dazu gehören als weiteres Unterscheidungsmerkmal auch die zum Einsatz kommenden Speichertechnologien auf der RFID-Marke.¹⁸⁹ Insbesondere die gegenüber bisherigen Kennzeichnungssystemen erhöhte Rechen- und Speicherkapazität macht RFID-Technik für den Einsatz in Anwendungen moderner IuK-Systeme interessant.

Die Verwendung elektronischer Datenspeicher, deren Kapazität bei hochwertigen RFID-Marken durchaus heute schon mehrere Kilobyte betragen kann, ermöglicht eine Speicherung von zusätzlichen Nutzdaten direkt auf der RFID-Marke. Hinzu kommt die zunehmende Verfügbarkeit von Rechenleistung auf ihr, die nicht nur die Verwaltung von unterschiedlichen Speicherbereichen, sondern auch die Implementierung von kryptographischen Funktionen erlaubt.¹⁹⁰ Grundsätzlich gibt es RFID-Marken, deren Datenspeicher wieder beschreibbar (Read/Write-Systeme) und welche, bei denen der Dateninhalt im

¹⁸⁷ Schoblick 2005, 138; Finkenzeller 2006, 23.

¹⁸⁸ Rechenkapazität meint die Möglichkeit der Datenverarbeitung im technischen Sinn.

¹⁸⁹ Lampel/Flörkemeier/Haller 2005, 81.

¹⁹⁰ Oertel u.a. 2004, 27; Sottriffer 2003, 27, 28.

Herstellungsprozess¹⁹¹ oder vor ihrer Verwendung fest einprogrammiert wird (Read-Only-Systeme).¹⁹²

Die einfachsten RFID-Marken speichern lediglich ein Bit, wodurch sich zwei Zustände abbilden lassen. Die Marke befindet sich im Ansprechbereich des Lesegeräts oder nicht.¹⁹³ Dabei sind auch Bauweisen erhältlich, bei denen sich die RFID-Marke reaktivieren, also quasi wieder beschreiben lässt. Diese so genannten „Ein-Bit-Transponder“ benötigen keine aufwendige Steuerlogik und werden wegen ihres dadurch geringen Herstellungspreises meist im Rahmen von Diebstahlsicherungssystemen wie die elektronische Artikelsicherung (Electronic Article Surveillance [EAS]) eingesetzt.¹⁹⁴

Ebenfalls können die RFID-Marken zu einer niedrigen Leistungsklasse gezählt werden, die eine mehrere Byte große Identifikationsnummer besitzen, die aber nicht veränderlich ist.¹⁹⁵ Als Festwert- oder ROM-Lösung¹⁹⁶ besitzen sie keine aufwendige Adress- und Sicherheitslogik und unterstützen meist keine Vielfachzugriffs- oder Antikollisionsverfahren¹⁹⁷. Die dadurch geringe Leistungsaufnahme ermöglicht es, größere Reichweiten zu überbrücken. Diese Festwert-RFID-Marken sind zwar günstiger in der Herstellung,¹⁹⁸ variable Informationen müssen jedoch im Hintergrundinformationssystem abgelegt werden. Sie kommen daher für Anwendungen in Betracht, bei denen eine niedrigpreisige Lösung und nur eine geringere Speicherkapazität benötigt werden.

Im mittleren Leistungsfeld können RFID-Marken angesiedelt werden, die mit wieder beschreibbaren Datenspeichern sowie einem festcodierten Zustandsautomaten oder einer „State-Machine“ ausgestattet sind. Diese führt einfache Befehle des Lesegeräts zum selektiven Lesen und Beschreiben des Datenspeichers aus und unterstützt Vielfachzugriffs- (Multi-Access) oder Antikollisionsverfahren (Anticollision-System). Teilweise sind kryptographische Funktionen mit implementiert.¹⁹⁹

¹⁹¹ Programmierung von Festwert-RFID-Marken erfolgt, indem bestimmte Leiterbahnen durch entsprechende Belichtungsmasken direkt eingebrannt oder durch Laser unterbrochen werden – s. *Finkenzeller* 2006, 343, 378; *Fischer* 2002, 173.

¹⁹² *Oertel u.a.* 2004, 30; *Finkenzeller* 2006, 25, 324.

¹⁹³ *Finkenzeller* 2006, 12, 32.

¹⁹⁴ *Schoblick* 2005, 129; *Finkenzeller* 2006, 12, 25, 32.

¹⁹⁵ *Finkenzeller* 2006, 25.

¹⁹⁶ Ein ROM- (Read Only Memory) oder Festwertspeicher ist ein digitaler Speicher, in dessen Halbleiterstruktur Daten dauerhaft und unveränderlich abgelegt werden, ohne dass eine Löschung der Daten elektrisch oder optisch möglich ist. In dieser Form werden auch bei dieser Klasse von RFID-Marken die Identifikationsnummer fest einprogrammiert – s. *Oertel u.a.* 2004, 30; oder auch WORM (Write Once Read Many) – s. *Lampel/Flörkemeier/Haller* 2005, 81.

¹⁹⁷ S. unten.

¹⁹⁸ *Oertel u.a.* 2004, 30; *Finkenzeller* 2006, 26.

¹⁹⁹ *Finkenzeller* 2006, 26, 213 f.; *Sottriffer* 2003, 27.

Bei dieser Klasse von RFID-Marken beträgt die Kapazität des Datenspeichers, meist als EEPROM²⁰⁰, SRAM²⁰¹ oder Flash-EEPROM²⁰² ausgeführt, zwischen wenigen Bytes bis zu mehreren Kilobytes.²⁰³ Gerade bei RFID-Marken mit Zustandsautomaten ist der Übergang zu der nächst höheren Leistungsklasse fließend, da die festcodierten Zustandsautomaten von ihrer Rechenkapazität her an die von verbaubaren Mikroprozessoren heranreicht.²⁰⁴

Eine höhere Leistungsklasse bilden Systeme, bei denen RFID-Marken eingesetzt werden, die statt mit einem unflexiblen, festcodierten Zustandsautomaten mit einem Mikroprozessor²⁰⁵ und einem entsprechenden Betriebssystem arbeiten, das die Ausführung komplexerer Algorithmen zur Verschlüsselung und Authentifizierung erlaubt.²⁰⁶ Dazu gehören zum einen RFID-Marken, die auch

²⁰⁰ Im Gegensatz zu festcodierten Daten der einfacheren RFID-Marken lassen sich bei EEPROM und FLASH-E-PROM Daten löschen und wieder neu einschreiben. Beim EEPROM (Electrically Erasable Programmable Read Only Memory) erfolgt der Schreib- und Löschvorgang mittels Spannungsimpulsen, die durch ein zusätzliches Gerät, den EPROM-Programmierer, erzeugt werden – s. *Finkenzeller* 2006, 345, 440; *Fischer* 2002, 153; *Rankl/Effing* 2002, 77. Dabei können bei EEPROM die Speichergröße von 16 Byte bis 8 KByte 10^6 - 10^8 -mal wiederholt werden. Allerdings benötigt ein Löschvorgang mehrere Minuten – s. *Rankl/Effing* 2002, 74 f.; *Finkenzeller* 2006, 30.

²⁰¹ Bei dem SRAM-Speichern (Static Random Access Memeroy) bleibt der Speicherinhalt auch ohne Energieversorgung erhalten. Bei diesen wird der Speicherinhalt mittels Transistoren, die als bistabile Kippstufe geschaltet sind, abgebildet. Diese werden auch Flip-Flop genannt – s. *Finkenzeller* 2006, 344, 440. Verbaut werden Speichergrößen von 256 Byte bis zu 64 Kbyte, allerdings meist nur bei Mikrowellensystemen – s. *Finkenzeller* 2006, 12, 18; *Heinrich* 2005, 83.

²⁰² Beim Flash-EEPROM geschieht die Speicherung von Daten funktionell, vergleichbar zu EEPROM. Anders als beim EEPROM werden die Daten auf einem Flash-EEPROM segmentweise geschrieben und gelöscht – s. *Finkenzeller* 2002, 177; *Rankl/Effing* 2002, 75. Durch die einfache und platzsparende Anordnung der Speicherzellen ist die Speicherkapazität beliebig skalierbar. Ohne Stromspeisung sollen die Daten bis zu zehn Jahren erhalten bleiben. Allerdings ist das Programmieren der Flash-EEPROM kompliziert und zeitaufwendig – s. *Finkenzeller* 2002, 287; *Rankl/Effing* 2002, 79 f.

²⁰³ *Finkenzeller* 2006, 26 f.

²⁰⁴ *Finkenzeller* 2006, 323.

²⁰⁵ Mikroprozessorsysteme arbeiten mit einem RAM als Arbeitsspeicher – s. *Finkenzeller* 2006, 337; *Rankl/Effing* 2002, 932. Ein RAM (Random Access Memory) oder Arbeitsspeicher ist ein schneller Zwischenspeicher eines Mikroprozessors für Daten und Programme, um die Gesamtleistung des Systems zu steigern – s. *Finkenzeller* 2006, 344; *Oertel u.a.* 2004, 31; *Fischer* 2002, 382. Ein herkömmlicher Arbeitsspeicher benötigt für den Datenerhalt eine kontinuierliche Energieversorgung. Wird diese unterbrochen, gehen die vorgehaltenen Daten verloren. Deshalb finden im Bereich der RFID-Systeme als schnelle Zwischenspeicher, sogenannte SRAM-, FRAM-Speicher Verwendung, deren Speicherinhalt auch ohne kontinuierliche Energieversorgung nicht verloren geht – s. *Finkenzeller* 2006, 440; *Oertel u.a.* 2004, 31; *Rankl/Effing* 2002, 81.

²⁰⁶ *Finkenzeller* 2006, 26, 287, 337.

als kontaktlose Chipkarten²⁰⁷ bezeichnet werden. Diese verwenden neben SRAM²⁰⁸ zunehmend auch FRAM²⁰⁹ und speichern um die hundert Kilobyte.

Zum anderen gehören zu der hohen Leistungsklasse moderne Chipkarten, wie Karten mit dualen Schnittstellen (Dual-Interface-Card), die neben einem Mikroprozessor mit einem kryptographischen Coprozessor bestückt sind. Ihre Speicherkapazität kann mehrere hundert Kilobyte betragen. Aufgrund ihrer größeren Rechen- und Datenspeicherleistung eignen sie sich vor allem für Anwendungen mit hohen Sicherheitsanforderungen.²¹⁰

Letztlich bedingen die Leistungsmerkmale vornehmlich den Beschaffungswert der RFID-Marken, der für die Einteilung von RFID-Systemen eine Orientierung bieten kann.²¹¹ Danach bilden RFID-Marken mit geringer Speicherkapazität und geringer Rechenleistung das Niedrigpreissegment. Zum mittleren Preissegment werden RFID-Marken mit einem Zustandsautomaten als Schaltwerk gezählt. Im Hochpreissegment findet man überwiegend RFID-Marken, mit einem Mikroprozessor als Chip-Kartensystem.

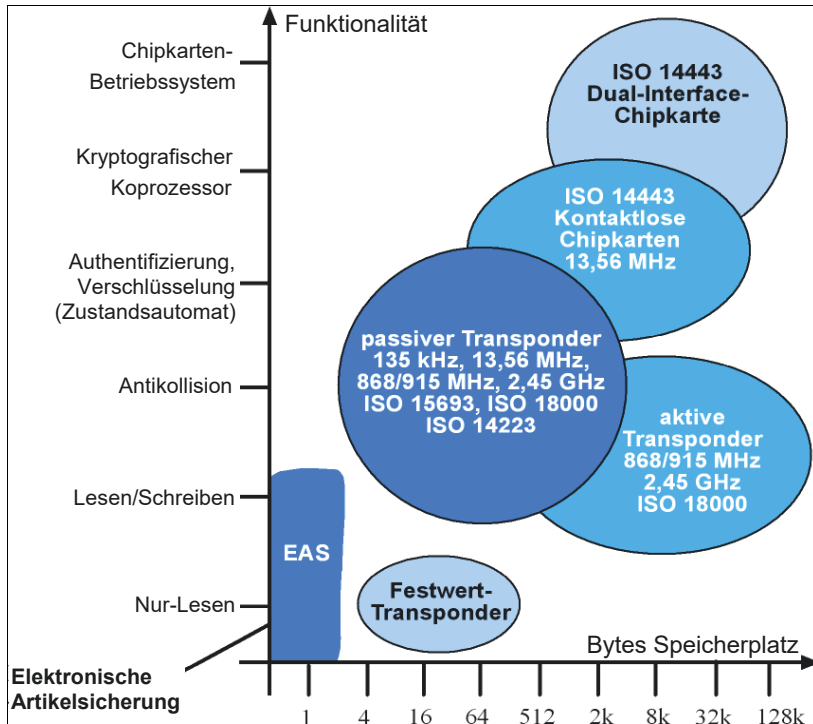
²⁰⁷ Diese Bezeichnung wird uneinheitlich verwendet. Teilweise werden hierzu auch RFID-Marken gezählt, die zum einen in die mittlere Leistungsklasse fallen und zum anderen gemäß der Spezifikation 14443 oder der 15693 arbeiten – s. *Finkenzeller* 2006, 338 ff., 391.

²⁰⁸ SRAM (Static Random Access Memory) sind statische Speicher, die zum Erhalt des Speicherinhalts keine zyklische Wiederauffrischung des Inhalts benötigen – s. *Finkenzeller* 2006, 440. Sie kommen hierzu mit einer konstanten Stromversorgung aus. Ihre Zugriffszeit ist gegenüber DRAM-Speicher geringer, jedoch sind sie wegen des größeren Platzbedarfs auf dem Chip teurer – s. *Rankl/Effing* 2002, 946.

²⁰⁹ Da RAM-Lösungen mit SRAM-Speicher nicht nur verhältnismäßig hohe Stromaufnahmen aufweisen, sondern auch mit vergleichsweise hohen Produktionskosten der RFID-Marken verbunden sind, werden zunehmend in RFID-Systemen FRAM-Speicher (Ferroelectric Random Access Memory) eingesetzt. Diese neu entwickelte Speichertechnologie benötigt für den Datenerhalt gegenüber herkömmlichen RAM-Speichern keine Stromversorgung. FRAM-Speicher sind zwar zu gängigen EEPROM kompatibel, ermöglichen aber bis zu 10.000-fach schnellere Schreib- und Lesezugriffe und sind gegenüber EEPROM mit garantierten 10¹⁰ Schreib-Lesezyklen leistungsfähiger. Die Datenhaltbarkeit liegt bei über zehn Jahren, auch dann, wenn der Chip starken Temperaturschwankungen ausgesetzt ist – s. *Finkenzeller* 2006, 440; *Oertel u.a.* 2004, 31; *Rankl/Effing* 2002, 80.

²¹⁰ *Finkenzeller* 2006, 27, 338.

²¹¹ *Oertel u.a.* 2004, 39; *Finkenzeller* 2006, 26.

Abbildung 5: Klassifizierung von RFID-Marken bzw. Transponder²¹²

2.2.2.4 Kommunikationsverfahren

Die Kommunikation zwischen RFID-Lesegerät und RFID-Marke erfolgt über die Luftschnittstelle. Je nach technischem Konzept der RFID-Systeme werden unterschiedliche physikalische Kopplungsverfahren oder Rückstreuverfahren verwendet.²¹³ Die Kommunikation mittels Koppelung wird durch Felder hergestellt, die magnetisch²¹⁴, elektrisch²¹⁵ (kapazitiv), elektro-magnetisch²¹⁶ oder akusto-magnetisch²¹⁷ erzeugt werden. Für andere Kommunikationsverfahren, wie das Rückstreuverfahren dienen elektromagnetische Wellen²¹⁸ oder Schallwellen. In der Regel werden für Kommunikation und Energieversorgung das Verfahren

²¹² Nach Finkenzeller 2002, 24.

²¹³ Rankl/Effing 2002, 94; Finkenzeller 2006, 13, 54, 65, 125; Oertel u.a. 2004, 31.

²¹⁴ Finkenzeller 2006, 54.

²¹⁵ Finkenzeller 2006, 54, 55 ff.

²¹⁶ Finkenzeller 2006, 38 f.

²¹⁷ Finkenzeller 2006, 40 f.

²¹⁸ Schoblick, 2005, 105; Finkenzeller 2006, 50 ff.

der induktiven Kopplung und das Rückstreuverfahren eingesetzt. Daneben findet bei Nahfeld-Systemen das Verfahren der magnetischen und kapazitiven Kopplung Verwendung.²¹⁹

2.2.2.5 Betriebsarten

Bei RFID-Marken, die eine Speicherkapazität von mehreren Byte besitzen, können Daten zum und vom Lesegerät auf verschiedene Weise übertragen werden. Als Übertragungsverfahren stehen Duplex-Verfahren in Form von Voll-Duplex (Full-Duplex [FDX]) und Halb-Duplex (Half-Duplex [HDX]) sowie sequentielle Verfahren (Sequentiell System [SEQ]) zur Verfügung.²²⁰ Im Voll-duplex-Verfahren werden Daten zwischen RFID-Marke und RFID-Lesegerät in beiden Richtungen²²¹ gleichzeitig übertragen. Dagegen erfolgt die Datenübertragung im Halbduplex-Verfahren zeitversetzt. Es wird immer nur eine Übertragungsrichtung, also vom oder zum Lesegerät bedient. In beiden Duplex-Verfahren werden die RFID-Marken stetig mit Energie versorgt.²²² Um während der periodischen Sendepausen des Lesegerätes den Betrieb der RFID-Marken zu gewährleisten, sind seitens der RFID-Marke Energiequellen, wie Stützkondensatoren oder Batterien erforderlich.²²³ Deshalb ist dieses Verfahren in der Praxis weniger gebräuchlich.

Vollduplexverfahren (FDX)	Halbduplexverfahren (HDX)	Sequentielles Verfahren (SEQ)
gleichzeitige Daten-Übertragung zwischen RFID-Marke und RFID-Lesegerät	zeitversetzte Daten-Übertragung zwischen RFID-Marke und RFID-Lesegerät	zeitversetzte unterbrochene Daten-Übertragung zwischen RFID-Marke und RFID-Lesegerät
kontinuierliche Energieübertragung vom Lesegerät zur RFID-Marke	kontinuierliche Energieübertragung vom Lesegerät zur RFID-Marke	nicht kontinuierliche Energieübertragung vom Lesegerät zur RFID-Marke. Unterbrechung der Energieübertragung nur während der Datenübertragung Lesegerät zur RFID-Marke

Tabelle 3: Betriebsarten von RFID-Systemen

²¹⁹ Rankl/Effing 2004, 94; Schoblick 2005, 111.

²²⁰ Schoblick 2005, 142 f.; Finkenzeller 2006, 11; Sottriffer 2003, 37.

²²¹ Der Übertragungskanal vom Lesegerät (Basisstation zum Transponder – untergeordnetes System) wird auch als Downlink, der umgekehrte Übertragungskanal als Uplink bezeichnet – s. Rankl/Effing 2002, 916; Sottriffer 2005, 37.

²²² Rankl/Effing 2002, 952, 924; Finkenzeller 2006, 42 f.

²²³ Schoblick 2005, 143; Finkenzeller 2006, 12.

2.2.2.6 Kommunikationsfrequenz

Die verwendeten Frequenzbereiche sind von den Kommunikationsverfahren und der zu erzielenden Reichweite abhängig. In der Praxis nutzen RFID-Systeme für ihre Kommunikation Frequenzen im Lang-, Kurz-, Ultrakurz- oder Mikrowellenbereich. Etabliert haben sich überwiegend Frequenzbereiche für RFID-Systeme unter 135 kHz sowie 13,56 MHz, um 868 MHz in Europa und um 915 MHz in den USA.²²⁴ Produkte für den Frequenzbereich von 2,45 GHz haben noch keine Produktionsreife erlangt.²²⁵ Dabei gelten Frequenzbänder unter 135 KHz und 13,56 MHz als weltweit harmonisiert. Für weltweit einsetzbare RFID-Systeme steht noch der Frequenzbereich 5,8 GHz zur Verfügung, der bisher noch kaum genutzt wird.²²⁶

Neben nicht einheitlich vergebenen Frequenzbändern für RFID-Anwendungen sind in den einzelnen Ländern derzeit auch die zulässigen Sendestärken der Lesegeräte verschieden. In den Vereinigten Staaten von Amerika beispielsweise sind im Bereich um 915 MHz eine maximale Sendeleistung von etwa 4 Watt,²²⁷ in Europa hingegen nur 2 Watt erlaubt.²²⁸ Dagegen ist der RFID-Einsatz in China unreguliert.²²⁹ Allein dadurch ergibt sich bei baugleichen RFID-Systemen ein Unterschied zwischen der theoretisch erzielbaren Reichweite, die in den USA 6 bis 8 Meter und in Europa 1 bis 2 Meter beträgt.²³⁰

Bereich	Frequenz in MHz		Reichweite	Sendestärke	Einsatzgebiete (Geographisch)
Niederfrequenz	< 0,135		1 bis 2,5 m	0,5 Watt	weltweit
Hochfrequenz	13,5		1 bis 2,5 m	0,5 Watt	weltweit
Ultrahochfrequenz	850 bis 950	865 bis 868	1 bis 2 m	2 Watt	EU (weitgehend)
		902 bis 928	6 bis 8 m	4 Watt	USA
Mikrowelle	2,45 bzw. 5,8 GHz		bis zu 15 m (in Einzelfällen bis zu 1 km)		teilweise nicht EU

Tabelle 4: Frequenzbereiche von RFID-Systemen

²²⁴ Lampe/Flörkemeier/Haller 2005, 73 ff.

²²⁵ Oertel u.a. 2004, 28.

²²⁶ Meyer, in: Jansen 1999, 29; Oertel u.a. 2004, 28.

²²⁷ Oertel u.a. 2004, 30.

²²⁸ OECD 2006, 19; andere Werte bei Oertel u.a. 2004, 30.

²²⁹ OECD 2006 19.

²³⁰ Oertel u.a. 2004, 30.

2.2.3 Prinzipielle Funktionsweise von RFID-Kommunikation

Die Kommunikation zwischen einer RFID-Marke und dem RFID-Lesegerät erfolgt über die Luftschnittstelle. Ein Lesegerät strahlt über seine Antenne elektromagnetische Wellen ab. Mit dieser werden, unabhängig von der Bauart des RFID-Systems, Datensignale, Taktinformation und Energie für die RFID-Marke übertragen. Sobald eine RFID-Marke in den Ansprechbereich eines RFID-Lesegeräts gelangt, findet zwischen den beiden Systemteilen ein undirektionaler (meist bei Read-Only-RFID-Marke, Read-Write-Marke aber denkbar) oder bidirektionaler (bei Read-Write-RFID-Marke) Datenfluss statt. Dabei kann eine RFID-Marke entweder ausgelesen oder beschrieben werden.

In beiden Fällen kann immer nur eine einzelne RFID-Marke vom Lesegerät bearbeitet werden. Anders als bei den gebräuchlichen digitalen Funktechniken, wie „Global System for Mobile Communications“ (GSM)²³¹, drahtlosen Netzwerktechniken (IEEE 802.11-Standard²³²) oder der des Bluetooths (IEEE 802.15-Standard) funktioniert die RFID-Technik grundsätzlich nur auf Abruf durch das Lesegerät.²³³ In der Regel werden für die Energieversorgung und Kommunikation das Verfahren der induktiven Kopplung und das Rückstreuverfahren eingesetzt. Daneben findet bei Nahfeld-Systemen das Verfahren der kapazitiven Kopplung Verwendung.

2.2.3.1 Ein-Bit-RFID-Systeme

Bei „Ein-Bit-Transpondern“ erfolgt die Kommunikation durch schnelles Verändern der Arbeitsfrequenz in einem eingestellten Toleranzbereich (Wobbeln), um dadurch trotz unterschiedlichster und ungünstiger Resonanzverhältnisse der einzelnen RFID-Marken eine möglichst hohe Erkennungsgenauigkeit zu erzielen.²³⁴

2.2.3.2 Kapazitiv gekoppelte RFID-Systeme

Das Verfahren der kapazitiven Kopplung beruht auf dem Plattenkondensator-Prinzip, bei dem die Signalübertragung zwischen zwei voneinander isolierten, elektrischen Leitern erfolgt, die sowohl in der RFID-Marke, als auch im Lesegerät parallel angeordnet sind.²³⁵ Eine Datenübertragung lässt sich dadurch bewerkstelligen, dass ein elektrisches Signal eine Ladungsveränderung auf einem Leiter hervorruft und diese sich über das elektrische Feld auf die Ladungsträger des zweiten Leiters auswirkt. Da die so erzeugte Koppelkapazität verhältnismä-

²³¹ Rankl/Effing 2002, 923.

²³² Umgangssprachlich als Wireless Local Area Network (WLAN) bekannt. Es basiert in der Regel auf dem 1999 verabschiedeten Standard des IEEE (Institute of Electrical and Electronics Engineers) mit der Referenznummer 802.11.

²³³ Oertel u.a. 2004, 27.

²³⁴ Schoblick 2005, 130; Finkenzeller 2006, 33.

²³⁵ Finkenzeller 2006, 54; Schoblick 2005, 79.

ßig gering ist, bedarf es für den Betrieb von Mikroprozessoren einer ergänzenden Energieversorgung, etwa durch Induktion.²³⁶

2.2.3.3 Induktiv gekoppelte RFID-Systeme

Induktiv gekoppelte Systeme nutzen das Prinzip der elektromagnetischen Induktion aus. Hierüber erfolgen die Energieversorgung der RFID-Marken und der Datenaustausch mit ihnen. Da die Energieversorgung solcher RFID-Marken meist passiv ist, muss das RFID-Lesegerät über seine Antenne ein starkes elektromagnetisches Feld abstrahlen.²³⁷ Ein Teil des Lesegerätfeldes durchdringt die Antennenspule der RFID-Marke. Dadurch wird dort eine Spannung induziert. Diese wird gleichgerichtet.²³⁸ Da sowohl im RFID-Lesegerät als auch in der RFID-Marke in der jeweiligen Antennenspule ein Kondensator zugeschaltet wird, entsteht in beiden Komponenten ein Resonanzschwingkreis. Mit der Kapazität des Kondensators und der Spuleninduktivität der Antennenspule im Lesegerät wird ein Parallelschwingkreis gebildet, dessen Resonanzfrequenz der Sendefrequenz des Lesegerätes entspricht. Auf diese ist ebenso der Schwingkreis in der RFID-Marke abgestimmt.²³⁹

2.2.3.4 Lastmodulation mit und ohne Hilfsträger

Daten können im Rahmen der Kommunikation zwischen RFID-Marke und Lesegerät mit Hilfe von Lastmodulation übertragen werden.²⁴⁰ Eine im Ansprechbereich des Lesegeräts befindliche resonante RFID-Marke entzieht dem vom Lesegerät erzeugten elektromagnetischen Feld Energie. Die dadurch bewirkte Rückkopplung der RFID-Marke auf das Lesegerät lässt sich als „transformierte Impedanz“ in der Antennenspule des Lesegerätes beschreiben.²⁴¹ Durch das Zuschalten eines Lastwiderstandes in der RFID-Marke wird diese transformierte Impedanz beeinflusst und verändert die Spannung an der Antenne des Lesegeräts.²⁴² Um Daten zu übertragen, die sich an der Antenne als verschiedene Spannungszustände darstellen, wird der Lastwiderstand entsprechend geschaltet. Durch Gleichrichtung der an der Antenne abgegriffenen Spannung können die Daten zurück gewonnen werden.²⁴³

Für die Datenübertragung ist es möglich, entweder direkt die Resonanzfrequenz zu nutzen (Lastmodulation ohne Hilfsträger) oder das Datensignal auf einen Hilfsträger aufzumodulieren (Lastmodulation mit Hilfsträger). Bei letzterem Übertragungsverfahren wird vom Lesegerät neben dem eigentlichen Takt- oder

²³⁶ Rankl/Effing 2002, 99.

²³⁷ Schoblick 2005, 121; Rankl/Effing 2002, 96; Finkenzeller 2006, 44.

²³⁸ Finkenzeller 2006, 44; Rankl/Effing 2002, 96.

²³⁹ Rankl/Effing 2002, 96; Finkenzeller 2006, 44.

²⁴⁰ Rankl/Effing 2002, 97.

²⁴¹ Finkenzeller 2006, 47; Rankl/Effing 2002, 97.

²⁴² Finkenzeller 2006, 47; Rankl/Effing 2002, 97.

²⁴³ Finkenzeller 2006, 47 f.; Rankl/Effing 2002, 97 f.; Oertel u.a. 2004, 14.

Trägersignal in geringem Frequenzabstand ein zusätzliches Taktsignal (auch Hilfsträger genannt) ausgesandt.²⁴⁴ In der Praxis kommt die Lastmodulation mit Hilfsträger oft zum Einsatz, um eine Überdeckung des Antwortsignals der RFID-Marke durch das Sendesignal des Lesegeräts zu vermeiden, weil die Signalstärke des Antwortsignals um Zehnerpotenzen schwächer ist als das Sendesignal.²⁴⁵

2.2.3.5 RFID-Systeme im Rückstreuverfahren

Das Rückstreuverfahren wird verwendet, um größere Entfernungen zu überbrücken. Man macht sich hierbei die, aus der Funkmesstechnik bekannte, Eigenschaft zu Nutze, dass elektromagnetische Wellen reflektiert werden, wenn die Ausdehnung des von ihnen getroffenen Körpers größer ist als die halbe Wellenlänge der ausgesandten elektromagnetischen Welle. Die Reflexionseigenschaft von Objekten, auf die die Front der elektromagnetischen Wellen treffen, verbessert sich, wenn das Objekt in Resonanzschwingung gerät.²⁴⁶ Mit Hilfe einer Dipolantenne sowohl an dem Lesegerät als auch an der RFID-Marke, die so dimensioniert ist, dass sie für die jeweils verwendete Frequenz ein Resonanzverhalten zeigt, lässt sich dieser Effekt erzeugen.²⁴⁷

Die von der Antenne des Lesegeräts abgestrahlte Sendeleistung dient auch der Energieversorgung der RFID-Marke. Zu diesem Zweck wird die an den Anschlüssen der Antenne der RFID-Marke anliegende Hochfrequenzspannung gleichgerichtet.²⁴⁸ Da ein Teil der vom Lesegerät ausgestrahlten Energie von der RFID-Marke wieder reflektiert wird, steht nicht die gesamte an der Antenne auftreffende Leistung zur Energiegewinnung zur Verfügung. Der Anteil der reflektierten Energie lässt sich durch die Antenneneigenschaften beeinflussen. Eine gebräuchliche Antennenform ist die Dipolantenne. Daneben kommen weitere Formen wie die Yagi-Uda-Antenne, die Patch- oder Mikrostripantenne sowie die Schlitzantenne zum Einsatz.²⁴⁹

Eine Datenübertragung zwischen der RFID-Marke und dem Lesegerät kann mit dem Verfahren des „modulierten Rückstrahlquerschnitts“ (Modulated Backscatter) durchgeführt werden.²⁵⁰ Ähnlich wie bei den induktiv gekoppelten RFID-Systemen wird ein Lastwiderstand parallel zur Dipolantenne im Takt des zu übertragenden Datenstroms ein- und ausgeschaltet, wodurch der Eingangswiderstand der RFID-Marke und somit der Rückstreuquerschnitt entsprechend verändert wird. Es entsteht ein amplitudenmoduliertes Signal, das über die Antenne des Lesegeräts empfangen werden kann. Mit dem Rückstreuverfahren

²⁴⁴ Rankl/Effing 2002, 98; Schoblick 2005, 136.

²⁴⁵ Finkenzeller 2006, 103; Rankl/Effing 2002, 98.

²⁴⁶ Oertel u.a. 2004, 33; Schoblick 2005, 138.

²⁴⁷ Oertel u.a. 2004, 14.

²⁴⁸ Oertel u.a. 2004, 33.

²⁴⁹ Schoblick 2005, 114 ff.; Finkenzeller 2006, 134, 136 f.; Sottriffer 2003, 32, 33.

²⁵⁰ Finkenzeller 2006, 151.

lässt sich zwischen Lesegerät und RFID-Marke ohne Stützbatterie eine Reichweite überbrücken, die bei der Sendefrequenz von 868 MHz bei ungefähr drei Metern und bei 2,45 GHz bei etwas über einem Meter liegt.²⁵¹

2.2.4 Vielfachzugriffsverfahren

Vielfachzugriffsverfahren kommen immer dann zur Anwendung, wenn mehrere Teilnehmer zeitgleich auf dasselbe Medium zugreifen wollen. Beim Einsatz von RFID-Systemen ergibt sich eine besondere Herausforderung, wenn sich mehrere RFID-Marken zeitgleich im Ansprechbereich desselben Lesegeräts befinden und gleichzeitig versuchen, ihre Identifikationsnummer an das Lesegerät zu übermitteln.

Da alle RFID-Marken eines bestimmten Typs oder derselben Anwendung im selben Frequenzbereich senden, überlagern sich deren Signale und das Lesegerät vermag keine der RFID-Marken zu identifizieren. Um eine solche Kollision zu verhindern, muss ein Lesegerät mit Hilfe von Selektionsverfahren erreichen, dass Signale der RFID-Marken getrennt verarbeitet werden können. Als Selektionsverfahren können verschiedene Vielfachzugriffs- oder Multiplex-Verfahren eingesetzt werden, die durch Aufteilung des Raumes, der Zeit, des Frequenzbereiches oder durch unterschiedliche Codierung eine Übertragung ohne gegenseitige Störung ermöglichen.²⁵²

Bei RFID-Systemen werden am häufigsten Antikollisionsprotokolle als Vielfachzugriffsverfahren verwendet, die nach dem Zeitmultiplex²⁵³-Prinzip arbeiten.²⁵⁴ Dabei lässt sich die Selektion entweder von der RFID-Marke oder vom Lesegerät aus steuern. Verfahren, die vom Lesegerät kontrolliert werden, sind im Vergleich zu RFID-Marken gesteuerten grundsätzlich schneller, da das Lesegerät seine Anfrage (Request) nicht wiederholen muss, bis alle RFID-Marken mit hinreichender Wahrscheinlichkeit selektiert sind.²⁵⁵ In der Praxis haben derzeit das durch die RFID-Marken gesteuerte Antikollisionsprotokoll „Aloha“, das ausschließlich bei Festwertspeicher-RFID-Marken verwendet wird,²⁵⁶ sowie das durch das Lesegerät gesteuerte Antikollisionsprotokoll „Suchbaum“, auch „Tree-Walking“ oder „Binary-Search“ genannt, Bedeutung erlangt.²⁵⁷

²⁵¹ Oertel, u.a. 2004, 33.

²⁵² Finkenzeller 2006, 213 ff., 215; Rankl/Effing 2002, 99; Heinrich 2005, 79 f.

²⁵³ Time Domain Multiple Access (TDMA).

²⁵⁴ Oertel u.a. 2004, 16; Rankl/Effing 2002, 100; Finkenzeller 2006, 218.

²⁵⁵ Oertel u.a. 2004, 35.

²⁵⁶ Finkenzeller 2006, 220.

²⁵⁷ Finkenzeller 2006, 226.

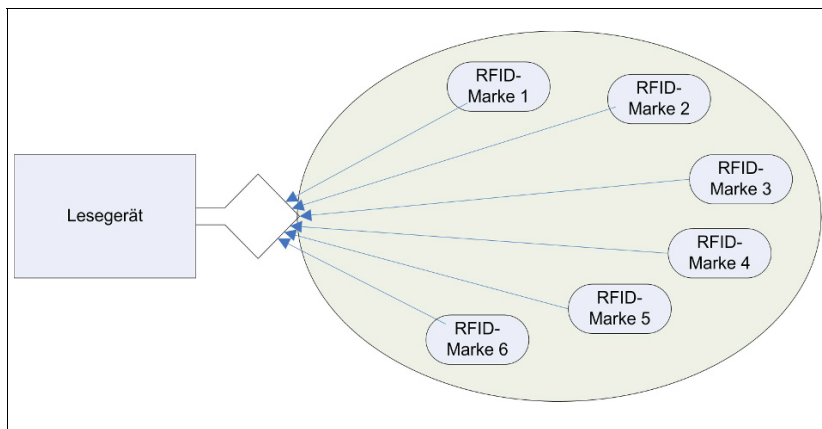


Abbildung 6: Vielfachzugriff von RFID-Marken im Ansprechbereich eines RFID-Lesegerätes²⁵⁸

2.2.4.1 Aloha, Slotted Aloha und Dynamisches Aloha-Verfahren

Das Antikollisionsprotokoll Aloha²⁵⁹ stellt ein einfaches Vielfachzugriffsverfahren dar und beruht auf einer probabilistischen Abfrage der Identifikationsnummer aller im Ansprechbereich befindlichen RFID-Marken. Nach einer Anfrage des Lesegeräts sendet jede RFID-Marke ihre vollständige Identifikationsnummer zu einem von ihm zufällig gewählten Zeitpunkt innerhalb des Anfrageintervalls an das Lesegerät. Da die Übertragung des Datenpaketes oder Datenblocks (Frame) der RFID-Marke, das die Identifikationsnummer enthält, im Verhältnis zum Anfrageintervall kurz ist, besteht bei einer begrenzten Anzahl von RFID-Marken eine hohe Wahrscheinlichkeit, dass alle RFID-Marken nach mehrfachem Durchlaufen der Anfragezyklen mindestens einmal ihre Identifikationsnummer kollisionsfrei senden konnten.²⁶⁰

Um den Datendurchsatz zu verbessern, sind auf dem Aloha-Verfahren basierend, abgewandelte Protokolle, wie das Slotted Aloha (S-Aloha) und das Dynamische Slotted Aloha (Dynamische S-Aloha) entwickelt worden. Bei dem Slotted Aloha stehen innerhalb eines Anfrageintervalls definierte Zeitschlitze zur Verfügung, in denen die RFID-Marken nach einer synchronisierenden Anfrage des Lesegeräts in der gleichen Weise wie beim Aloha-Protokoll zufallsgesteuert

²⁵⁸ Nach Finkenzeller 2002, 205.

²⁵⁹ 1971 wurde das Alohanet – ein Funknetz zur Datenverarbeitung – entwickelt. Es verband die Inseln um Hawaii mit der Universität Honolulu und Hawaii – s. Finkenzeller 2006, 220.

²⁶⁰ Oertel u.a. 2004, 35; Lampel/Flörkemeier/Haller 2005, 77; Sottriffer 2003, 44; Finkenzeller 2006, 286.

senden.²⁶¹ Um zusätzlich Anfragezyklen zu verringern, werden in weiteren Protokollvarianten die bereits selektierten RFID-Marken stumm geschaltet, die dadurch in nachfolgenden Anfrageintervallen keine (unnötigen) Kollisionen erzeugen können.²⁶²

2.2.4.2 Suchbaum-, auch Tree-Walking- oder Binary-Search-Verfahren

Im Gegensatz zum Aloha-Verfahren führt das Suchbaum-, auch Tree-Walking- oder Binary-Search-Verfahren eine deterministische Suche durch den Adressraum²⁶³ durch, der sich durch die möglichen Identifikationsnummern der RFID-Marken ergibt. Nach einer synchronisierenden Anfrage des Lesegeräts, fragt es die Identifikationsnummern der im Ansprechbereich befindlichen RFID-Marken, beginnend beim höchstwertigen Bit ab. Sobald bei der absteigenden Suchabfrage an einer Stelle der Identifikationsnummer die RFID-Marken ein Bit mit unterschiedlichem Binärwert senden, kommt es zu einer Kollision in der Übertragung. An dieser Stelle wird die Suchabfrage durch das Lesegerät mit einem nunmehr von ihm gewählten Binärwert fortgesetzt. Ähnlich eines binären Suchbaums werden an den Stellen der Identifikationsnummer, an denen eine Kollision aufgetreten ist, die sich ergebenden Verzweigungen weiterverfolgt. RFID-Marken, die während der Suchabfrage eindeutig selektiert wurden, werden mit einem Abwahl-Befehl (Unselect Command) stumm geschaltet, um die weitere Suchabfrage nicht zu stören.²⁶⁴ Mit diesem Protokoll lässt sich eine sehr große Anzahl von RFID-Marken im Ansprechbereich eines Lesegeräts bearbeiten.

2.2.4.3 Kooperative Übertragungsverfahren

Zu den Vielfachzugriffsverfahren sind ergänzende Protokolle entwickelt worden, die nachteilige Begleiterscheinungen der eingesetzten Zugriffsverfahren, wie verhältnismäßig lange Abfragezeiten oder Signaldämpfungsprobleme zu vermeiden suchen. Bei einer Menge von RFID-Marken im Rahmen einer Pulkabfrage ist es interessant, schnell zu erfahren, wie groß der Anteil der RFID-Marken mit einem bestimmten Schwellwert²⁶⁵ ist. Die Verwendung eines kooperativen Übertragungsverfahrens (Cooperative Transmission), wie das Protokoll zur überlagerten, probabilistischen Datenübertragung (Synchronous Distributed

²⁶¹ Finkenzeller 2006, 222; Rankl/Effing 2005, 736 f. Ein Problem entsteht, wenn mehr RFID-Marken im Ansprechbereich des Lesegeräts als Zeitschlitzzeilen vorhanden sind. Daher arbeitet das dynamische Slotted ALOHA nicht mit drei sondern mit einer dynamischen Anzahl von Zeitschlitzzeilen. Diese werden vom Lesegerät entweder bei vorgegebener Anzahl gesperrt, sobald eine RFID-Marke erkannt wurde oder deren Anzahl wird solange dynamisch erhöht bis eine Marke selektiert wurde – s. Finkenzeller 2006, 225.

²⁶² Lampe/Flörkemeier/Haller 2005, 77.

²⁶³ Für die Bitdarstellung wird bei diesem Algorithmus die Manchester-Codierung verwendet – s. Finkenzeller 2006, 226; Sottriffer 2003, 40.

²⁶⁴ Finkenzeller 2006, 228 ff.; Rankl/Effing 2002, 116.

²⁶⁵ Dabei könnte der Schwellwert ein überschrittenes Mindesthaltbarkeitsdatum einer Produktmenge sein.

Jam Signalling [SDJS]) ermöglicht eine Parallelübertragung durch Signalüberlagerung im Kanal und lässt eine Abschätzung der Schwellwertverteilung in der Gesamtmenge ohne direkten Zugriff auf die einzelnen RFID-Marken zu.²⁶⁶

2.2.5 Bauformen und Produktionsverfahren

2.2.5.1 Bauformen der RFID-Komponenten

So vielfältig wie die Einsatzmöglichkeiten, so vielfältig sind auch die Bauformen der RFID-Marken und Lesegeräte. Bei den Lesegeräten gibt es stationäre, die beispielsweise in Form von Kartenlesern an Zugangskontrollsystemen oder in Form von Schleusen an Produktionsstraßen oder an großen Toren der Logistikeinrichtungen aufgestellt sein können.²⁶⁷ Es sind aber auch portable Ausführungen erhältlich, die beispielsweise im Mobilfunkendgerät oder als Handterminal mit Schnittstelle zu einem Drahtlosnetzwerk (wie nach IEEE 802.11-Standard) Verwendung finden.²⁶⁸

RFID-Marken werden je nach Anwendung in unterschiedlichen Größen und auf verschiedenen Trägermaterialien angeboten. Für den Logistikbereich können RFID-Marken beispielsweise zur Kennzeichnung von Produktverpackungen, Paketen, Paletten oder Fluggepäck verwendet werden, die als Funketiketten oder als sogenannte „Smart Label“ auf Papier, Pappe oder Kunststoffolie aufgebracht oder eingebettet sind. Hingegen werden großformatige RFID-Marken für Container- oder Waggonlogistikaufgaben eingesetzt, um größere Lesereichweiten zu erzielen.²⁶⁹ Für Anwendungen mit besonders großen Sicherheitsanforderungen, wie elektronische Wegfahrsperre oder Türschließsysteme werden RFID-Marken – eingebettet in einer Kunststoffhülle (Plasticpackage [PP]) – im mechanischen Schlüssel integriert.²⁷⁰

Zur Identifikation von Tieren verwendet man vorzugsweise RFID-Marken im Glaszylinder, die dem Tier unter die Haut gespritzt werden.²⁷¹ Um gegen Hitze, Feuchtigkeit- oder Chemikalieneinwirkungen beispielsweise in industriellen Fertigungsprozessen widerstandsfähig zu sein, werden Transponder von Metallkapseln umschlossen. Marken in metallischer Bauform müssen speziell konstruiert sein, etwa mit einem Schlitz, um funktechnisch nicht abgeschirmt zu werden.²⁷² Ebenso stehen in Kunststoff eingebettete RFID-Marken im Scheck-

²⁶⁶ Krohn/Zimmer/Beigl/Decker, 3rd International Conference on Pervasive Computing 2005 – s. auch <http://www.teco.edu/~krohn/collaborative.pdf>; Krohn/Beigl/Wendhack, 12th IEEE International Conference on Network Protocols (ICNP) 2004 – s. <http://www.teco.edu/~krohn/sdjs.pdf>.

²⁶⁷ Finkenzeller 2006, 372 f.; Mattern, in: Taeger/Wiebe 2005, 9; Sottriffer 2003, 42.

²⁶⁸ Schoblick 2005, 169; Finkenzeller 2006, 372.

²⁶⁹ Finkenzeller 2006, 391; Oertel u.a. 2004, 88.

²⁷⁰ Schoblick 2005, 152 ff.; Finkenzeller 2006, 15.

²⁷¹ Finkenzeller 2006, 14; Schoblick 2005, 157.

²⁷² Sottriffer 2003, 42; Finkenzeller 2006, 16; Rietzler, in: Hansen 1999, 49.

kartenformat²⁷³ zur Verfügung, die beispielsweise zur Zugangskontrolle als Berechtigungs- oder Eintrittskarten sowie zur Dienstabwicklung als Kunden, Service- oder Bonuskarten Anwendung finden.²⁷⁴

Bei der Produktion von RFID-Systemen sind die Hersteller bemüht, Produktionsverfahren weiterzuentwickeln, die eine großtechnische Serienfertigung erlauben, die Zuverlässigkeit verbessern und vor allem Herstellungskosten optimieren helfen. Hier sind noch weitere Fortschritte und Innovationen zu erwarten. Die Optimierung betrifft vornehmlich die Herstellung der RFID-Marken, da bei massenhaftem Einsatz deren Produktionsaufwand ein wesentlicher Kostenfaktor für die aufzubauende Infrastruktur darstellt.

2.2.5.2 Produktionsverfahren der RFID-Komponenten

Eine RFID-Marke besteht aus dem elektronischen Datenträger und ihrem funktionell gestalteten Gehäuse. Die einzelnen Bauteile des elektronischen Datenträgers, werden mit Verfahren der Halbleitertechnik²⁷⁵ produziert und zum sogenannten „Transponderhalbzeug“²⁷⁶ verbaut. Das Transponderhalbzeug muss zum Schutz und Anbringen an einen Gegenstand in ein Gehäuse gekapselt werden. Dies kann durch Spritzgießen, Vergießen, Verkleben oder durch Einsetzen in einen Glaszylinder erfolgen.²⁷⁷ Die insbesondere für induktiv gekoppelte RFID-Systeme wichtige Antennenspule kann mittels Wickeltechnik, Verlegetechnik, Siebdrucktechnik²⁷⁸ oder Ätztechnik auf den Träger aufgebracht werden. Schwierigkeiten bereitet noch die Verbindung des Chips mit den Antennenanschlüssen, da zum einen die Verbindung in einem eigenen Prozessschritt vorgenommen werden muss und zum anderen hierin eine erhöhte Fehleranfälligkeit liegt. Daher entfällt derzeit gerade bei den einfacheren RFID-Marken ein großer Anteil der Herstellungskosten auf den Verbindungsprozess.

Verwendung finden verschiedene Verbindungstechniken. Für Antennenspulen aus Drähten kommen Löt- und Schweiß-Techniken, für Spulen auf Polymer-Dickfilmpasten-Basis Flip-Chip-Technologien²⁷⁹ oder Schneid-Klemm-Techno-

²⁷³ Chipkarten im ID 1 Format mit den Maßen: 85,72 mm x 54,03 mm x 0,76 mm nach ISO 7810.

²⁷⁴ Finkenzeller 2006, 18; Sottriffer 2003, 43.

²⁷⁵ Die Strukturen werden fototechnisch auf eine Siliziumscheibe (Wafer) als Systemträger aufgebracht. Nach Tests wird die sogenannte Gutware auf Module fixiert und die elektrische Verbindung zu den Kontaktflächen hergestellt (Bonden des Chips). Dieser Chip wird mit einer Vergussmasse, gewöhnlich Epoxidharz vergossen, um den Chip vor Umwelteinflüssen zu schützen – s. Rank/Effing 2002, 613 ff.; Finkenzeller 2006, 377 ff.

²⁷⁶ Hierunter wird eine ungehäute RFID-Marke verstanden.

²⁷⁷ Finkenzeller 2006, 380.

²⁷⁸ Verwendung von Polymer-Dickfilmpasten (Polymer Thick Film - PTF), die durch ein mit Druckmasken belegtes Sieb auf das Trägermaterial gedrückt werden – s. Finkenzeller 2006, 383.

²⁷⁹ Die Fixierung und Kontaktierung des ungehäuten Chips erfolgt durch einen leitfähigen Kleber – s. Finkenzeller 2006, 384.

logien²⁸⁰ und für geätzte Spulen mit Chipmodulen überwiegend Aufschmelz- bzw. Reflow-Lötverfahren²⁸¹ zum Einsatz.

Herstellungstechnik	Beschreibung	Anwendungsbereich	Verbindungstechnik	Produktionsaufwand
Wickeltechnik	Herstellung der Antennenspule mittels herkömmlichem Wickelwerkzeug und Fixierung auf Trägermaterial durch Backlack	niederfrequente RFID-Marken wegen der Vielzahl der benötigten Windungen	Löten- und Schweißen	hoch
Verlegetechnik	Feiner Draht wird mittels Ultraschall auf das Trägermaterial (PVC-Folie) aufgebracht und mit diesem verschmolzen	gewinnt an Bedeutung	Punktschweißverfahren	niedrig
Siebdrucktechnik	Mit einer elektrisch leitfähigen Farbe werden auf eine Inlettfolie ²⁸² die Windungen einer Spule gedruckt	Wegen der breiten Leiterbahnführung ist die Windungszahl begrenzt. Nur für Anwendungen >8 MHz geeignet. Für vornehmlich 1-Bit-RFID-Marken und nur-Lese-Marken, Smart Label 13,56 MHz	Flip-Chip-Technologie oder Schneid-Klemm-Technologie (Cut Clamp Technology CCT), da wegen Material nicht lötbar	niedrig
Ätztechnik	Schaltkreise werden im fototechnischen Verfahren auf Kupferfolie aufgeätzt		Reflow-Lötverfahren	niedrig

Tabelle 5: Herstellungstechniken von RFID-Marken

RFID-Marken, die als Kundenkarten Verwendung finden, werden als Plastikkarte im Format einer Scheckkarte produziert, bei der das Transponderhalbzeug

²⁸⁰ Mit der Schneid-Klemm-Technologie (Cut Clamp Technologie [CCT]) wird das Chipmodul auf das Trägermaterial befestigt und so mit der Antenne kontaktiert – s. *Finkenzeller* 2006, 385.

²⁸¹ Lötpaste wird an die Fügestellen aufgebracht. Wenn die zugeführte Wärme die Schmelztemperatur überschreitet, wird die Paste flüssig und benetzt die zu lötende Anschlussoberfläche – s. *Finkenzeller* 2006, 386.

²⁸² Inlettfolie befindet sich zwischen zwei Deckfolien - s. *Rankl/Effing* 2002, 926.

zwischen Kunststofffolien gepresst wird. Für RFID-Marken, die in Verpackungs- oder Ummantelungsmaterialien von Gegenständen eingebettet werden sollen, ist die neuere Siebdrucktechnik interessant. Dadurch lassen sich Antennen auf dünne und biegsame Folien mit den gleichen Druckmaschinen aufbringen, mit denen bisher ebenso das Verpackungs- oder Ummantelungsmaterial bedruckt wurde. Für den aufwendigen Schritt, das Mikrochipmodul auf der Antennenfolie zu fixieren (derzeit mittels Schneid-Klemm-Techniken), wird für die großtechnische Serienfertigung noch an effizienteren Verfahren gearbeitet.²⁸³

2.2.6 Normungsstandards

Eine Standardisierung der technischen Parameter ist für den überbetrieblichen und überregionalen Einsatz von LuK-Techniken besonders wichtig.²⁸⁴ Die Standardisierung und Normierung von RFID-Komponenten wurde durch eigene ökonomische Interessen der beteiligten Staaten und Industriekonzerne erschwert.²⁸⁵ Die für Normierung zuständigen nationalen und internationalen Gremien vereinheitlichten bislang vor allem Standards für Kommunikationsschnittstellen und -protokolle und Grenzwerte hinsichtlich der elektromagnetischen Verträglichkeit für die verbreitetsten RFID-Systeme.

2.2.6.1 Normungsstandards Spezifikation

Für RFID-Systeme haben sich verschiedene Industriestandards etabliert, wobei heute die sogenannte ISO/IEC-Kompatibilität maßgeblich ist. Daneben existiert eine Reihe von nicht frei zugänglichen Spezifikationen als proprietäre Branchenlösungen.²⁸⁶

Durch die weltweit führende „International Organization for Standardization“ (ISO), gemeinschaftlich mit der „International Electrotechnical Commission“ (IEC) und dem „Joint Technical Committee 1“ (JTC1) sind Standards für RFID-Systeme erarbeitet worden, die die zu verwendenden Kommunikationsfrequenzen, Übertragungsverfahren, Übertragungsgeschwindigkeiten, Energieversorgung, Kommunikationsprotokolle und Codierungen regeln.²⁸⁷

Eine parallel laufende Standardisierungsorganisation ist EPCglobal, eine von der Industrievereinigung GS1(Global Standards One) getragene nicht gewinnorientierte Organisation. Ihr Schwerpunkt konzentriert sich auf eine schnelle

²⁸³ Ergebnis der Diskussion mit dem Leiter der Entwicklungsabteilung Dr. Martin Werner der Firma Alcan Packaging Singen GmbH auf der internationalen Konferenz „Smart Labels Europe“ in Nizza, 12.10.2004.

²⁸⁴ Oertel u.a. 2004, 27.

²⁸⁵ Sottriffel 2003, 44.

²⁸⁶ Beispielsweise gibt es im Bereich der Luftfahrtindustrie von Airbus Bemühungen, RFID-Systeme und Anwendungen zu harmonisieren, um nicht nur Lösungen einsetzen zu können, die branchenspezifischen Bedürfnissen Rechnung tragen, sondern auch über ihre Marktmacht allgemeine Industriestandards durchzusetzen.

²⁸⁷ Lampe/Flörkemeier/Haller 2005, 82 f.

Etablierung von Standards vor allem für die Konsumgüterbranche großer Einzelhandels- und Logistikunternehmen.²⁸⁸

ISO RFID-Standards werden in vier Kategorien unterteilt: Luftschnittstelle, Testmethoden, Datenprotokolle und Anwendungsstandards. Zu den wichtigen ISO/IEC-Standards gehören die ISO/IEC 10536, 15693, 14443, 18000 und 15961 bis 15963. Induktiv gekoppelte RFID-Systeme werden vor allem durch die Standards 14443, 15693 und 10373 beschrieben. Die ISO/IEC 14443 ("Identification cards – Contactless Integrated Circuit(s) Cards – Proximity Cards") legt Funktionsweise und Betriebsparameter der Proximity-Coupling-Systeme fest.²⁸⁹ Sie regelt unter anderem die mechanischen Eigenschaften²⁹⁰ sowie Parameter der Kommunikationsschnittstelle²⁹¹ und der Kommunikationsverfahren²⁹².

Die ISO/IEC 15693 („Identification Cards – Contactless Integrated Circuit(s) Cards – Vicinity Cards“) betrifft die „Vicinity-Coupling-Systeme“.²⁹³ Sie normiert vergleichbar zur ISO/IEC 14443 die mechanischen Eigenschaften²⁹⁴ sowie Parameter der Luftschnittstelle²⁹⁵ und der Kommunikationsverfahren²⁹⁶.

Eng gekoppelte RFID-Systeme oder auch Close-Coupling-Systeme werden von der ISO/IEC 10536 („Identification Cards – Contactless Integrated Circuit(s) Cards“) spezifiziert.²⁹⁷ Sie definiert unter anderem – ähnlich im Aufbau wie die genannten ISO-Standards – physikalisch mechanische Eigenschaften,²⁹⁸ Abmessungen und Lage der Koppellemente²⁹⁹ sowie Parameter der elektronischen Signalübertragung und der Rücksetzabläufe.³⁰⁰

²⁸⁸ BT-Drs. 17/405, 49. EPCglobal wurde im September 2011 in den Global Standards Management Prozess (GSMP) eingegliedert.

²⁸⁹ Rankl/Effing 2002, 107 ff.; Finkenzeller 2006, 270 ff.

²⁹⁰ ISO/IEC 14443 Part 1 mit Abmessung, Hinweise für Biege- und Torsionseigenschaften, Grenzwerte für Belastung durch elektrische und magnetische Wechselfelder (entsprechend ISO/IEC 7810).

²⁹¹ ISO/IEC 14443 Part 2 mit Parameter für Energie- und Signalübertragung, Ansprechfeldstärke und Grenzwerte des magnetischen Wechselfeldes. Kommunikationsschnittstelle existiert.

²⁹² ISO/IEC 14443 Part 3 mit Vorgaben für den Aufbau des Protokollrahmens und das Vielfachzugriffs- oder Antikollisionsverfahren. Genormt werden zwei unterschiedliche Typen von RFID-Marken (Typ A und Typ B).

²⁹³ Rankl/Effing 2002, 151; Finkenzeller 2006, 287 ff.

²⁹⁴ ISO/IEC 15693 Part 1 mit mechanischen und physikalischen Parametern (entsprechend ISO 7810).

²⁹⁵ ISO/IEC 15693 Part 2 mit Parameter für Sendefrequenz, der Energieversorgung durch das Lesegerät sowie Grenzwerte für das magnetische Wechselfeld.

²⁹⁶ ISO/IEC 15693 Part 3 mit Vorgaben für das Übertragungs- und Antikollisionsprotokoll.

²⁹⁷ Rankl/Effing 2002, 101 ff.; Finkenzeller 2006, 268 ff.

²⁹⁸ ISO/IEC 10536 Part 1 (entsprechend 7860).

²⁹⁹ ISO/IEC 10536 Part 2.

³⁰⁰ ISO/IEC 10536 Part 3 mit Vorgaben für Energieversorgung, für die Modulationsverfahren der kapazitiven und induktiven Kopplung für die Datenübertragung vom und zum Lesegerät.

In der ISO/IEC 10373 („Identification Cards – Test Methods“) sind zur besseren Übersicht alle Testverfahren, sowohl für kontaktbehaftete als auch für kontaktlose Chipkarten, zusammengefasst.³⁰¹ Für RFID-Marken finden sich in Part 4 für eng gekoppelte und in Part 6 und 7 für fern gekoppelte Systeme dieser ISO/IEC-Norm Vorgaben zur Prüfung allgemeiner Qualitätsmerkmale (z.B. Entflammbarkeit, Chemikalien- oder UV-Lichtbeständigkeit, Biegesteifigkeit) und der Konformität zu den spezifizierten Parametern der Kommunikationsschnittstelle (z.B. Amplitude der Lastmodulation, vom Lesegerät generierte Feldstärke, das Ein- und Ausschwingverhalten des vom Lesegerät erzeugten Signals) und Datenübertragung.³⁰²

Die ISO/IEC 18000 Part 1, 2, 3, 4, 6 und 7 legen Parameter für die Luftschnittstelle aller RFID-Systeme fest.³⁰³ Sie geben Hinweise zu Referenzarchitekturen und Definitionen der zu standardisierenden Parameter.³⁰⁴ Des Weiteren werden Parameter der Luftschnittstelle für RFID-Systeme mit einer Kommunikationsfrequenz unterhalb von 135 kHz,³⁰⁵ mit einer Kommunikationsfrequenz von 13,56 MHz,³⁰⁶ von 433 MHz,³⁰⁷ von 860 bis 960 MHz,³⁰⁸ geregelt. Weitere Spezifikationen enthalten die Standards ISO/IEC 15961 über die Schnittstelle zu den RFID-Anwendungen, ISO/IEC 15962 über Regeln für die Codierung und Speicherung der Daten sowie ISO/IEC 15963 zur Beschreibung der Identifikationsnummer.

Überarbeitungen der bereits existierenden RFID-Standards finden laufend statt. Die bedeutendste Erweiterung ist zurzeit im ISO-Standard 18000 Part 6 zu verzeichnen. Gegenüber früheren Standards bieten ISO/IEC 18000 Part 6-C und EPC Gen 2 eine schnellere Erfassung und eine erhöhte Erfassungssicherheit, indem mehrere Leseversuche gestartet werden können. Um den Forderungen der Datenschutzbeauftragten nachzukommen, ist in dem Protokoll ein Kill-Kommando vorgesehen. Es ermöglicht die Zerstörung der RFID-Marke.³⁰⁹

Seit 2012 existiert ein von dem Industrieverband AIM³¹⁰ entwickeltes RFID Emblem, das in dem Standard ISO/IEC 29160³¹¹ mit der Bezeichnung „Information Technology – Radio frequency identification for item management – RFID Emblem“ normiert wurde. Es dient der visuell wahrnehmbaren Kennzeichnung

³⁰¹ Rankl/Effing 2002, 151 f.; Finkenzeller 2006, 293 ff.

³⁰² Finkenzeller 2006, 268 ff.

³⁰³ Finkenzeller 2006, 302.

³⁰⁴ ISO/IEC 18000 Part 1.

³⁰⁵ ISO/IEC 18000 Part 2.

³⁰⁶ ISO/IEC 18000 Part 3.

³⁰⁷ ISO/IEC 18000 Part 7.

³⁰⁸ ISO/IEC 18000 Part 6.

³⁰⁹ S. Walk/Büth 2012, 98 ff.

³¹⁰ AIM-D e. V. ist der führende Industrieverband für Auto-ID, Datenerfassung und mobile Datenkommunikation. Der Verband fördert Auto-ID-Technologien und -Verfahren, RFID-Technologien sowie Barcode, Sensorik.

³¹¹ S. auch Abschnitt 4.5.2.3.3 und 4.5.2.3.4.

von RFID-Marken, RFID-Lesegeräten und mit RFID-Marken versehenen Objekten.

EPCglobal standardisiert mit „EPC Tag Data Standards (TDS)“ und „EPC Tag Data Translation (TDT)“ Vorgaben für die Speicherinformationen auf RFID-Marken. Daneben sind für Marken verschiedener Frequenzbereiche und Leistungsklassen Anforderungen hinsichtlich Aufbau und Funktionsweise definiert. Die zweite Generation des EPC-Standards, ist unter der Bezeichnung „EPC-Gen-2“³¹² bekannt. Die Spezifikation umfasst die Datenformate und die Kommunikation zwischen Marke und Lesegerät und arbeitet im 860 MHz - 960 MHz Frequenzbereich. Das erlaubt eine hohe Lesegeschwindigkeit (bis zu 600 RFID-Marken pro Sekunde). Ein implementiertes Kill-Kommando ermöglicht die endgültige Zerstörung der RFID-Marke. Abgelegte Daten können mit Hilfe eines Access Kennwortes gegen ungewolltes Überschreiben geschützt werden. Das Pendant zu Gen 2 ist der HF (13,56 MHz) Standard.³¹³ Er ist kompatibel zu ISO/IEC 15693 und 18000 Part 3 und bietet verbesserte Leistungsmerkmale hinsichtlich der Lesegeschwindigkeit.

Weitere EPC Standards:

Bezeichnung	Funktion
Reader Protocol	Schnittstelle zwischen Lesegerät und Middleware
Reader Management	Konfiguration und Überwachung individueller Lesegeräte
Application Level Event	Filterung und Sammlung ausgelesener RFID-Markendaten.
EPC EPCIS Informationsservice	Verfolgung von Produkten entlang der Lieferkette
Object Naming Service (ONS)	Lokalisierung von zusätzlichen mit dem elektronischen Produktcode verknüpften Daten und Services durch die Verwendung des Domain Name System

Tabelle 6: Weitere EPC Standards³¹⁴

2.2.6.2 Datenstruktur

Gemäß der ISO 15693/Part 3-Spezifikationen³¹⁵ werden bei konformen RFID-Marken 64 Bit für die individuelle Zuordnungsnummer (Unique Identifier [UID])

³¹² EPC Gen2 ist bekannt unter „Class 1 Generation 2 UHF Air Interface Protokoll Standard“.

³¹³ HF-Standard trägt den Titel „EPCTM Radio Frequency Identity Protocols, EPC Class 1 HF RFID Air Interface Protokoll for Communications at 13,56 MHz“.

³¹⁴ S. BT-Drs. 17/405, 51.

³¹⁵ V. 10.3.2000.

aufgewandt, wobei für die jeweilige Seriennummer 48 Bit und für die Herstelleridentifikation (gem. ISO/IEC 7816-6/AM1) 8 Bit zur Verfügung stehen. Die übrigen 8 Bit sind E0.

Daneben steht die Anwendungsidentifikation (Application Family Identifier [AFI]) zur Verfügung, die der Zuordnung zu bestimmten Kategorien von Anwendungen dienen soll, wie zum Beispiel der der Telekommunikation, des Transports oder der Logistik. Sie umfasst 1 Byte, das in zwei Blöcken organisiert ist. Die Anwendungsidentifikation (AFI) soll sicherstellen, dass auf eine allgemeine Anfrage des Lesegeräts mittels Melde-Befehl (Inventory Command) nur bestimmte RFID-Marken reagieren.

Informationen über die Speicherstruktur der Marke enthält die Datenspeicherstrukturkennung (Data Storage Format Identifier [DSFID]). Für diese ist 1 Byte reserviert. 2 Byte sind für Werte im Rahmen der Prüfsummenkontrolle (Cyclic Redundancy Check [CRC]) vorbehalten, mit deren Hilfe die Fehlererkennung beim Empfänger durchgeführt werden kann. Maximal kann die Marke über 256 Blöcke zu jeweils je maximal 256 Bits, somit über insgesamt 8 kBytes, verfügen.

Die seitens EPCglobal standardisierte Datenstruktur (gem. EPC Tag Data Standards³¹⁶) teilt den 64 oder 96 Bit umfassenden Speicher der Marke in einen Kopf (Header) und mehrere Wertfelder, die in einen optionalen Filterwert sowie ein Branchenkodierungsschema gegliedert sein können. Der Kopf oder Header definiert die Gesamtlänge und das Format der besagten übrigen Felder. Er hat eine variable Größe und ist mehrstufig aufgebaut. Seine Größe beträgt 2 oder 8 Bit. Die Aufgliederung des Branchenkodierungsschemas als Wertfelder ist abhängig von dem verwendeten Zuweisungssystem, das den Beteiligten bekannt ist. Als branchenspezifische Zuweisungssysteme kommen das „Serialized Global Trade Item Number“ (SGTIN), „Serial Shipping Container Code“ (SSCC), „Serialized Global Location Number“ (SGLN), „Global Returnable Asset Identifier“ (GRAI) oder „Global Individual Asset Identifier“ (GIAI) in Betracht. In diesem Zusammenhang wurde ein neuer allgemeiner Zuordnungsstandard, der GID-96, verabschiedet. Dieser gliedert die 96 Bit in 8 Bit für den Kopf bzw. Header, 28 Bit für die Allgemeine Identifikationsnummer, die von EPC an Unternehmen oder Organisationen vergeben wird, 24 Bit für die Objektklasse und 36 Bit für die Seriennummer.

2.2.6.3 Kenngrößen der RFID-Technik

Aus den Merkmalen der verschiedenartigen Frequenzbereiche ergeben sich signifikante Eigenschaften, die bei den RFID-Lösungen bedacht werden müssen. Es haben sich charakteristische Einsatzfelder entwickelt, die sich auch bei den RFID-Marken widerspiegeln

³¹⁶ Version 1.1, Rev. 1.24 v. 1.4.2004. S. oben.

Parameter	Niederfrequenz	Hochfrequenz	Ultrahochfrequenz	Mikrowelle
Leseabstand	bis 1,2 m	bis 1,2 m	bis 4 m	bis zu 15 m (in Einzelfällen bis zu 1km)
Lesegeschwindigkeit	langsam	je nach ISO-Standard ³¹⁷	schnell	sehr schnell (aktive Transponder)
Feuchtigkeit³¹⁸	kein Einfluss	kein Einfluss	großer Einfluss	großer Einfluss
Metall	großer Einfluss	großer Einfluss		
Ausrichtung des Transponders beim Auslesen	nicht nötig	nicht nötig	teilweise nötig	immer nötig
Weltweit akzeptierte 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, Plastikgehäuse-Transponder, Chipkarten, Smart Label	Smart Label, Industrie-Transponder	Smart Label, Industrie-Transponder	Großformatige Transponder
Verwendung	Zutritts- und Routenkontrolle, Verleihsysteme, Wegfahrsperren, Tier ID, Diebstahlsicherung	Ticketing, Asset Management, Behälter ID, Logistik, Tracking und Tracing, Pulk-Erfassung	Palettenerfassung, Container ID	Straßenmaut, Container ID

Tabelle 7: Kenngrößen der RFID Technologie³¹⁹

³¹⁷ Unter 1 s bis 5 s bei ISO 14443 (5 s für 32 kByte) mittel (0,5 m/s Vorbeibewegung bei ISO 15693)

³¹⁸ Der Einfluss von Metall und Flüssigkeit variiert je nach Produkt. Es werden RFID-Transponder angeboten, die den Einsatz nach Aussage der Hersteller im Niedrigfrequenzbereich erlauben.

³¹⁹ Erweiterte Darstellung der Tabelle in Anlehnung an *Ischebeck*, Funkschau 13/2004, 31 ff.

2.2.6.4 Entwicklungsperspektiven der RFID-Technologie

Der Markt für RFID-Systeme hat an Dynamik gewonnen. Die große Nachfrage der Industrie und die zunehmende Standardisierung und Normierung der Protokolle, Frequenzen, Haltbarkeit der gespeicherten Daten und Übertragungsverfahren führen zu jährlichen Zuwachsraten. Grundsätzlich lassen sich zwei Trends beobachten. Zum einen werden höhere Frequenzen verwendet, um größere Datenmengen über größere Reichweiten sicher zu übermitteln. Zum anderen werden RFID-Marken entwickelt, die preiswert in Produktverpackungen oder auf Gegenstände aufgebracht oder integriert werden können. Die Einführung der RFID-Technik in viele Bereiche der Wirtschaft gilt mittlerweile als unumkehrbar.³²⁰

2.2.7 Alternative Auto-ID-Verfahren

Alternativ zu der RFID-Technik werden von der Industrie weitere Auto-ID-Verfahren mit vergleichbaren Funktionseigenschaften entwickelt. Insbesondere für Bereiche, in denen der Einsatz der beschriebenen RFID-Technik nicht möglich ist oder an seine Grenzen stößt, werden alternative Techniksysteeme erprobt. Beispielhaft sollen die Systeme RuBee und Near Field Communication (NFC) sowie das sogenannte „Super-Label“ vorgestellt werden.

2.2.7.1 Auto-ID-Technik RuBee

RuBee wurde ursprünglich von der Firma Visible Assets, Inc. entwickelt mit finanzieller Beteiligung der japanischen Firma Epson Electronics. Das Institute of Electrical and Electronics Engineers (IEEE) hat 2009 den entsprechenden Standard vergeben.³²¹

Im Unterschied zur RFID-Technik verwendet die RuBee-Technik aktive Marken oder Etiketten, die magnetische Wellen aussenden. Die Spezifikation beschreibt diesen neuen Standard als bidirektionales Verfahren, das auf Anfrage (On-Demand) Verbindungen erlaubt, dabei auf Frequenzen unterhalb 450 kHz operiert und eine Reichweite zwischen 0,5 und 30 Metern ermöglicht. Die Marken verbrauchen äußerst wenig Energie. Mit Hilfe einer kleinen Lithiumbatterie sollen sie fünf bis zehn Jahre funktionsfähig bleiben.³²² Nach Angaben des Hauptnutzers Visible Assets, Inc. lassen sich die Funktionen der Marke außerdem mit Sensoren sowie einem Mikroprozessor erweitern.³²³

Vorteil der RuBee-Technik ist vor allem ihre Robustheit. Marken und Etiketten können, anders als bei gängigen Bautypen von RFID-Marken, auch durch

³²⁰ Wiegink, in: Eberspächer/v. Reden 2006, 91.

³²¹ IEEE 1902.1-2009-IEEE Standard for Long Wavelength Wireless Network Protocol – s. <http://standards.ieee.org/findstds/standard/1902.1-2009.html>.

³²² S. Beschreibung zur IEEE RuBee Working Group, abrufbar unter: <http://standards.ieee.org/develop/wg/RuBee.html>.

³²³ S. <http://www.rubee.com/page2/Hard/index.html>.

Metalle und Flüssigkeiten hindurch korrekt ausgelesen werden und arbeiten auch unter unwirtlichen Bedingungen.³²⁴ Andererseits erlaubt RuBee mit 10 Auslesevorgängen pro Sekunde wesentlich weniger Anfragezyklen und damit eine erheblich geringere Datenübertragungsrate (nur 300 bis 9.600 Bits pro Sekunde) als vergleichbare RFID-Systeme, die durchaus 200 Auslesevorgänge je Sekunde ermöglichen. RuBee-Marken können viele Signale gleichzeitig empfangen. Die RuBee-Technik unterstützt das Interesse der Wirtschaft an einer zuverlässigen Verfolgung von Produkten innerhalb der Warenwirtschaftskette, insbesondere von solchen, die Metall enthalten, wie z.B. Waffen oder Baumaschinen.³²⁵ Trotz ihrer Standardisierung hat die RuBee-Technik bislang zu keinem breiten Einsatz gefunden, sondern wird für die beschriebenen Spezialanwendungen verwendet.

2.2.7.2 Auto-ID-Technik NFC

Die Technik der Near Field Communication (NFC) weist ebenfalls wesentliche technische Unterschiede zu der RFID-Technik auf, auch wenn sich die Handhabung ähnlich darstellt. Die NFC-Technik ist eine Kombination aus Smartcard- und kontaktlosen Verbindungstechniken. Sie kommt in verschiedenen Varianten zum Einsatz.³²⁶

Einerseits kann die Kommunikation zwischen zwei aktiven Transmittern erfolgen (aktiv-aktive Lösung). Die aktiven Komponenten benötigen eine eigenständige Energieversorgung. Andererseits ist aber auch eine Kommunikation zwischen einem aktiven Transmitter und einer passiven RFID-Marke möglich (aktiv-passive Lösung). Die letztere Art der Verbindung ist nicht gegen Angriffe von Dritten (Abhören, Manipulation) geschützt. Sicherheitsfunktionen, wie sie etwa für Zahlungssysteme erforderlich sind, lassen sich nur über eine aktiv-aktive Verbindung realisieren.

Die Spezifikationen für NFC werden vom NFC-Forum, einer Industrievereinigung, festgelegt und sind sehr umfangreich.³²⁷ Wie sich daraus ergibt, kann die Hardware für NFC-Komponenten, wie die der RFID-Technik, sehr klein gebaut und beispielsweise in Mobiltelefone oder Kreditkarten integriert werden. Hauptanwendungen der NFC-Technik sollen Bezahlverfahren sein. Die Deutsche Telekom AG hat beispielsweise angekündigt, ein drahtloses, auf NFC basierendes Bezahlverfahren einführen zu wollen.³²⁸ Das „Touch&Travel“-System der Deutschen Bahn AG zur Abrechnung von Zugfahrten verwendet ebenfalls die NFC-Technik als eine der Möglichkeiten, um Start und Ende der Benutzung eines

³²⁴ S. <http://standards.ieee.org/develop/wg/RuBee.html>.

³²⁵ S. „Store 20/20“ Sensitive Item Stores Security and Visibility, abrufbar unter: <http://www.rubee.com/Store/>.

³²⁶ S. zum Folgenden den Überblick unter: http://de.wikipedia.org/wiki/Near_Field_Communication.

³²⁷ S. http://www.nfc-forum.org/specs/spec_list/.

³²⁸ S. <http://www.heise.de/newsticker/meldung/1630474.html>.

Verkehrsmittels zu signalisieren. Es genügt dann, das Smartphone an eine im Bahnhof angebrachte NFC-Marke zu halten.³²⁹

Weitere denkbare Anwendungsfelder sind papierlose Eintrittskarten oder andere Zugangskontrollen. Dabei können mittels der NFC-Technik zusätzlich persönliche Einstellungen an das Empfängersystem übertragen werden. Beispielsweise kann die IuK-Einheit des Automobilbesitzers (PDA, Smartphone) als Autoschlüssel fungieren, der automatisiert Konfigurationsdaten an die Autoelektronik weitergibt. Umgekehrt ist ebenso die Steuerung des Mobiltelefons über NFC-Marken vorstellbar.

In den vergangenen Jahren wurde die NFC-Technik immer wieder als Zukunftstechnologie angepriesen. Gleichwohl ist die Verbreitung nach wie vor gering, insbesondere verfügen nur wenige Mobiltelefon-Modelle über den nötigen Chip.³³⁰ Bis die für den Echteinsatz erforderliche Robustheit, Datensicherheit und Rechtssicherheit erreicht sind, wird noch an vielen Details zu arbeiten sein. Gerade für Bezahlverfahren müssen weitere Fragen geklärt werden. Dazu gehören nicht nur Verfahren, wie der Nutzer seine Zustimmung zu einem Bezahlvorgang ausdrückt und damit die Zahlung rechtsgültig autorisiert, sondern auch das allgemeine Vertrauen der Nutzer wird eine wichtige Rolle spielen.³³¹

Welche Bedeutung NFC in Zukunft erlangen wird, lässt sich noch nicht einschätzen. Nicht zuletzt ist die Marktdurchsetzung als infrastrukturelles System von der Unterstützung durch die wichtigen Beteiligten (Gerätehersteller, Bezahldienstleister, Handel) abhängig.

2.2.7.3 Auto-ID-Technik Super-Label

Ein weiterer neuer Ansatz auf dem Gebiet der Auto-ID-Verfahren sind Systeme mit kombinierten Etiketten. Das Institut für integrierte Produktion Hannover hat ein von ihr als „Super-Label“ bezeichnetes Identifikationssystem vorgestellt, das die Vorzüge der anderen, bislang im Einsatz befindlichen Auto-ID-Techniken vereinen will. Es kombiniert die menschliche Lesbarkeit von Etiketten mit der maschinellen Lesbarkeit z.B. von Strichcodes und der Widerbeschreibbarkeit, wie sie bei RFID-Marken möglich ist.³³²

Jedes Etikett besteht aus mehreren Komponenten. Eine Anzeige stellt Informationen sowohl in für Menschen lesbarer als auch in maschinell lesbarer Form (z.B. als QR-Code) dar. Um den Energieverbrauch niedrig zu halten, wird eine energieverbrauchsfreie Anzeigetechnik (sog. „No Power“-Display) verwendet, die die Daten unabhängig von einer dauerhaften Spannungsversorgung

³²⁹ S. <http://www.touchandtravel.de/touchandtravel/faq> unter dem Abschnitt „An- und Abmeldung“; *Bischoff/Uckelmann*, in: ident Jahrbuch 2012, 140.

³³⁰ Näheres über die „Verbreitung bei aktiven Geräten“ – s. [http://de.wikipedia.org/wiki/Near Field Communication](http://de.wikipedia.org/wiki/Near_Field_Communication); *Bischoff/Uckelmann*, in: ident Jahrbuch 2012, 138 f.

³³¹ Näher dazu *Osweller*, in: ident Jahrbuch 2012, 142 f.; *Bischoff/Uckelmann*, in: ident Jahrbuch 2012, 141.

³³² http://www.hannover.de/sites/default/files/press/2013/IPH_20130312_HannoverMesse.pdf.

darstellt. Ein Solarzellenbaustein versorgt die elektronischen Bauteile insbesondere bei Auslese- und Schreibvorgängen mit Energie. Welche Daten das Etikett anzeigen soll, wird ihm über eine optische Kommunikation mitgeteilt (Beschreiben des Etiketts). Dazu verfügt es über eine Fotozelle. Als Sender fungiert eine an ein gängiges Mobiltelefon (Smartphone) angeschlossene Leuchtdiode.

Die Leuchtdiode wird über ein Programm auf dem Mobiltelefon gesteuert, das die nötigen Daten an das Etikett überträgt. Verwendet wird Licht des sichtbaren Bereichs. Es wurde der Rotlichtbereich um 660 nm Wellenlänge gewählt, da hier die geringsten Störungen durch andere, vor allem künstliche Lichtquellen zu erwarten sind. Zudem ist dadurch für den Nutzer leicht erkennbar, welches Etikett er konkret beschreibt.

Für das Auslesen des „Super-Labels“ können gängige Geräte zum Lesen von QR- oder Strichcodes verwendet werden, wiederum auch in der Form von Programmen für Betriebssysteme von Mobilfunkgeräten (Smartphone-Apps). Dadurch ist das „Super-Label“ nach den Angaben des Instituts leicht in bestehende Systeme integrierbar. Noch ist dieses kombinierte Etikett zu groß und teuer, um es produktiv einzusetzen. Aber seine Kombifunktionen könnten es für Bereiche in der Logistik interessant machen.

2.3 Szenarische Darstellung des Einsatzes von RFID-Systemen im Kontext allgegenwärtiger Datenverarbeitung

2.3.1 Folgenabschätzung durch Szenarientechnik

2.3.1.1 Ziel und Arten von Szenarienbildung

„Die Technik fragt nicht in erster Linie nach dem, was ist, sondern nach dem, was sein kann (...), (dessen) letzte Beglaubigung freilich nicht in bloßen Urteilen, sondern im Herausstellen und Produzieren bestimmter Gebilde zu suchen ist.“ „Die Gewinnung dieses Blick- und Richtpunktes bedeutet, in rein theoretischer Hinsicht, vielleicht die größte und denkwürdigste Leistung der Technik.“³³³

Mit der Entwicklung und dem Einsatz von Technik werden Bedingungen geschaffen, die Sachzwänge und Anschlusssachzwänge erzeugen, aber auch vielleicht erst später erkennbare Entwicklungsmöglichkeiten eröffnen oder verschließen.³³⁴ Durch heutige Entscheidungen werden bereits die Grundlagen für die künftigen Entwicklungen gelegt. Daher müssen zur Bewertung heutiger Entscheidungen auch deren künftige Auswirkungen berücksichtigt werden.³³⁵

³³³ Cassirer 2004, 176.

³³⁴ Im Ansatz Paschen/Petermann, in: Petermann 1991, 26 f.; Paschen, in: Dierkes/Petermann 1986, 34 f.

³³⁵ Roßnagel 1993, 105; Fuchs, in: Boral/Decker u.a. 2005, 48 ff.

Um Entscheidungen zur Technikentwicklung verantwortlich treffen zu können, bedarf es einer Abschätzung der mit der Technik verbundenen Risiken und Chancen.³³⁶ Diese Abschätzung verlangt ein Hinausgehen über eine auf betriebswirtschaftliche Kosten und Nutzen beschränkte Betrachtung.³³⁷ Bei Einführung, Betrieb und Ausbau von Systemen der modernen Informations- und Kommunikationstechniken sind vor allem die Auswirkungen in den Blick zu nehmen, die sich für die informationellen und kommunikativen Grundrechte der Nutzer oder anderer Betroffener ergeben.

Die allgemeine interdisziplinäre Technikforschung, wozu Disziplinen der Jurisprudenz gehören, insbesondere derjenigen die unter rechtswissenschaftlichem Fokus Technikgestaltung betreiben, zielen anders als die Ingenieurwissenschaften, die gemeinhin mit der Aufgabe theoriegeleiteter Erfindung und Entwicklung hin zur Innovation befasst sind, nicht auf das „Herausstellen und Produzieren bestimmter Gebilde“.³³⁸ Vielmehr hat sie die Prozesse des Herausstellens und Produzierens, also des Umgangs mit der Technik zum Gegenstand und behandelt somit nicht technische, sondern „sozio-technische Systeme“.³³⁹

In solchen sozio-technischen Systemen³⁴⁰ spielen die Akteure und ihre Entscheidungen, ihre Handlungen und Handlungsoptionen eine wichtige Rolle. Entscheidungen bestimmen maßgeblich die Zukunft, wie auch jedes Handeln auf Zukunft gerichtet ist.³⁴¹ „Zukunft ist demnach Folge von Wahlmöglichkeiten in einer bestimmten historischen Situation“.³⁴² Deshalb spricht man auch davon, dass wir nicht nur eine, sondern viele mögliche Zukünfte haben.³⁴³ Um aber Zukunft gestalten zu können, müssen wir diese Entscheidungs- und Handlungsalternativen erkennen und bewerten lernen.³⁴⁴

Da technische Systeme und ihr Rückbezug zur Gesellschaft ein hochkomplexes, nicht-lineares und nicht-determiniertes Wirkungsgeflecht darstellen,³⁴⁵ lassen sich allerdings genaue Vorhersagen über die Zukunftsentwicklung nicht machen.³⁴⁶ „Wir müssen uns auf längerfristige Risikodimensionen einstellen,

³³⁶ BT-Drs. 10/5844; vgl. *Petermann*, in: *Dierkes/Petermann/v. Thienen* 1986, 365 f.; oft mit Verzögerung eintretende Sekundär- und Tertiäreffekte – s. *Bechmann*, in: *Petermann* 1992, 47 f.

³³⁷ *Roßnagel* 1993, 105.

³³⁸ *Cassirer* 2004, 176.

³³⁹ *Roßnagel* 1993, 66; *Hubig*, in: *Heesen/Hubig/Siemoneit/Wiegerling* 2005, 1.

³⁴⁰ *Ropohl* 2009, 81; *Wagner-Döbler* 1989, 142.

³⁴¹ *Zöpel*, in: *Hesse/Rolff/Zöpel* 1988, 13.

³⁴² *Roßnagel* 1993, 106.

³⁴³ S. hierzu *Kreibich*, in: *Hesse/Kreibich/Zöpel* 1989, 25.

³⁴⁴ *Roßnagel* 1993, 106 f.; für Unternehmen *Fink/Schlake/Siebe* 2001, 7 ff., 11 f.

³⁴⁵ *Popper*, in: *Topitsch* 1980, 113 ff., insbes. 115, 117 f.

³⁴⁶ Näher *Geschka/v. Reibnitz*, PolDi 4/1979, 13; *Lohmeyer* 1984, 242 ff., 562; *Huisinga* 1985, 180; *Wagner-Döbler* 1989, 148 ff., insbes. 151; *Frederichs/Hartmann*, in: *Petermann* 1992, 83 ff.; *Paschen/Bechmann*, in: *Petermann* 1991, 157 f.

die mit dem klassischen Ingenieursprinzip des Trial-and-Error-Vorgehens nicht ermittelt werden können“.³⁴⁷ Deshalb ist eine frühzeitige, innovativ-problemorientierte Technikbewertung anzustreben, die ermöglicht, noch regulierend in den Entwicklungsprozess einzugreifen und mögliche schwerwiegende, irreversible Folgen zu kompensieren.

Nachdem die zu betrachtenden technischen Systeme zum einen unübersehbare Schadenspotentiale in sich bergen und zum anderen eine kaum abbildbare Komplexität aufweisen, versagen Instrumente, die im Wege des Versuchs die Risiken und Chancen abschätzen wollen. Sie versagen nicht zuletzt deshalb, weil nicht nur die Einbeziehung von sozio-technischen Konfigurationsänderungen begrenzt bleibt, sondern weil auch mögliche Irrtumskosten nicht tragbar sind.³⁴⁸ Dazu bedarf es Instrumente mit einer längerfristig angelegten Betrachtung, die es erlauben, die Voraussetzungen und Folgen des jeweiligen Entwicklungskonzepts in ihrem systemaren Bezug zu erkennen.³⁴⁹

Als Instrumente der Technikbewertung bieten sich Gedankenexperimente an, die die künftigen Entwicklungen hypothetisch vorwegnehmen. Mit Gedankenexperimenten können auch langfristige Auswirkungen der technischen Systeme erfasst, Veränderungen der gesellschaftlichen Rahmenbedingungen einbezogen und Reaktionsmöglichkeiten der Akteure berücksichtigt und so sozio-technische Entwicklungsalternativen verglichen werden.³⁵⁰ Abhängig vom Untersuchungsinteresse können unterschiedliche Arten von Gedankenexperimenten durchgeführt werden. Sie alle versuchen, die Zukunft zu beschreiben und sind Entwürfe eines Zukunftsbildes oder Szenarios. Der Begriff wird auf das griechische Wort „skene“ zurückgeführt, mit dem der Schauplatz einer Handlung, eine Szenenfolge in einem Bühnenstück beziehungsweise der Rohentwurf eines Dramas bezeichnet wird.³⁵¹

Durch die Krise der bisherigen quantitativen (Trend-)Prognosen, die im Rahmen hochturbulenter, dynamischer Umwelten nur noch bedingte Aussagekraft beanspruchen konnten, wurde die Hinwendung zur Szenariomethode in den 60er- und 70er-Jahren des letzten Jahrhunderts gefördert. Unsicherheit und Diskontinuität, Trendbrüche und das Auftreten überraschender Störgrößen machen das Errechnen von Trends praktisch unmöglich und erforderten eine neue Generation von Planungs- und Prognoseinstrumenten, die „unvollständige Definitionsbereiche“ berücksichtigen.³⁵²

Untersuchung mit Hilfe von Szenarien hat also eine wichtige heuristische Funktion.³⁵³ Szenarien können dann eine entscheidungs- und handlungsleiten-

³⁴⁷ Ueberhorst 1986, 39 f.; zur Mittel- und Langfristigkeit – s. auch Huisinga 1985, 180.

³⁴⁸ Roßnagel 1993, 11 f., 14 ff., 24, 74.

³⁴⁹ Roßnagel 1993, 141; näher Ueberhorst 1986, 38 ff.; s. auch Huisinga 1985, 180.

³⁵⁰ Roßnagel 1993, 141.

³⁵¹ Der kleine Pauly, Lexikon der Antike, Band 5 1979, 223.

³⁵² Vgl. Hubig 1995, 80 ff.

³⁵³ Vgl. Hubig, in: Heesen/Hubig/Siemoneit/Wiegerling 2005, 2 f.

de Hilfe anbieten, wenn sie den Möglichkeitsraum künftiger Entwicklungen ausloten und aufzeigen, welche Prozesse und Handlungen die geschilderte Entwicklung bestimmen und beeinflussen.³⁵⁴

Hierdurch besteht die begründete Hoffnung, der Gefahr vorzubeugen, dass beim zukünftigen Handeln mit und in diesen technischen Systemen Überraschungen positiver oder negativer Art auftreten, sich Einsatzmöglichkeiten zeigen, mit denen niemand gerechnet hat oder Effekte zutage treten, die in zu geringem Maße auf ihre Akzeptabilität hin untersucht worden sind.³⁵⁵

2.3.1.2 Rechtswissenschaftliches Interesse an der Szenarienbildung

Anders als die Technikphilosophie, die auf ein (logisch) „schwächeres“ Konzept von Akzeptabilität im Sinne einer Akzeptanzfähigkeit zielt,³⁵⁶ verfolgt die rechtswissenschaftliche Technikfolgenforschung die Analyse und Bewertung der Techniksysteme unter dem Blickwinkel der Akzeptabilität im Sinne der möglichen Folgen für Rechtsziele.³⁵⁷ Dabei liegt ihr Fokus hinsichtlich der technikbedingten Risiken weniger auf dem gegenwärtigen Rechtsgüterschutz als vielmehr auf den Auswirkungen für Rechtsziele aufgrund der durch die Techniksysteme veränderten Verwirklichungsbedingungen.³⁵⁸ Der Maßstab der Akzeptabilität bedeutet danach zu fragen, inwieweit ein Techniksystem und seine Folgen Vorgaben der relevanten Rechtsziele fördern oder mit Rechtszielen vereinbar sind, also inwieweit sich es rechtsverträglich darstellt. Dabei sollte man über die Analyse der Veränderungen der Verwirklichungsbedingungen von Rechtszielen und über die rechtswissenschaftliche Bewertung der Technikfolgen hinausgehen. Sie sollten in Ansätze und Vorschläge münden, die geeignet sind, die Technikenese rechtsverträglich zu steuern.³⁵⁹

Als Untersuchungsgegenstand bieten sich vor allem Techniksysteme an, denen voraussichtlich die weitreichendsten und tiefgreifendsten Folgewirkungen innewohnen und mit denen die Möglichkeit sozialer Konflikte verbunden sind.³⁶⁰ Zu solchen konfliktträchtigen Systemen dürfen wegen ihres umgreifenden und infrastrukturähnlichen Charakters Techniken gezählt werden, die eine Welt der „allgegenwärtigen Datenverarbeitung“ realisieren helfen.³⁶¹

³⁵⁴ Roßnagel 1993, 119; *Geschka/v. Reibnitz*, PolDi 4/1979, 71 ff.; *Lohmeyer* 1984, 471 f.; *Huisinga* 1985, 157.

³⁵⁵ Hubig, in: *Heesen/Hubig/Siemonet/Wiegerling* 2005, 3.

³⁵⁶ „Akzeptanzfähigkeit in dem Sinne, dass sie ein bewusstes Entscheiden und Bewerten seitens der Nutzer ermöglicht“ – s. Hubig, in: *Heesen/Hubig/Siemonet/Wiegerling* 2005, 3.

³⁵⁷ Roßnagel 1993, 99.

³⁵⁸ Roßnagel 1993, 99.

³⁵⁹ Roßnagel 1993, 99 f.

³⁶⁰ Roßnagel 1993, 100.

³⁶¹ Auto-ID-Verfahren, wie die der RFID-Systeme, werden wichtige Basistechniken eines sich weiter informatisierenden Alltags sein, der schrittweise in die Vision der allgegenwärtigen Datenverarbeitung mündet.

Schwierigkeiten bereitet allerdings, abzuschätzen, wie sich noch nicht entwickelte und erst in der Zukunft eingesetzte Techniksysteme auf Rechtsziele auswirken werden, da eine Antizipierung des künftigen Rechtsverständnisses kaum möglich ist. So gilt es, im Blick auf die im Szenario beschriebenen Wirklichkeitsbedingungen und angedeuteten Folgen zu ermitteln, welcher Änderungsdruck auf Rechtsvorschriften, welche Einflussmöglichkeiten hinsichtlich rechtlich gewollter Zustände bestehen und wie das Rechtssystem auf die Herausforderungen reagieren wird.

Der Rechtsverträglichkeitsprüfung kann nur das derzeitige Verständnis von Rechtsnormen zugrunde gelegt und mit dem Rechtsverständnis verglichen werden, wie es aufgrund heutiger Kenntnisse über die Situation in der Zukunft zu vermuten ist.³⁶² Dazu ist der Versuch zu unternehmen, die gegenwärtig gültigen Prinzipien konsistent fortzuentwickeln.

2.3.1.3 Methodik der Szenarienbildung

Nach Einführung der Szenariomethode als Alternativ- oder Multioptionsdenken für klar begrenzte Probleme mit langfristigem Charakter³⁶³ in die Zukunftsforschung, durch eine Arbeitsgruppe um Hermann Kahn seit den 60er- und 70er-Jahren, wurden eine Reihe von szenariobasierten Verfahren entwickelt,³⁶⁴ wie u.a. die „Prospective Analysis“ in der französischen Regionalplanung.³⁶⁵ Diese werden seitdem primär in den Wirtschafts- und Sozialwissenschaften angewendet.³⁶⁶

Die Szenario-Methodik³⁶⁷ wird im Rahmen futurologischer Methoden oftmals mit der Prognose verglichen, die aber nur begrenzt und unter Außerachtlassung externer, veränderlicher Faktoren die Gegenwart in die Zukunft projiziert.³⁶⁸ Im Gegensatz dazu ist sie auch nicht bloß als quantitativ zu verstehen, sondern als Ansatz zu qualitativer bzw. inhaltlicher Analyse.³⁶⁹

Auch versteht sich die Szenario-Methode im Kontrast zu jener als mehrdimensional³⁷⁰ und flexibel bezüglich ihrer Denkweise, sieht ihren Gegenstand in

³⁶² Roßnagel 1993, 102.

³⁶³ Mißler-Behr 1993, 21.

³⁶⁴ Steinmüller 1997, 7, 58 ff.; Segner 1976, 6; Huisinga 1985, 164; Kaluzal/Ostendorf 1995, 4 ff.; Meyer-Schönherr 1992, 12 f.

³⁶⁵ Vgl. Kaluzal/Ostendorf 1995, 5 und Fußnote 34; Huisinga 1985, 164; Segner 1976, 6.

³⁶⁶ Fink/Schlake/Siebe 2001, 59.

³⁶⁷ Zum Problem der uneinheitlichen Definition – vgl. Meyer-Schönherr 1992, 13, 20 ff.

³⁶⁸ v. Reibnitz 1987, 16.

³⁶⁹ Mißler-Behr 1993, IX; vgl. Steinmüller 1997, 51; Huisinga 1985, 156. Dies bedeutet aber keinesfalls den Ausschluss von quantitativen Daten im Rahmen der Szenario-Methodik, vielmehr kann diese beide Ansätze vereinen bzw. Quantitatives nutzen; vgl. Breiner 1997, 22, 27; Meyer-Schönherr 1992, 21 f., 30 f. Explizit als Kombinationsmethode bezeichnet Leutzbach 2000, 35; vgl. Kaluzal/Ostendorf 1995, 9.

³⁷⁰ Dazu vergleiche die Ausführungen zu Chaos-Theorie und Wettervoraussage bei Christensen, in: Kornwachs 1991, 96 f. Und auch als äußerst komplex – vgl. Kaluzal/Ostendorf 1995, 91.

komplexen Systemen und setzt an die Stelle mathematischer (bloß scheinbarer) Exaktheit die Plausibilität einer Argumentation.³⁷¹ Statt einer determiniert scheinenden Entwicklung sind alternative Szenarien zu berücksichtigen.³⁷²

Hingegen lassen sich Szenarien von Simulationen dadurch unterscheiden,³⁷³ dass letztere alle möglichen Zukünfte, rechnergestützt erarbeitet, darstellen.³⁷⁴ Daneben soll ein Szenario gerade die systematische Analyse hypothetischer, in logischen Schritten entwickelter Entwicklungen sein und ist deswegen weder Utopie noch „Science-Fiction“,³⁷⁵ die nicht den Anspruch auf wissenschaftliche Stringenz und Methodenstrenge erheben, sondern künstlerischer Tätigkeit entspringen.³⁷⁶ Zweck der Methode ist es, wahrscheinliche von unwahrscheinlichen Zukünften zu unterscheiden, Probleme zu eruieren und Ansätze zur Steuerung zu erkennen.

Indem die Szenariomethode auf intersubjektive Nachvollziehbarkeit und auf Begründung von Aussagen mit relevanten Informationen Wert legt, kommt ihr gegenüber Prophezeiungen und bloßem Science-Fiction eine Wissenschaftlichkeit zu. Plausibilität, Nachvollziehbarkeit und Transparenz – besonders auch der zugrunde liegenden expliziten und impliziten Werturteile – zeichnen das wissenschaftliche Vorgehen der Szenariomethode aus.

Die Szenariotechnik ist primär im Sinne eines deskriptiven³⁷⁷ Foresight-Prozesses angelegt.³⁷⁸ Es wird unterschieden, ob sich die Szenarioentwicklung auf mathematische Algorithmen (modellgestütztes Szenario) oder auf die Bewertung von Personen oder Personengruppen stützt (intuitives Szenario).³⁷⁹ Begrenzt wird diese Methodik u.a. durch die formale Logik, die Ressourcen wie die benötigte Datenmenge, Zeitaufwand und Rechnerkapazitäten sowie die Lern- und Nachvollziehbarkeit.³⁸⁰

Vor dem eigentlich interessierenden Schritt der Analyse der Szenarien und ihrer Bewertung, liegt der Prozess der Szenarienbildung.³⁸¹ Dieser Prozess umfasst zunächst vor der eigentlichen Szenarienkonstruktion als ersten Schritt die

³⁷¹ Zur Scheinpräzision Kornwachs, in: ders. 1991, 16. Zur Plausibilität Meyer-Schönherr 1992, 19.

³⁷² Steinmüller 1997, 49; Breiner 1997, 203. Vgl. Meyer-Schönherr 1992, 22.

³⁷³ Allgemein zu den Systematisierungsbemühungen – s. Steinmüller 1997, 29 ff.

³⁷⁴ v. Reibnitz 1987, 17.

³⁷⁵ Segner 1976, 6; Kahn/Wiener 1968, 20.

³⁷⁶ Steinmüller 1997, 64 ff.

³⁷⁷ Präskriptive sind ebenso möglich – vgl. Fink/Schlake/Siebe 2001, 63.

³⁷⁸ Vgl. Steinmüller 1997, 61.

³⁷⁹ Fink/Schlake/Siebe 2001, 63; vgl. zu intuitiv und davon zu differenzierenden Kategorien Steinmüller 1997, 29. Als „weiche“ Methode im Vergleich zur „harten“ der Mathematik Meyer-Schönherr 1992, 21 ff.

³⁸⁰ Segner 1976, 80 ff.

³⁸¹ Steinmüller 1997, 41. Für die Gliederung der einzelnen Schritte der Szenariotechnik bestehen vielfältige Ausprägungen, vgl. bspw. Mißler-Behr 1993, 23 ff. Vgl. auch Tessun, in: Gausemeier/Fink/Schlake 1998, 114 f.

Aufgabenanalyse, in der Untersuchungsgegenstand und Erkenntnisziel festzulegen sind.³⁸² Bei der Szenarioentwicklung selbst – als zweitem Schritt – sind zum ersten (endogene wie exogene) Einfluss- und Schlüsselfaktoren und Abhängigkeiten³⁸³ zu identifizieren, zum zweiten für jeden Schlüsselfaktor Zukunftsprojektionen zu entwickeln und schließlich zum dritten die Zukunftsprojektionen unter Beachtung der Widerspruchsfreiheit – also durch Herstellung von Konsistenz³⁸⁴ – zu verknüpfen und auf Grundlage dessen eine überschaubare Anzahl von Rohszenarien zu entwerfen.³⁸⁵ Kritische, d.h. Einflussfaktoren mit mehreren möglichen Ausprägungen erhöhen dabei die Anforderungen an die subjektive Bewertung des Szenarios.³⁸⁶

In Anbetracht der verschiedenen, die Zukunft und somit auch die Szenarien, bestimmenden Faktoren, ergeben sich, um so ferner die Zukunft, immer neuere Abzweigungen und dadurch mehr Möglichkeiten. Das lässt sich bildlich durch einen (umgekehrten) Trichter (im Sinne eines Art Duschkopfs) darstellen.³⁸⁷ Ein Entwicklungspfad, der zu einem bestimmten Szenario führen soll, kann durch ein unvorhergesehenes Ereignis gestört werden.³⁸⁸ Der Möglichkeitsraum von Zukünften kann, je nach Ansatz und Untersuchungsziel, aber auf Zukünfte extremer Entwicklungen beschränkt werden.³⁸⁹

Als Hilfsmittel zur Erarbeitung von Szenarien können dabei u.a. Fallstudien³⁹⁰, historische Analogien³⁹¹, sozialwissenschaftliche Theorien³⁹², Literaturstudien, Betroffenenbeteiligungen und Expertenbefragungen³⁹³ dienen. Trotz einer methodisch geleiteten Erarbeitung von Szenarien ist diese ohne ein gewisses Maß an Intuition und Kreativität nicht denkbar, da unterschiedliche Einschätzungen und widersprüchliche Informationen subjektiv bewertet und mit viel Sachkenntnis und „Phantasie“ zu einem plausiblen Gesamtbild verbunden werden müssen.³⁹⁴

³⁸² Fink/Schlake/Siebe 2001, 65.

³⁸³ Mathematisch formalisierend Mißler-Behr 1993, 23 ff. Vgl. Tessun, in: Gausemeier/Fink/Schlake 1998, 114 f.

³⁸⁴ Geschka/v. Reibnitz, PolDi 4/1979, 15; Mißler-Behr 1993, 30 f.; Steinmüller 1997, 52; Meyer-Schönherr 1992, 19.

³⁸⁵ In anderer, abgestufter Einteilung Fink/Schlake/Siebe 2001, 68. S. auch Mißler-Behr 1993, 9 ff.

³⁸⁶ Mißler-Behr 1993, 21, 14.

³⁸⁷ Geschka/v. Reibnitz, PolDi 4/1979, 72; v. Reibnitz 1987, 29 ff.; Mißler-Behr 1993, 3; hinsichtlich der zunehmenden Anzahl an Szenarien Segner 1976, 79.

³⁸⁸ Mißler-Behr 1993, 3 f.

³⁸⁹ Das Gegenstück zu diesen extremen oder auch peripheren Szenarien sind die trendorientierten – s. Gausemeier/Fink/Schlake 1995, 113 f.

³⁹⁰ Roßnagel 1993, 176 ff.

³⁹¹ Roßnagel 1993, 178 ff.

³⁹² Roßnagel 1993, 181.

³⁹³ Roßnagel 1993, 182 ff.; Geschka/v. Reibnitz, PolDi 4/1979, 74.

³⁹⁴ Roßnagel 1993, 185; Segner 1976, 41 f.

Im Schritt drei, der Szenarioausarbeitung (Szenario-Writing), gilt es dann den erarbeiteten mentalen Zukunftsentwurf (intensionale Szenario)³⁹⁵ in einer zielgruppengerechten Darstellungsform (extensionale Szenario) plastisch zu beschreiben.³⁹⁶ Neben mathematischen und graphischen Darstellungsformen stehen verbale, insbesondere in Form von Erzählungen in chronologischer Abfolge, zur Verfügung.³⁹⁷

In der Zukunftsforschung können – je nach Fragestellung – zur Abschätzung von Technikfolgen verschiedene Arten von Szenarien, idealtypisch vor allem Trend-, Visions-, Umfeld- und determinierte Szenarien unterschieden werden.³⁹⁸ In Trendszenarien werden die Auswirkungen gesellschaftlicher Entwicklungstrends beschrieben, die in bestimmten Gesellschaftsbereichen für Techniknutzungskonzepte relevant sind. Dabei werden die sich bereits abzeichnenden Entwicklungslinien unter Einbeziehung von Trendextrapolationen³⁹⁹ und die wahrscheinlich durchsetzungsmächtigen Interessen berücksichtigt.⁴⁰⁰

Visionsszenarien stellen dagegen eine mögliche Zukunft dar, die bei der Wahrnehmung vorgeschlagener Handlungsoptionen bisherige Lebenswirklichkeit am Maßstab bestimmter Kriterien verbessert. Durch diese normativen Projektionen werden Gestaltungschancen aufgezeigt, die durch politische, soziale und rechtliche Veränderungen sowie durch die Nutzung von Techniksystemen real bestehen.⁴⁰¹

In einem determinierten Szenario wird ein Techniksystem hinsichtlich seiner gesellschaftlichen und auch rechtlichen Auswirkungen untersucht. Dabei liegt der Fokus auf dem Techniksystem, dessen Realisierung unabhängig von seiner Einführung entgegenstehender Trendentwicklungen angenommen wird.⁴⁰² Umfeldszenarien entwickeln Zukunftsbilder eines Untersuchungsfeldes, indem sie dessen relevante Umfelder⁴⁰³ und deren Zukunftsentwicklung analysieren. Von diesen ausgehend wird dann versucht, die Entwicklungspotentiale, Handlungsmöglichkeiten und Auswirkungen in dem eigentlichen Untersuchungsfeld zu bestimmen. In Umfeldszenarien sollen schließlich fördernde oder hemmende Ein-

³⁹⁵ Steinmüller 1997, 52, 65.

³⁹⁶ Steinmüller 1997, 61 ff.

³⁹⁷ Segner 1976, 45 ff.

³⁹⁸ Roßnagel 1993, 148. Zu weiteren Arten möglicher Szenarien z.B. Scharioth, CM 12/1987, 20.

³⁹⁹ Zu Trendextrapolationen – s. Geschka/v. Reibnitz, PoDi 4/1979, 5 f.; Huisinga 1985, 164.

⁴⁰⁰ Kubicek 1991, 44 f.

⁴⁰¹ Roßnagel 1993, 152 ff.

⁴⁰² Roßnagel 1993, 154 ff.

⁴⁰³ Nicht beeinflussbar als weiteres Merkmal – s. Fink/Schlake/Siebe 2001, 70. Gausemeier/ Fink/Schlake differenzieren nach dem Kriterium der Lenkbarkeit zwischen Umfeld-, Lenkungs- (bzw. Gestaltungs-) und Systemszenarien.

flussfaktoren auf eine Entwicklung identifiziert und dadurch Wechselwirkungen zwischen dem Feld des Untersuchungsgegenstandes erkennbar werden.⁴⁰⁴

Um verschiedenen Untersuchungsinteressen bei einer solchen Zukunftsvision wie der des Einsatzes von Auto-ID-Systemen im Kontext allgegenwärtiger Datenverarbeitung gerecht zu werden, könnte es sich für die Bewertung eines angedachten Techniksystems anbieten, die Risiken mit Hilfe eines determinierten Szenarios abzuschätzen, die möglichen Alternativen zur Lösung des zugrundeliegenden sozialen Problems mit Hilfe von Visionsszenarien zu thematisieren und die gegebenen Handlungsspielräume durch Umfeldszenarien abzu stecken.

2.3.1.4 Datenschutzrechtlich relevante Leitlinien für die Szenarienbildung

Für das Forschungsfeld des Datenschutzrechts ist besonders interessant, wie sich die Verwirklichungsbedingungen der informationellen Selbstbestimmung und kommunikativer Grundrechte der Menschen durch die neuen Systeme der Informations- und Kommunikationstechnik verändern. Um im Szenario das Verletzungspotential und den erforderlichen Schutzbedarf für die datenschutzrechtlichen Rechtsgüter unter den Bedingungen einer Welt des „Ubiquitous Computing“ deutlich machen zu können, müssen zum einen im Rahmen der Szenarienburgildung Interessen und Situationen Berücksichtigung finden, die datenschutzrechtlich relevant sind. Bei der Ausarbeitung von Szenarien sind zum anderen die datenschutzrechtlichen Anforderungen im Auge zu behalten. Die im Folgenden angesprochenen Leitlinien stellen in Ergänzung der Szenariomethodik Hinweise dar, die die Szenarienburgildung im interdisziplinären Diskurs unterstützen und konkretisieren.⁴⁰⁵

2.3.1.4.1 Datenschutzrechtliche Anforderungen bei der Szenarienburgildung

Für die datenschutzrechtliche Relevanz sollten die Szenarien in verschiedenen Lebensbereichen spielen und jeweils Konstellationen und Situationen beinhalten, bei denen Daten mit Personenbezug entstehen, ausgewertet, gespeichert und auch ausgetauscht werden. Als Orientierung können folgende Anhaltspunkte dienen.

2.3.1.4.1.1 Verschiedene Lebensbereiche und unterschiedlicher Datenumgang

Für die datenschutzrechtliche Bewertung kann es einen Unterschied machen, wo, mit welcher Art von Daten und gegenüber wem der Datenverarbeitungsvorgang stattfindet. Da das Datenschutzrecht unterschiedliche Anforderungen für

⁴⁰⁴ S. hierzu *Paschen*, in: *Dierkes/Petermann/v. Thienen* 1986, 35; *Scharioth*, CM 12/1987, 20 ff.

⁴⁰⁵ *Müller* 2003b, 1 ff.

verschiedene Lebensbereiche vorsieht, sollten die Szenarien die folgenden Aspekte berücksichtigen.

Sie sollten Lebensbereiche im lokalen Sinn skizzieren und Alltagsfelder umfassen, in denen sich die Menschen bewegen. Dies reicht von der Wohnung über das Arbeitsleben bis hin zu der Teilnahme am öffentlichen Leben (z.B. Verkehrsmittelbenutzung, Einkaufserledigungen, Spaziergänge). Gegenüber der häuslichen Sphäre, in der Datenverarbeitungsvorgänge zu persönlichen und familiären Zwecken aus dem Anwendungsbereich des Datenschutzrechts ausgenommen sind und in der eher anzunehmen ist, dass der Betroffene die datenverarbeitenden Vorgänge zu kontrollieren vermag, stellen sich beim Bewegen im öffentlichen Raum die Fragen nach der Gewährleistung des Datenschutzes in stärkerem Maß.

Die Anwendungen im Kontext der allgegenwärtigen Datenverarbeitung sollten Daten mit unterschiedlicher Qualität oder Sensitivität erheben und verwenden. Auch wenn das Bundesverfassungsgericht für ein Datum voraussetzt, es könne nicht belanglos sein, ist es für eine mögliche Neubewertung hilfreich, wenn der Datenumgang verschieden intensiv in die Bereiche des allgemeinen Persönlichkeitsrechts und des informationellen Selbstbestimmungsrechts eingreift. Es hat eine andere Bedeutung, ob die RFID-markierte Ware eines Kunden oder das Gesicht eines Passanten registriert wird oder ob Gesundheitsdaten über die genomische Disposition des Einzelnen über Techniksysteme ausgelesen werden können.

Zudem sollten typische Abhängigkeitsverhältnisse mit einbezogen werden, die sich durch ungleiche Bedingungen auszeichnen, wie Nutzer gegenüber Infrastrukturanbieter, Arbeitnehmer gegenüber Arbeitgeber, Patient gegenüber Arzt, Mieter gegenüber Vermieter und Bürger gegenüber hoheitlich handelndem Staat. Wegen des in solchen Beziehungen grundsätzlich bestehenden Vertrauens- und dauerhaften Abhängigkeitsverhältnisses sind datenschutzrechtlich relevante Vorgänge oft anders zu beurteilen als die übrigen Beziehungen des Geschäftsverkehrs.

Da das geltende Datenschutzrecht für den Umgang mit personenbezogenen Daten durch nicht-öffentliche Stellen und öffentliche Stellen unterschiedliche Anforderungen vorsieht, ist auch bei Anwendungen der allgegenwärtigen Datenverarbeitung grundsätzlich interessant, die Beteiligung privater Anbieter einerseits und von Hoheitsträgern andererseits zu betrachten. Allerdings werden insbesondere im Bereich der Eingriffsverwaltung für das beabsichtigte Verwaltungshandeln erforderliche Datenverarbeitungsvorgänge oft durch Schaffung neuer Rechtsgrundlagen gerechtfertigt, sodass der Konflikt um die Gewährleistung der informationellen Selbstbestimmung sich verlagert und weniger rechtsdogmatisch als politisch auszutragen ist.⁴⁰⁶

⁴⁰⁶ Deshalb beschränkt sich vorliegende Untersuchung auf Auto-ID-Verfahren und den mit ihrem Einsatz verbundenen Datenumgang, der von nicht-öffentlichen Stellen verantwortet wird.

2.3.1.4.1.2 Datenschutzrechtliche Konfliktkonstellation

Für eine datenschutzrechtliche Betrachtung zur Abschätzung der möglichen Risiken sind Konstellationen interessant, in denen ein Datenumgang stattfindet, der eine Gefährdung der informationellen Selbstbestimmung der jeweils Betroffenen bedeutet. Eine solche „Konfliktkonstellation“ ist grundsätzlich gegeben, wenn die erhobenen, verarbeiteten oder genutzten Daten nicht in der kontrollierten Sphäre des Betroffenen verbleiben. Das informationelle Selbstbestimmungsrecht ist betroffen und eine Beeinträchtigung droht, wenn ein außenstehender Dritter beteiligt ist und die Datenverarbeitungsvorgänge nicht allein beim Betroffenen selbst abgewickelt werden. Bei einem Rückgriff auf eine Infrastruktur zur Erfüllung von Informations- oder Lokalisationsdiensten (RFID-gestützte Führung auf dem Ausstellungsgelände), die hierfür Daten erhebt, verarbeitet und nutzt, ist beispielsweise datenschutzrechtlich eine aktive Lösung wesentlich problematischer als eine passive. Bei einer aktiven (also weniger datenschutzfreundlichen) Lösung werden personenbezogene Daten des Betroffenen benötigt, indem er sich zum Beispiel authentifizieren oder Profildaten abgeben muss. Dagegen ermöglicht die Inanspruchnahme einer satellitengestützten Positionsbestimmung (GPS) beispielsweise eine rein anonyme Nutzung.

Ebenso sollten Konstellationen Eingang finden, in denen der Einsatz von (neuartigen) Techniksystemen und die Einführung von Anwendungen verdeutlichen, welche neue Qualität im Umgang mit personenbezogenen Daten entsteht und wie sich dadurch die Bedingungen für die Gewährleistung der informationellen Selbstbestimmung verändern werden. Dabei können die Anwendungen in einer Welt der allgegenwärtigen Datenverarbeitung eine neue Qualität des Datenumgangs hervorrufen. Es finden Datenverarbeitungsvorgänge im Hintergrund unmerklich statt. Sie greifen hierbei überall auf (Straßen, Kaufhäusern, Verkehrsmitteln) vorhandene Sensoreinheiten oder Lesegerätestationen zurück und verknüpfen verschiedene, auch in Datenbanken hinterlegte Datenbestände. Dadurch wird der Einzelne, ohne es beeinflussen zu können, Gegenstand von Vorgängen der Datenerhebung und Datenverwendung.

Deshalb sollten, um eine Untersuchung von Anwendungen im Kontext der allgegenwärtigen Datenverarbeitung zu unterstützen, in den unterschiedlichen Situationen Elemente oder Bedingungen eingearbeitet sein, die diese Vision kennzeichnen. Ausgehend von dem Umstand, dass Alltagsgegenstände mit Rechnertechnik ausgestattet werden, findet die damit verbundene Datenerhebung und Datenverarbeitung, wie angesprochen, im Hintergrund unmerklich statt. Dies stellt neue Herausforderungen für die Transparenz der Datenverarbeitung und ihrer Struktur sowie für die Datenschutzkommunikation dar (Unterrichtung und Einwilligung). Zum einen wird die Datenverarbeitung Teil des Verhaltens und der Handlungen des Betroffenen (z.B. bei der Registrierung des Kundenverhaltens durch das mit RFID-Technik versehene Warenregal). Zum anderen passiert die Datenverarbeitung bei der Inanspruchnahme eines Dienstes oder einer Leistung, ohne dass der Betroffene den in den Hintergrund getretenen Datenverarbeitungsvorgang ermessen oder sich gar bewusst machen kann (z.B. Buchung und Abrechnung beim Einsteigen in ein Verkehrsmittel).

Das Szenario sollte weiter zum einen die Möglichkeit der Erstellung von Leistungs- sowie Verhaltensprofilen berücksichtigen und zum anderen das Problem der Zusammenführung und Auswertung aufzeigen. Dabei ist die Rolle des Infrastrukturbetreibers zu klären (wo fallen die Daten an und wer vermag diese zusammenzuführen).

Ferner ist bei der Ausgestaltung der Konfliktkonstellation zu bedenken, dass eine Datenerhebung, Datenverarbeitung und Datennutzung nur mit einem bestimmten Zweck durchgeführt werden darf. Um das komfortable Funktionieren der unterschiedlichen Anwendungen zu ermöglichen, ist es in einer Umgebung allgegenwärtiger Datenverarbeitung vorstellbar, dass sich zum einen der Zweck vorher nicht genau festlegen lässt und zum anderen im Laufe des Geschehens eine Zweckänderung eintritt. Insbesondere für die Wirksamkeit der datenschutzrechtlichen Einwilligung wird es schwierig sein, wenn sich der ursprüngliche Zweck, für den Daten erhoben und verarbeitet wurden, ändert.

Weiter sollte die Erweiterung und Einschränkung der Autonomie durch die Welt einer allgegenwärtigen Datenverarbeitung deutlich werden. Zum Beispiel kann die anonyme Vergemeinschaftung zu einer geringeren Transparenz, dagegen die Verbesserung der individuellen Information zu einer höheren Transparenz für den Einzelnen führen.

2.3.1.4.1.3 Integration von datenschutzgerechten Lösungsansätzen

Sinnvoll ist in den Szenarien, soweit im Vorfeld abschätzbar, datenschutzfördernde Techniken als Lösungsvorschläge zu berücksichtigen. In Betracht kommt hierbei das Agieren unter einem Pseudonym. Bei Diensten oder Anwendungen, die einer personalisierten Zuordnung, aber nicht der natürlichen Identität bedürfen, könnte als milderer Mittel eine künstlich zugewiesene Identität ausreichen. Vielleicht ließe sich auch eine Fallkonstellation bilden, in der ein Aufhebungsbedürfnis der Zuordnung des Pseudonyms entsteht.

Um gestufte Anforderungskriterien für die Rechtfertigung einer Datenerhebung und -verarbeitung darstellen zu können, wäre es hilfreich, wenn Anwendungen in den Szenarien beschrieben werden, bei denen es einmal um die Verarbeitung der personenbezogenen Daten selbst geht und solche, bei denen die personenbezogenen Daten nur indirekt zur Erfüllung der Anwendung und des Zwecks benötigt werden.

2.3.1.4.2 Anforderungen bei der Ausarbeitung der Szenarien

Bei der Ausarbeitung des Szenarios gilt es, die Konstellationen in einer Weise darzustellen, die eine rechtliche Prüfung ermöglicht. Daher sollten die einzelnen Anwendungen nicht nur hinsichtlich ihrer Aufgabe beschrieben werden. Vielmehr muss die Beschreibung auch das technische Konzept erkennen lassen, mit dem sie realisiert werden könnten. Je konkreter die technische Umsetzung, umso präziser lässt sich eine rechtliche Untersuchung durchführen. Dabei brauchen die technischen Komponenten allerdings nicht genau spezifiziert, sondern nur hinsichtlich ihrer Funktionalität dargestellt zu werden.

Zur Orientierung können folgende Fragen dienen:

- Welche Vorgänge, bei denen Daten erhoben, gespeichert, übermittelt oder genutzt werden, beinhaltet die betreffende Anwendung?
- Wer ist die datenerhebende, -verarbeitende und -nutzende Stelle?
- Welche Datenverarbeitungsvorgänge werden durchgeführt?
- Werden Daten in dem Techniksistem, dessen sich die Anwendung bedient, gespeichert und lediglich in diesem selbst verarbeitet? Oder werden die Daten zum Abgleich mit anderen Datenbeständen an ein weiteres Techniksistem (z.B. Datenbankrechner) übermittelt?
- Welcher Art sind die angefallenen, also erhobenen, gespeicherten, übermittelten und genutzten Daten? Sind es Daten über Merkmale der Person selbst oder Daten über Umstände, die in Beziehung zur Person stehen (wie z.B. Position, Bewegungsmuster, abgefragte Information oder Kaufvorlieben)?
- Mit welchem Zweck, also zur Erfüllung welcher Aufgabe, werden die Daten erhoben, verarbeitet oder genutzt?
- Inwieweit sind die erhobenen, verarbeiteten oder genutzten Daten wirklich zur Erfüllung des beschriebenen Zwecks oder der von der betreffenden Anwendung verfolgten Aufgabe technisch erforderlich?

2.3.2 Szenarische Darstellung vom Leben im Kontext allgegenwärtiger Datenverarbeitung

Das folgende Szenario beschreibt typische Verrichtungen in einem Tagesablauf eines Angestellten. Dieser wird beim Reisen, Einkaufen, Konferenzbesuch aber auch beim Zurechtfinden in einer fremden Stadt begleitet. Es erscheint durchaus vorstellbar, dass in der Zukunft Menschen in den verschiedenen Lebensbereichen sowohl Dienstangebote in Anspruch nehmen als auch mit Techniksyste-men konfrontiert sind, die dieser Vision des „Ubiquitous Computing“ zugeordnet werden können. Auch wenn die Integration von Sensor- und Rechner-technik in Alltagsgegenstände und Umgebungselemente, wie auch deren Vernetzung untereinander bei weitem nicht in diesem Ausmaß fortgeschritten ist, zeigen sich in Technologien und Techniksyste-men, an denen heute schon in Forschungseinrichtungen und Entwicklungsabteilungen von Unternehmen gearbeitet wird, Ansätze einer Informatisierung des Alltages. Teilweise sind manche Anwendungsideen insbesondere im Hinblick auf die weitergehenden Möglichkeiten durch neue Mobilgeräte, wie Smartphone oder Smartwatches, in Verbindung vieler öffentlicher Informationsangebote und entsprechend abgestimmter Dienstangebote stückweit bereits umgesetzt.

2.3.2.1 Funktion der vorgestellten Szenariodarstellung

Im Zusammenhang mit der vorliegenden Untersuchung werden Szenariopas-sagen vorgestellt, die die Facetten des Lebens in einer smarten Umgebung il-lustrieren und den Möglichkeitsraum ein Stück weit ausloten sollen. In kleinen Handlungs- und Interaktionsprozessen soll das Konzept von „Ubiquitous Com-

puting“ mit seinen allgegenwärtigen, unmerklichen, vernetzten und ineinandergreifenden Techniksystemen plastisch werden. Deshalb orientiert sich die erarbeitete Szenariengeschichte an den in diesem Forschungsfeld existierenden Szenarien.⁴⁰⁷

Da durch die Techniken der allgegenwärtigen Datenverarbeitung alle Lebensbereiche erfasst und verknüpft sein sollen, sind vorstellbare Technikanwendungen dieser Vision in typische Alltagssituationen unterschiedlicher Zusammenhänge eingebettet. Um sich die Welt des „Ubiquitous Computing“ besser vorstellen zu können, ist eine Szenariotechnik gewählt worden, die am Beispiel eines handelnden Protagonisten das Leben in einer solchen Umgebung der allgegenwärtigen Datenverarbeitung beschreibt.

2.3.2.2 Grenzen der vorgestellten Szenariodarstellung

Das heißt aber auch, dass die gewählte Szenariendarstellung an ihre Grenzen stößt, wenn es um gesellschaftliche Veränderungen oder gar Machtverschiebungen durch die neuen Techniksysteme geht. Zum einen kann die Einführung neuer Techniken die Bedingungen in einer Gesellschaft so verändern, dass dadurch die Grundlagen für das Interessengefüge der Akteure beeinflusst werden. Auf der anderen Seite können ebenso unerwartete Entwicklungen, völlig neue, unbedachte Verwendungsweisen und Nutzungsformen der Techniksysteme entstehen, mit denen Veränderungen der Gesellschaft als sozio-ökonomisches System einhergehen.

Diese möglichen Interessengegensätze und Machtverschiebungen in der Gesellschaft sind zwar im vorgestellten Szenario angelegt, können aber nicht explizit herausgearbeitet werden. Das Szenario greift bisher in Industrieländern gewohnte Lebensbedingungen auf. Jedoch könnten beispielsweise öffentliche Büchereien, das Lesen von papierbasierten Schriftstücken, Konferenzen mit körperlicher Anwesenheit der Beteiligten, Lebensmittelgeschäfte mit in Regalen ausgelegter Ware oder ein von privaten Kraftfahrzeugen dominierter Individualverkehr mit großer verkehrstechnischer Infrastruktur der Vergangenheit angehören. Ebenso wenig ist es möglich, Geschäftsmodelle zu identifizieren, die sich in der künftigen Welt des „Ubiquitous Computing“ durchsetzen werden.

Zum anderen zeigen die Szenarienpassagen einen Nutzer, der technisch interessiert und medienkompetent mit der Technik umzugehen weiß. Auch wenn der Blickwinkel im vorgestellten Szenario nutzerzentriert ist, muss man sich bewusst sein, dass in einer Welt des „Ubiquitous Computing“, gerade auch bei den Auto-ID-Verfahren, der einzelne Betroffene oft den Techniksystemen mehr als passives Objekt denn als handelndes Subjekt gegenübersteht. Daneben gestaltet sich die Bildung von Anwendungsbeispielen schwierig, auch wenn man sich an sich abzeichnenden Techniktrends orientiert. Zum einen existieren viele der im „Ubiquitous Computing“ überlegten Technologien und Techniksys-

⁴⁰⁷ S. näher *Coroama*, in: *ders. u.a.* 2003, 2 f., 7 f.; *Roßnagel* 2007b, 71 f.

teme noch gar nicht. Zum anderen stellt „Ubiquitous Computing“ selbst nur eine Idee oder Vision einer informatisierten Welt dar, die durch konkrete Technikanwendungen erst noch Gestalt annehmen will.

2.3.2.3 Ausrichtung der vorgestellten Szenariodarstellung

Für eine datenschutzrechtliche Betrachtung kommt es allerdings, wie oben erörtert, letztlich auf die konkrete Technologie nicht an, mit der IuK-Anwendungen realisiert werden. Von Interesse ist vornehmlich das technische Konzept, das in seiner Ausgestaltung auf Verwirklichungsbedingungen von Rechtsgütern einwirkt. Daher werden im Folgenden in (fiktiven) Szenarien erdachte, paradigmatische Anwendungsbeispiele denkbarer Techniksysteme beschrieben, bei denen das Interesse auf den Umstand gerichtet ist, wo und in welcher Weise Datenspuren entstehen und verwendbar sind. Für die weitere datenschutzrechtliche Betrachtung werden anschließend bestimmte, typische Anwendungsbeispiele aufgegriffen, deren Realisierung durch die Technik der „Radio Frequency Identification“ möglich und nicht völlig abwegig erscheint.

2.3.2.4 Beteiligte und Ressourcen

Im folgenden Szenario könnten Claudia und Alfonso Menschen sein, die beispielsweise als Angestellte eines im Dienstleistungssektor tätigen Unternehmens und als Eltern von schulpflichtigen Kindern in ihrem privaten und beruflichen Alltag die Möglichkeiten der neuen Techniksysteme nutzen. Hierfür verwenden sie eine tragbare IuK-Einheit, die es ihnen erlaubt, über drahtlose Netzwerkverbindungen auf andere Informationsangebote zuzugreifen, mit anderen Personen zu kommunizieren, mit anderen Geräten Daten auszutauschen sowie Daten zu verwalten und zu bearbeiten. Diese Einheit ermöglicht ihnen, sich Informationen in optischer, akustischer oder taktiler Form wahrnehmbar zu machen, wenn die jeweilige Umgebung nicht ohnehin direkte Interaktionsmöglichkeiten anbietet, etwa durch Multimodale Interaktion mit dem Umgebungsmodell (z.B. durch Zeigegesten).

Eine solche IuK-Einheit könnte ein Kleinstrechner mit Anzeige und Lautsprechern (z.B. PDA oder Smartphone) sein. In der Zukunft ist durchaus vorstellbar, dass der Rechner im Taschenformat durch eine Anzeige und ein Bedienfeld auf dem Jackenärmel, durch eine akustische Ausgabe mittels Ohrring und eine zentraleessoreinheit in der Gürtelschnalle ersetzt wird.⁴⁰⁸ Die Eingabe könnte neben herkömmlichen Tastaturen, Zeigegeräten (Maus, Steuerknüppel, Stift) oder berührungsempfindlichen Anzeigen, auch über gesprochene Sprache, Gestik oder Blick der Augen erfolgen. Als weitere Ausgabemedien könnten Brillen Verwendung finden, bei denen das optische Bild direkt auf die Netzhaut des Auges projiziert wird, oder Anzeigeeinheiten eingesetzt werden, durch die

⁴⁰⁸ Zu I-Wear und sogar der Vision der digitalen Aura – vgl. *Behrendt/Erdmann/Würtenberger*, in: TA SWISS 2003, 97.

das optische Bild auf Flächen beliebiger Gegenstände in der Umgebung des Nutzers projiziert wird.

Viele der Möglichkeiten im Kontext allgegenwärtiger Datenverarbeitung werden durch Anwendungen zur Verfügung gestellt, die in der Navigation im Außen- und Innenraum, in der Aufbereitung und dem teilautonomen Verarbeiten von Informationen (wie Streunachrichten, Reise-, Termin- und Ereignisinformationen) oder in der Planung von Ressourcen (wie das Verkehrsleitsystem in der Innenstadt, die Vergabe von Sitzplätzen oder von Mitfahrgelegenheiten), aber auch in der Verwaltung von Gegenständen (wie das Einkaufsunterstützungs- und das Büchereibestellsystem) bestehen. Dabei greifen viele der Anwendungen auf Funktionen eines oder mehrerer Dienste zurück, die Daten zu registrierten Gegenständen, drahtlose Kommunikation (dezentral wie auch zentral), Lokalisierungsdienste und Ereignisüberwachung sowie Auswertung von Kontextdaten und weiteren Datenbeständen entsprechender Datenbanken bereitstellen.

Zu der Erbringung dieser Dienste werden Techniksysteme benötigt, die oft ausgebaute technische Infrastrukturen voraussetzen. Es zählen Dienste der Positionsbestimmung durch Satelliten- oder Funksignale oder Dienste der Kommunikation durch Verfahren der Ad-Hoc-Kommunikation, Informationsdiffusion oder über drahtlose Netze im GSM-, UMTS-, LTE- oder IEEE 802.11-Standard dazu. In und an den Gebäuden (z.B. Konferenzräumen oder Haushalten) müssen wichtige Elemente des Gebäudes und der Innenausstattung mit Sensoren und Aktoren (von Fenster-, Türschließ-, Beleuchtungs- oder Heizungsanlagen bis hin zu Kaffeemaschine oder Stühlen) sowie mit Rechnersystemen ausgestattet sein, die Kommunikationsschnittstellen zu anderen IuK-Einheiten besitzen. Aber auch Sensortechnik in anderen Gegenständen und Auto-ID-Verfahren, wie der RFID-Technik, werden zur Registrierung von Umweltbedingungen und Gegenständen eingesetzt werden.

Die nachfolgend beschriebenen Anwendungen nutzen die Möglichkeiten von RFID-Systemen, die im Abschnitt 2.2 typisiert dargestellt sind. Allerdings gehen die angesprochenen Anwendungsbeispiele von einer verbesserten Einsatzfähigkeit und einer ausgebauten Infrastruktur aus, die heute so noch nicht existiert und realisierbar ist. Um nachfolgend beschriebene oder ähnliche Anwendungen umzusetzen, müssen physikalisch bedingte und technische Schwierigkeiten gelöst oder das technische Konzept der RFID-Technik modifiziert werden. Dennoch ist vorstellbar, dass unter Verwendung von Auto-ID-Verfahren, wie die der RFID-Technik, die beschriebenen Anwendungsbeispiele eingeführt werden.

2.3.2.5 Szenarische Darstellung eines Tages von Claudia und Alfonso

Claudia hat heute einen Geschäftstermin in einer anderen Stadt und macht sich im Morgengrauen mit dem vorreservierten Kraftfahrzeug einer PKW-Genossenschaft auf den Weg zum Hauptbahnhof. Da die Straßenverhältnisse wegen überfrierender Nässe eine längere Fahrzeit erwarten lassen, wurde sie von ihrem Hausleitsystem, das nicht nur Heizung, Beleuchtung und Küchenge-

räte energieoptimiert steuert, früher als ursprünglich geplant, geweckt. Entsprechend früher hat die Teemaschine den Tee bereitgestellt.⁴⁰⁹

Am digitalen Briefkastenschild, hinterlässt sie für den Postboten, der eine Zustellung einer größeren Sendung angekündigt hat, einen – nur für ihn – lesbaren Hinweis über den Ersatzzustellort, einschließlich einer entsprechenden Vollmacht. Ihre Restmülltonne wird heute dem vorbeifahrenden Abfallsorgungsfahrzeug signalisieren, dass eine Leerung aufgrund ihrer Füllmenge erforderlich ist.

Bei der Fahrt zum Bahnhof lässt sich Claudia durch ihr im Fahrzeug eingebautes Navigationssystem leiten. Als sie auf der Stadtautobahn, im Bereich einer Abfahrt, auf einen Stau zufährt, drosselt das Fahrzeug frühzeitig seine Geschwindigkeit, da vorausfahrende Fahrzeuge entsprechende Verkehrssituationen übermitteln.⁴¹⁰ In der Innenstadt wird sie durch das städtische Verkehrsleitsystem, das neben der Mautabrechnung auch Verkehrsflusinformationen an die Navigationssysteme der Kraftfahrzeuge übermittelt, auf eine Alternativroute umgeleitet und zu einem freien Parkplatz nahe des Bahnhofs geführt. Standort des abgestellten Personenkraftwagens sowie die notwendigen Abrechnungsdaten werden an die Geschäftsstelle der PKW-Genossenschaft automatisch übermittelt.⁴¹¹

Als Claudia in die Nähe des Bahnhofsgebäudes gelangt, erhält sie gemäß ihrer Präferenzen Informationen der virtuellen Zugzielanzeige mit aktualisierten Ist-Ankunftszeit und Gleis- und Wagenstandsangaben ihres Zuges. Diese, sowie weitere sich automatisch aktualisierende Informationen zu erreichbaren Umsteigemöglichkeiten, sind über ihre LuK-Einheit verfügbar.⁴¹²

Claudia hatte sich mit ihrem Arbeitskollegen, Alfonso, der ebenfalls zu der Konferenz fährt, im Bahnhofsgebäude verabredet. Sie fragt einen Ortsdatendienst ab, wo sich Alfonso gerade befindet. Dadurch erfährt sie, dass ihr Kollege mit dem öffentlichen Personennahverkehr in Kürze eintreffen wird. Daraufhin aktiviert Claudia einen Ereignisdienst, über den Alfonso eine Mitteilung beim Betreten des Gebäudes elektronisch erhält, in der sie ihm einen gemeinsamen Treffpunkt, in einem noch vom Bahnhofinformationssystem zu bestimmenden Gleisabschnitt, vorschlägt bzw. sich vorschlagen lässt.

Da bis zur Abfahrt des Zuges noch Zeit bleibt, wird Claudia vom Bahnhofsinformationssystem nicht sofort zum Abfahrtsgleis geleitet, sondern über Gestaltungsmöglichkeiten während der Wartezeit informiert, die anhand der Zielgruppenanalyse durch das Einlass- und Videoüberwachungssystem gefiltert sind. Beim Weg zur Wartehalle macht der um die Ecke liegende Zeitungsladen durch „spontane“ Mitteilung an Claudia auf sich aufmerksam. Da sie ihre Tageszeitung, abhängig von ihrem Lesebedarf, in elektronischer Form abonniert hat,

⁴⁰⁹ Hansen/Fabian/Klafft, in: Bizer/Spiekermann u.a. 2006, 48; BSI 2006, 23.

⁴¹⁰ BSI 2006, 83; Hansen/Fabian/Klafft, in: Bizer/Spiekermann u.a. 2006, 191.

⁴¹¹ S. Abschnitt 2.1.3; BSI 2006, 86.

⁴¹² Magerkurth, in: Coroama u.a. 2003, 87.

geht sie weiter in Richtung Wartehalle, um dort einen zuvor über das Umgebungsinformationssystem ermittelten Backwarenstand aufzusuchen. Als Claudia eine Gruppe von Jugendlichen passiert, schnappt sie einen digitalen Hinweis einer in der Nachbarschaft zum Bahnhofsgebäude gelegenen Bäckerei auf, die, so die beigefügte Notiz eines Kunden, gut durchgebackenes fränkisches Bauernbrot als Sonderangebot offeriert. Die Information wurde durch das luK-Gerät eines der Jugendlichen weitergetragen und an empfangsbereite luK-Einheiten anderer Passanten gestreut.

Auf dem Rückweg vom anvisierten Backwarenstand entschließt sich Claudia, eine Illustrierte in herkömmlicher Papierform zu besorgen. Die von ihr ausgewählte Zeitschrift ist zwar noch im gewohnten Schwarzschriftdruck, dennoch sind Anzeigen und viele Beiträge um digitale Hinweise ergänzt, die auf integrierte Datenträger abgelegt sind und über die luK-Einheit des Lesers weiterverwendet werden können. Nachdem das Auslagenregal die Entnahme der betreffenden Zeitschrift registriert, wickelt der Zeitschriftenvertrieb den Bezahlvorgang über das Regal mit Claudias luK-Einheit ab, die für automatisierte Transaktionen von Kleinbeträgen freigeschaltet ist.

Auf dem Weg zum Bahnsteig fällt ihr ein Veranstaltungsplakat auf. Um dessen Veranstaltungshinweise jetzt nicht vollständig lesen zu müssen, ruft sie die am Plakat vorgehaltenen digitalen Informationen ab. Diese enthalten auch eine Internetadresse zu dem Buchungsportal, über das Eintrittskarten unter Verwendung der Veranstaltungsdaten reserviert oder gebucht werden können.

Auf dem Bahnsteig trifft Claudia ihren Kollegen Alfonso. Gemeinsam besteigen sie den eingefahrenen Schnellzug. Beim Passieren der Wagentür werden ihnen durch das Zuginformationssystem zwei freie Sitzplätze im Nachbarwagen zugewiesen, zu denen sie durch ein kleines Innenraumnavigationssystem geleitet werden. Wenn man nicht vorbuchen möchte, kann auch die Buchung des Zuges und Abrechnung der Leistung beim Ein- und Aussteigen automatisch erfolgen.⁴¹³

Während der Fahrt ergibt sich eine Abweichung vom Fahrplan. Diesen Umstand gibt das Zuginformationssystem an die kommunikationsbereiten luK-Einheiten der Fahrgäste weiter. Daraufhin generiert das von Alfonso mitgeführte luK-Gerät Vorschläge möglicher Handlungsoptionen. Alle vorgeschlagenen Möglichkeiten, wie Suche einer alternativen Reiseverbindung, Mitteilung an das Sekretariatssystem des Geschäftspartners verwirft Alfonso.

Am Zielbahnhof angekommen, möchte sich Alfonso mittels Abfrage der verschiedenen Informationsportale, einen Überblick verschaffen, welche öffentlichen und privaten Verkehrsmittel, wann, wo und zu welchem Preis zum Konferenzort zur Verfügung stehen. Das gelingt aber nicht. Deshalb ruft er ein Taxi, dem durch die Buchungsanfrage sein Standort und gegebenenfalls besondere Kundenwünsche mitgeteilt werden. Alfonso erhält eine bestätigende Rückmel-

⁴¹³ Hansen/Fabian/Klafft, in: Bizer/Spiekermann u.a. 2006, 56.

derung mit Daten über voraussichtliche Wartezeit und Koordinaten des genauen Anfahrtpunktes zum Zusteigen.⁴¹⁴

Am Tagungsort erhalten Claudia und Alfonso im Empfangsbereich, der mit einer animierten, einem Menschen nachgebildete Gestalt (Avatar) besetzt ist, ihre Namensschilder. Mit Hilfe derer wird ihnen Zutritt zu den Tagungsräumlichkeiten und zur Kantine gewährt. An einer virtuellen Litfaßsäule lassen sie sich die Konferenzunterlagen überspielen. Den Konferenzraum finden sie mittels des Umgebungsinformationssystems, das für dieses Gebäude angeboten wird. An der Tür ist ein elektronisches Türschild angebracht, das über Raum und Veranstaltung informiert. Es ist einer der modernen Konferenzräume, die nicht nur mit multimedialer Präsentationstechnik ausgestattet sind, sondern durch Sensortechnik erkennen, ob und welche Besprechung in diesem Raum stattfindet. Dadurch können in Räumlichkeiten Parameter der Raumtechnik, wie Beleuchtung und Klimatisierung voreingestellt, der Raumbesetzung im Umgebungsinformationssystem eingetragen, aber auch Zugangsberechtigungen zum Intranet oder digitale Dokumente vorangegangener Sitzungen bereitgestellt werden.⁴¹⁵

Die Präsentationstechnik erlaubt zum einen die Projektion von digitalen Dokumenten von jedem Platz aus, auf eine für alle sichtbare Tafel oder Projektionsfläche. Zum anderen können an dieser Tafel mit Hilfe von Zeigegeräten, die einem Stift nachgebildet sind, angezeigte Dokumente direkt verändert oder solche direkt erstellt werden. Für kleinere Arbeitsgruppen stehen Tische zur Verfügung, an denen jeder Teilnehmer, von seiner jeweiligen Sitzposition aus, an gemeinsamen digitalen Zeichnungen und Dokumenten arbeiten kann.⁴¹⁶

Claudia und Alfonso benutzen während der Besprechung für die Mitarbeit an den gemeinsam zu erarbeitenden Konzeptsdokumenten und für eigene Notizen jeweils kleine Geräte, die in diesem Besprechungsraum bereitliegen. Dadurch soll aus Sicherheitsgründen die Verwendung von un zertifizierten, mitgebrachten Geräten vermieden werden. Am Ende der Besprechung werden ihre Daten an ihre angegebenen digitalen Postfächer überspielt und diese Daten einschließlich ihrer Arbeitskonfigurationen auf den kleinen Geräten gelöscht. Bei Mitnahme dieser Geräte aus dem Konferenzraum würden die Daten auf ihnen ebenfalls gelöscht und die Geräte deaktiviert werden.

Im Laufe der Besprechung stößt ein langjähriger Geschäftspartner von Claudia und Alfonso, Alireza zu ihrer Runde und begrüßt alle Anwesenden mittels einer geographisch platzierten Nachricht, um das im Gange befindliche Gespräch nicht unnötig zu stören. Er lädt sie zu einem Mittagessen mit anschließendem Rundgang durch eine neu gebaute Produktionsstraße ein. Am Ende der Konferenz verabschieden sich die Teilnehmer voneinander. Claudia tauscht

⁴¹⁴ Müller, in: *Coroama u.a.* 2003a, 61.

⁴¹⁵ Müller, in: *Coroama u.a.* 2003a, 56 f.

⁴¹⁶ S. hierzu bereits Müller, in: *Coroama u.a.* 2003a, 56 f.

mit einem neuen Geschäftspartner noch ihre Kontaktdaten aus, indem sie ihre mitgeführten LuK-Geräte kurz miteinander, gleich eines Handschlages, schütteln, um dadurch den Datentransfer der Geräte anzustoßen. Claudia und Alfonso begeben sich mit dem Geschäftsfreund Alireza zur Kantine, in der sie aufgrund ihres Namensschildes als Gäste von Alireza bedient werden.⁴¹⁷

In dem Fabrikgebäude, das sie gemeinsam besichtigen, produzieren Arbeiterinnen und Arbeiter hochwertige Maschinenbauteile. Dabei sind sie mit Brillen und Arbeitskleidung ausgerüstet, in die eine Rechneranzeige und Bedienelemente am Jackenarm einschließlich einer Kommunikationseinheit eingewebt sind.⁴¹⁸ In Begleitung ihres Geschäftsfreundes erhalten Claudia und Alfonso Zutritt zu dem speziell gesicherten Kontrollzentrum der Werkshalle, von dem aus sie einen guten Überblick haben. Sie sehen, wie ein Transportroboter ein frisches Werkzeug bringt und ein verschlissenes Teil autonom abholt. Ein Arbeiter benötigt ein Spezialwerkzeug, das er aber nicht im Zentrallager holt, sondern bei der Kollegin an der Nachbarwerkbank.⁴¹⁹

Um im Investitionsgütermarkt, der von Einzel- und Kleinserienfertigung, maßgeschneiderten Kundenlösungen bei geringer Losgröße und großer Variantenzahl gekennzeichnet ist, die Maschinenbauprodukte mit dem hohen Individualisierungsgrad fertigen zu können, ist es notwendig, so erklärt Alireza, eine Vielzahl hochspezialisierter, für einzelne Bearbeitungsaufgaben angepasste Werkzeuge und Vorrichtungen einzusetzen. Gerade die Abstimmung des laufenden Produktionsprozesses mit den komplexen Kreisläufen der Betriebs-, Prüf- und Verbrauchsmittel, wie Werkzeuge oder Fräsen, von ihrer Lagerung, Transport, Handhabung bis hin zu ihrer neuerlichen Instandsetzung, ist schwierig zu steuern. Deshalb sind hier alle Werkstücke, Werkzeuge und Vorrichtungen elektronisch gekennzeichnet und in der Werkshalle ortbar. Maschinen mit Sensorik sind so ausgerüstet, dass ihr Wartungszustand, ihre Auslastung, Konfiguration oder das aktuell bearbeitete Werkstück im Betriebsinformationssystem in Echtzeit abrufbar sind.⁴²⁰

Auf der Rückreise sehen Claudia und Alfonso die ihnen bereits zugegangenen Besprechungsprotokolle durch und bearbeiten ihren dienstlichen Schriftverkehr. Claudia erhält eine Nachricht vom Informationssystem des Schulhortes, dass ihre Kinder nach Hause aufgebrochen sind. Als der Zug in den Zielbahnhof einfährt, überprüfen Claudia und Alfonso den Inhalt ihrer Aktentaschen auf Vollständigkeit. Mit einem Blick auf eine Kontrollanzeige in der Schnalle erkennen sie, dass auch alle ausgepackten Gegenstände, von Schriftstücken, Stiften bis zum Rechner, auch wieder eingepackt sind.

Wieder in der Heimatstadt angekommen, verabschieden sich Claudia und Alfonso. Alfonso macht sich auf den Nachhauseweg. Unterwegs geht er noch

⁴¹⁷ Hansen/Fabian/Klafft, in: Bizer/Spiekermann u.a. 2006, 58.

⁴¹⁸ Roßnagel 2007b, 75.

⁴¹⁹ Roßnagel 2007b, 75.

⁴²⁰ Roßnagel 2007b, 78.

bei der städtischen Bücherei vorbei und holt dort, die auf der Rückfahrt im Zug vorbestellten Bücher ab. Für den weiteren Weg möchte Alfonso eine Mitfahrgelegenheit oder ein Mietfahrrad benutzen. Dafür setzt er über sein mitgeführtes Mobilgerät eine Anfrage ab, ob passende Angebote mietbarer Stadtfahrräder oder Mitfahrgelegenheiten angemeldet sind, die sich gerade in der Nähe des Anfrage-Standortes bewegen. Alfonso wird auf dem Umgebungsplan, der mittels seines Mobilgeräts zugreifbar ist, ein Standort angezeigt, an dem ein mietbares Stadtfahrrad abgestellt wurde. Um das Schloss des betreffenden Fahrrades freizuschalten, übermittelt er die Registriernummer des Fahrrades an das Verwaltungssystem. Daraufhin wird per Funksignal das Schloss entriegelt und Alfonso kann seinen Nachhauseweg fortsetzen. Die Abrechnung erfolgt von seinem Bankkonto anhand der Kilometerstands- und Positionsdaten des Fahrrades über das Verwaltungssystem.

Claudia muss noch Einkäufe des täglichen Bedarfs erledigen, da sie am Abend Besuch erwartet. Diesen will sie später an einem kleinen Vorstadtbahnhof abholen. Zunächst fährt sie bei einem Einkaufszentrum vorbei, bei dem die Ladengeschäfte ihre Waren in klassischen Auslageregalen feilbieten. Allerdings sind die Ladengeschäfte mit einem Einkaufsunterstützungssystem ausgerüstet.⁴²¹ Über eine kleine Anzeige am Einkaufswagen oder über eine mobile IuK-Einheit des Kunden lässt sich dieses Informationssystem nutzen. Claudia überspielt die Liste ihres digitalen Einkaufszettels an das ladeneigene Einkaufsunterstützungssystem und geht durch die Regalreihen, um die vermerkten Produkte in ihren Einkaufswagen zu legen. Beim Durchschieben durch die Regalreihen werden immer wieder auf der Anzeige des Einkaufswagens Hinweise eingeblendet, die Sonderangebote, die nicht auf der Einkaufsliste notiert waren, anpreisen.

Als Claudia ein Produkt aus dem Regal in die Hand nimmt, aber zögert, es in ihren Wagen zu legen, bietet ihr das Einkaufsunterstützungssystem einen Sonderpreis an, der gilt, wenn sie ein hierzu passendes Ergänzungsprodukt mit erwirbt. Unter den Angeboten ist auch ein sonst hochpreisiges Meeresfrüchteprodukt, dessen Mindesthaltbarkeitsdatum sich wegen kurzzeitiger schlechter Kühlung auf dem Transportweg verkürzt. Deshalb wurde der Verkaufspreis herabgesetzt. Claudia kauft dieses Produkt, ruft gleichzeitig vom Einkaufsunterstützungssystem Vorschläge für dessen Zubereitung ab. Sie wählt einen Kochrezeptvorschlag aus und lässt sich mittels des ladeneigenen Informationssystems über Richtungssymbole auf der Wagenanzeige zu den fehlenden Zutaten führen. Das Kochrezept wird allen betreffenden Produkten elektronisch angeheftet.

⁴²¹ S. Abschnitt 2.1.3; *Magerkurth*, in: *Coroama u.a.* 2003, 20 f.

Nach Abschluss des Einkaufs in diesem Ladengeschäft braucht Claudia keinen Kassenbereich mehr zu passieren, da die Abrechnung sofort erfolgte, sobald die Produkte in den Einkaufswagen eingelegt wurden. Ein späteres Zurücklegen der bereits erworbenen Produkte wird gleichfalls auf der sich stets aktualisierenden Rechnung berücksichtigt.⁴²²

Danach besucht Claudia noch ein benachbartes Ladengeschäft für Textilwaren. Als sie vor dem Spiegel einen Hosenrock prüft, wird ihr in einem Spiegelausschnitt eine Videosequenz eingespielt, die sie bekleidet mit der anprobieren Kollektion animiert in einer Naturszene zeigt. Des Weiteren werden im Spiegel weitere kombinierbare Kleidungsstücke eingeblendet, um deren Wirkung in Verbindung mit dem betreffenden Hosenrock an ihr vorzustellen.⁴²³ Claudia möchte das anprobierbare Kleidungsstück mit nach Hause nehmen. An der Kasse wird es ihr eingepackt und sie initialisiert über ihre LuK-Einheit die elektronische Zahlungsabwicklung.

Auf dem Weg zum Parkplatz kommt Claudia an einem Informationsstand vorbei, bei dem in Regalen Informationsmaterial ausgelegt ist. Sie nimmt die Gelegenheit wahr, in einigen Prospekten zu blättern. Ein paar von diesen steckt sie für zu Hause ein.

2.4 Potentiale und Risiken des Einsatzes von RFID-Systemen durch ihre technischen Charakteristika

Durch die Darstellung der Möglichkeiten der RFID-Technik in Szenarien⁴²⁴ und Anwendungsbeispielen⁴²⁵ sowie ihrer technischen Funktionsweise⁴²⁶ ist einerseits deutlich geworden, welches wirtschaftliche Potential in RFID-Systemen als einer der Auto-ID-Verfahren zu sehen ist, andererseits aber auch welche Befürchtungen von Verbraucher- und Datenschützern⁴²⁷ mit deren Einsatz verbunden werden.

Im Folgenden wird aufgezeigt, welche datenschutzrechtlich relevanten Folgen sich aus diesen technisch bedingten Möglichkeiten ableiten lassen. Daher erfolgt zuerst eine Darstellung der Verwendungsmöglichkeiten eines RFID-Systems ebenfalls in typisierter Weise, die sich aus den technischen Charakteristika eines solchen Systems ergeben.⁴²⁸ Zudem wird auf wichtige Ansatzpunkte möglicher technischer Angriffe eingegangen.

⁴²² Magerkurth, in: *Coroama u.a.* 2003, 21.

⁴²³ S. Abschnitt 2.1.3.

⁴²⁴ S. Abschnitt 2.3.2.

⁴²⁵ S. Abschnitt 2.1.3.

⁴²⁶ S. Abschnitt 2.2.

⁴²⁷ S. Abschnitt 2.5.

⁴²⁸ Ausführlich dazu Abschnitt 2.2

2.4.1 Technisch bedingte Verwendungsmöglichkeiten der RFID-Systeme

Aus den technischen Merkmalen von RFID-Systemen lassen sich bestimmte Verwendungsmöglichkeiten ableiten. Die Kommunikation über die Luftschnittstelle ermöglicht nicht nur ein Auslesen und Beschreiben der RFID-Marke über eine gewisse Distanz. Vielmehr erfolgt die Kommunikation mit den RFID-Marken, anders als bei dem herkömmlichen Strichcode, ohne jeden Sichtkontakt. Da hierbei zudem mit Vielfachzugriffsverfahren gearbeitet wird, sind RFID-Marken im Ansprechbereich des Lesegeräts im Verhältnis zu anderen Identifikationstechniken in großer Anzahl, einfach, schnell und nahezu gleichzeitig auslesbar.

Auf der einen Seite kann auf RFID-Marken auch ohne Sichtkontakt zugegriffen werden. Auf der anderen Seite bleiben solche Zugriffe durch die RFID-Marke unregistriert. Zur Kontrolle, ob durch das RFID-Lesegerät aktuell Kommunikationsvorgänge stattfinden, fehlen RFID-Marken gesonderte Ausgabemedien. Auch nachträglich lässt sich ein erfolgter Kommunikationsvorgang in Ermangelung einer Zugriffsprotokollierung auf der RFID-Marke nicht feststellen. Des Weiteren fehlen auf RFID-Marken, außer bei denen der hohen Leistungs-klasse, meist Schutzmechanismen, die die RFID-Marke vor dem Detektieren durch das Lesegerät (Zugangsschutz) oder die Daten vor dem Auslesen und Verändern (Zugriffsschutz) wirkungsvoll schützen.

Dies bedeutet, dass Daten der RFID-Marke sowohl in Form der Identifikationsnummer als auch der weiteren Nutzdaten unabhängig von Berechtigungen zugänglich sind und offen liegen. Dies gilt ebenso für die Kommunikation zwischen der RFID-Marke und dem Lesegerät, da auch hier meist keine Schutzvorkehrungen, wie etwa Verschlüsselung, wie oben bereits dargestellt, vorgesehen sind. Allerdings ist die Reichweite der RFID-Kommunikation auf verhältnismäßig kurze Distanzen beschränkt, so dass diese in einem räumlich begrenzten und abgrenzbaren Bereich stattfindet.

Infolge der extrem kleinen Baugrößen von RFID-Marken wird die Verbindung mit fast jedem Gegenstand möglich. Sie lassen sich in einer Weise platzieren, dass sie unbemerkt bleiben. Trägermaterialien und Gehäuse aus modernen und hochflexiblen Werkstoffen erlauben es, wie angesprochen, RFID-Marken nicht nur an Gegenstände anzuheften, sondern auch, sie in diese zu integrieren. Dabei können die Marken durchaus unlösbar mit dem Gegenstand verbunden sein. Da sie je nach Bauform eine hohe Widerstandsfähigkeit gegenüber äußeren Umwelteinwirkungen aufweisen und insbesondere passive RFID-Marken ohne eine eigene Energiequelle auskommen, sind sie hinsichtlich Wartung und Instandsetzung ohne große Infrastruktur zu betreiben und von langer Lebensdauer.

Neben den materiellen Bedingungen des RFID-Einsatzes sind vor allem die technischen Merkmale wichtig, die die Funktion als Auto-ID-Technik bestimmen. Über die Identifikations- oder Seriennummer auf den RFID-Marken lässt sich jede einzelne RFID-Marke im Ansprechbereich des Lesegeräts detektieren, selektieren und verwalten. Diese RFID-Seriennummer ermöglicht es, durch ihre Einmaligkeit, eine RFID-Marke weltweit zu identifizieren. Dadurch wird auch der

Gegenstand eindeutig identifizierbar, mit dem die betreffende RFID-Marke verbunden ist.

Wenn nun die Identifikationsnummer der RFID-Marke Informationen in codierter Form enthält oder auf der RFID-Marke in weiteren Speicherbereichen zusätzliche Daten abgelegt sind, dann hat ein RFID-Lesegerät Daten verfügbar, die eine höhere Aussagekraft als das bloße Identifikationsdatum besitzen. Sollten diese Daten nicht in irgendeiner Weise verschlüsselt sein, gäben sie abhängig von den RFID-Anwendungen, für die die RFID-Marke bestimmt ist, Auskunft über den betreffenden Gegenstand selbst, seinen Bestimmungszweck, über den Inhaber oder über andere Umstände.

Dies bedeutet, dass ohne weiteren Zugriff auf ein Hintergrundinformationssystem je nach Informationsgehalt der Daten Aussagen über den Gegenstand getroffen werden können und ihm eine Art inhaltliche Identität zuwächst. Dagegen ermöglicht es ein Hintergrundinformationssystem, unbegrenzt Daten zu der jeweiligen RFID-Marke abzuspeichern, zu verwalten und auszuwerten. In diesem Hintergrundinformationssystem könnten Daten über den Gegenstand abgelegt werden, mit dem die RFID-Marke verbunden ist, Daten der RFID-Lesegeräte gesammelt und mit Daten über die Umstände der Auslesesituation verknüpft werden.

Dadurch stehen bei Zugriff auf ein solches Informationssystem mittels der Identifikationsnummer der RFID-Marke beliebig generierbare Zusatz- und Kontextdaten zur Verfügung, die die RFID-Marke und ihren Gegenstand betreffen. Des Weiteren könnten über das Hintergrundinformationssystem weiterführende Dienste abgewickelt werden.

2.4.2 Folgen durch die Verwendungsmöglichkeiten von RFID-Systemen

Die Gesamtschau der Verwendungsmöglichkeiten, die durch die technischen Merkmale von RFID-Systemen bestimmt werden, lässt Folgen erkennen, die datenschutzrechtlich relevant sein können. Die Vision des „Ubiquitous Computing“ ist hauptsächlich dadurch gekennzeichnet, dass Rechenleistung und Kommunikationsmöglichkeiten allgegenwärtig, aber auch unmerklich in Alltagsgegenständen vorhanden sind.

Die RFID-Technik könnte als eine der Auto-ID-Techniken allgegenwärtig präsent sein, indem sie nicht nur in geschlossenen Betriebsabläufen, sondern auch in den Alltag der Menschen Einzug hält und in vielen verschiedenen Lebensbereichen eingesetzt wird. Dies wird dadurch begünstigt, dass zum einen das Auslesen der RFID-Marken in großer Anzahl, einfach, schnell und nahezu gleichzeitig und zum anderen die RFID-Markierung verhältnismäßig langlebig, infrastrukturarm und unempfindlich gegenüber äußeren Umwelteinwirkungen möglich ist.

Daneben führen gerade die technischen Merkmale der RFID-Technik zu der Möglichkeit, Gegenstände in eine virtuelle Welt unmerklich einzubinden und dort abzubilden. Wenn RFID-Marken mit Gegenständen verbunden, unbemerkt an und in ihnen platziert und auch unlösbar integriert werden können, dann tritt diese Technik in den Hintergrund und ist unmerklich vorhanden. Aber sichtkon-

taktlose Auslesbarkeit bedeutet nicht nur, dass auch die notwendige Infrastruktur durch Lesegeräte in Umgebungselementen unmerklich aufgestellt sein kann, vielmehr können Kommunikationsvorgänge unmerklich stattfinden.

Dabei verhindert die Unkontrollierbarkeit stattfindender Kommunikationsvorgänge, dass sich ein Besitzer eines RFID-markierten Gegenstandes dessen bewusst ist und so die Situation im aktuellen Kommunikationszeitpunkt sowie eventuelle Reaktionsmöglichkeiten nicht abzuschätzen vermag. Wegen der fehlenden Möglichkeit, durch die RFID-Marke erfolgte Kommunikationsvorgänge zu kontrollieren, lässt sich auch nachträglich nicht erschließen, ob eine RFID-Marke durch das Feld eines Lesegeräts erfasst und ob weitere Zugriffe auf Daten durchgeführt wurden. Zeitpunkt und Umstände der Kommunikationssituation bleiben in allen Fällen aus der Perspektive der RFID-Marke im Dunkeln. Letztlich ist die Erfassung von RFID-Marken und ihre Auslesbarkeit durch Lesegeräte und damit auch die Identifikation von Gegenständen von der Konzeption der RFID-Technik her nicht kontrollierbar.

RFID-Marken werden über das vom Lesegerät erzeugte elektromagnetische Feld mit Energie versorgt und gesteuert. Sie sind passiver Teil des Kommunikationsvorgangs. Dadurch kommt einem mit RFID-Marken versehenen Gegenstand im Rahmen einer RFID-Kommunikation lediglich die Position zu, ein Objekt der Datenverwendungs- und Identifikationsvorgänge zu sein.

Darüber hinaus wird über eine RFID-Infrastruktur mit Lesegeräten, möglicherweise ergänzt um ein Hintergrundinformationssystem, nicht nur erkennbar, ob der RFID-markierte Gegenstand sich im Ansprechbereich des Lesegeräts befindet, sondern auch wie mit ihm agiert wird. Die RFID-Technik ist in einer Weise mit dem Gegenstand unmerklich und unbeeinflussbar verbunden, dass sie sich in seinen Gebrauch integriert.

Vermittelt über den markierten Gegenstand wird das Verhalten und Handeln des Besitzers Teil der RFID-Kommunikation. So wird es in einer Welt des „Ubiquitous Computing“ mit einer verbreiteten Auto-ID-Infrastruktur für den Einzelnen schwierig, sich der Erfassung und Auswertung durch diese Technik zu entziehen. Um auszuschließen, dass RFID-markierte Gegenstände erfasst und deren Daten ausgewertet werden, reicht es nicht aus, auf die Verwendung ihrer Auto-ID-Funktion zu verzichten. Für den nur passiv Beteiligten einer RFID-Kommunikation lässt sich die Erfassung ausschließlich über den Nichtgebrauch der Gegenstände kontrollieren, die mit RFID-Marken markiert sind.

Der Gebrauch von mit RFID-Technik versehenen Gegenständen führt nicht nur zu einem Ausgeliefertsein an Identifizierungsvorgängen und deren Auswertung in Informationssystemen. Vielmehr bedeutet dies auch, dass über die Interaktion selbst, ein gewisser Kontrollverlust des Betroffenen eintritt, da das RFID-Techniksystem in der Welt des „Ubiquitous Computing“ zunehmend Kontextinformationen, beispielsweise ein Verhalten des Betroffenen, einbeziehen kann und so Handlungsoptionen des Betroffenen verändert.

Dadurch, dass die Seriennummer auf der RFID-Marke ausgelesen werden kann, hinterlässt der Gegenstand Datenspuren. Diese erlauben es, Muster zu erkennen. Anhand des Identifikationsmerkmals der RFID-Marke kann erschlos-

sen werden, wann welche RFID-Marke und damit wann welcher Gegenstand den Ansprechbereich eines bestimmten Lesegeräts passierte.

Es ermöglicht aber darüber hinaus auch festzustellen, dass sich weitere Gegenstände zur gleichen Zeit ebenfalls im Ansprechbereich desselben Lesegeräts befanden. Hieraus ließen sich Rückschlüsse auf wiederkehrende Abläufe, Zusammengehörigkeiten oder nur wahrscheinliche Korrelationen ziehen und einfache Profile bezüglich der Gegenstände bilden. Des Weiteren können die markenseitig gespeicherten Nutzdaten das Kontextwissen zum Gegenstand anreichern. Die dadurch verfügbaren, aussagekräftigeren Daten helfen, den Gegenstand besser einzuordnen, wenn es um dessen Wiedererkennen oder das Erkennen von Mustern bezüglich seiner Verwendung geht.

Nachdem die Einbindung der RFID-Lesegeräte in ein Hintergrundinformationssystem eine Speicherung von unbegrenzten Zusatzdaten zum jeweiligen Gegenstand ermöglicht, steht hierüber ein gegenstandsbezogenes Kontextwissen zur Verfügung, das mehr als in der Seriennummer und im zusätzlichen Datenspeicher der RFID-Marke codierte Informationen sowie mehr als punktuelle Orts- und Zeitparameter enthält. Durch die Möglichkeit, Daten verschiedener RFID-Lesegeräte zusammenzuführen, würden beispielsweise anders als bei einem einzelnen RFID-Lesegerät zusätzlich Standortdaten bezüglich eines Gegenstandes über eine Zeitachse, also in Form eines Bewegungsprofils, aufgezeichnet. Zudem können auch Daten aus anderen Quellen mitberücksichtigt werden, die beispielsweise Herkunft, Beschaffenheit oder Geschichte des Gegenstandes, aber auch rechtliche Verhältnisse, wie Eigentum oder Gewährleistungstatus, näher beschreiben.

2.4.3 Angriffe auf RFID-Systeme

Schließlich bieten die ungeschützte Kommunikation und die offenliegenden Daten der RFID-Marke infolge fehlender oder zu geringer Schutzmechanismen Angriffsmöglichkeiten. Angriffe können auf die RFID-Marke, das RFID-Lesegerät oder das Hintergrundinformationssystem gerichtet sein.⁴²⁹ Sie können das Ziel haben, die Integrität, Vertraulichkeit oder Verfügbarkeit des Systems zu beeinträchtigen, indem abgelegte Daten unbefugt ausgelesen, falsche Daten eingespeist werden oder das RFID-System in seiner Funktionstüchtigkeit bis zum Totalausfall beeinträchtigt wird.⁴³⁰

- Angriffe auf die Integrität des RFID-Vordergrundsystems: Mit Angriffen auf die RFID-Marke lassen sich auf die auf ihr abgelegten Daten in Form der Identifikationsnummer, Sicherheitsinformationen oder anderer Nutzdaten ausspähen, aber auch durch unbefugte Schreibzugriffe manipulieren. Zum einen ist es durch eine veränderte Seriennummer der RFID-

⁴²⁹ Oertel u.a. 2004, 41 f.

⁴³⁰ Oertel u.a. 2004, 43; Finkenzeller 2008, 237; s. auch *Fraunhofer Sit*, RFID-Sicherheit und Angriffsmethoden, abrufbar unter: <http://www.rfid-basis.de/rfid-sicherheit.html>.

Marke möglich eine Identität des mit ihr verbundenen Gegenstandes vorzutauschen. Zum anderen lassen sich durch Veränderung der weiteren Nutzdaten mit dem Gegenstand, an die die RFID-Marke angeheftet ist, nicht zugehörige oder neue Informationen verbinden.⁴³¹ Um gegenüber dem RFID-Lesegerät ebenfalls eine falsche Identität vorzuspiegeln und falsche Daten vorzuhalten, können Duplikate von im Lauf befindlicher RFID-Marken (Cloning⁴³²) hergestellt und verwendet werden.⁴³³ Das Ausspähen und Manipulieren der Identifikationsnummer und der zusätzlichen Daten der RFID-Marke ist für Dritte entweder standardmäßig durch ein beliebiges RFID-Lesegerät oder durch falsche Autorisierung über ein RFID Lesegerät möglich.

- Angriffe auf die Vertraulichkeit des RFID-Vordergrundsystems: Eine weitere Angriffsmöglichkeit liegt in dem Abhören des Datenverkehrs (Sniffing), der zwischen der RFID-Marke und dem Lesegerät über die Luftschnittstellen ausgetauscht wird.⁴³⁴
- Angriffe auf die Verfügbarkeit des RFID-Vordergrundsystems: Des Weiteren können Angriffe auf die Funktionsfähigkeit der RFID-Marke oder das Funktionieren der Kommunikation gerichtet sein. Zum einen ist es möglich, die RFID-Marke zu deaktivieren oder durch mechanische oder elektromagnetische Einwirkung zu zerstören.⁴³⁵ Die RFID-Marke kann aber auch vom ursprünglichen Träger mechanisch gelöst werden, um sie einem anderen Gegenstand anzuheften, der dadurch eine neue, gefälschte Identität erhält.⁴³⁶ Zum anderen können Angriffe gegen die Luftschnittstelle in einer Weise geführt werden, dass die RFID-Kommunikation beeinträchtigt oder vollständig blockiert wird.⁴³⁷
- Angriffe auf die Integrität, Vertraulichkeit und Verfügbarkeit des Hintergrundinformationssystems: Für das Hintergrundinformationssystem bestehen die typischen Gefährdungen einer EDV-Anlage mit seiner Netzwerkinfrastruktur, seinen in diese integrierten Datenverarbeitungsanlagen und den hierauf verwendeten Anwendungsprogrammen. Dabei muss das Hintergrundinformationssystem grundsätzlich gegen zielgerichtetes Eindringen (Intrusion) oder konfuse Beeinträchtigungen durch zufällig ein-

⁴³¹ Oertel u.a. 2004, 42.

⁴³² Das Übertragen von echten Daten auf eine zweite Karte zum Zwecke der Herstellung einer oder mehrerer identischer (geklonter) Karten – s. Rankl/Effing 2002, 918. Zum „Cloning“ s. Oertel u.a. 2004, 42, 45; Finkenzeller 2008, 252.

⁴³³ Oertel u.a. 2004, 45.

⁴³⁴ Oertel u.a. 2004, 42; Finkenzeller 2008, 240; s. auch Fraunhofer Sit, RFID Sicherheit und Angriffsmethoden, abrufbar s.o.

⁴³⁵ Oertel u.a. 2004, 42.

⁴³⁶ Finkenzeller 2008, 240; Oertel u.a. 2004, 42; s. auch Fraunhofer Sit, RFID Sicherheit und Angriffsmethoden, abrufbar s.o.

⁴³⁷ Oertel u.a. 2004, 42.

geschleuste Programmanomalien (vor allem Viren oder Würmer) geschützt werden.⁴³⁸

2.5 Gesellschaftliche Diskussion des Einsatzes von RFID-Systemen

Angesichts des zunehmenden Einsatzes der RFID-Technologie nahmen verschiedene Nichtregierungsorganisationen, Verbände und Unternehmen, aber auch öffentliche Stellen Stellung und veröffentlichten Leitlinien und Positionspapiere zum Umgang mit RFID-Systemen. Diese berücksichtigen vor allem datenschutzrechtliche Belange.

Die folgende Auswahl von Stellungnahmen soll die kontroverse Diskussion um das Für und Wider des RFID-Einsatzes und die widerstreitenden Interessen der Akteure widerspiegeln, ohne damit einen vollständigen Überblick über den Meinungsstand zu geben.

2.5.1 Organisation Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)

Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN)⁴³⁹ war eine im Jahr 1999 gegründete Verbraucherorganisation, die in der RFID-Technologie große Risiken für bürgerliche Freiheiten sah. Sie stand daher weitgehend der neuen Technik skeptisch gegenüber. Dies kam in dem „Position Statement on the Use of RFID on Consumer Products“,⁴⁴⁰ ein unter Beteiligung weiterer Organisationen erarbeitetes Positionspapier, zum Ausdruck.⁴⁴¹

RFID wurde als Technologie mit starken sozialen Implikationen und dem Potential zur Zerstörung der Privatsphäre des Verbrauchers, der Anonymität beim Einkaufen und insgesamt als Gefahr für zivile Rechte vorgestellt. Bei der Darstellung der mit dem RFID-Einsatz verbundenen Gefahren wurde vor allem auf die Möglichkeit der Profilbildung und Konsumentenverfolgung hingewiesen. Hiergegen entwickelte CASPIAN ein dreigliedriges Schutzkonzept. Zuerst müsse eine Technikfolgenabschätzung in interdisziplinärer und alle Betroffenen beteiligender Weise geschehen. Bis zum Abschluss dieser dürften RFID-Marken keinesfalls mit einzelnen Produkten verbunden werden. Den zweiten Schritt stellte eine faire, nebst weiteren Prinzipien von Transparenz und Sicherheit als auch Datensparsamkeit getragene, verbindliche Verhaltensanforderung für Industrie und Verwaltung⁴⁴² dar, welche sich an Vorgaben der Organisation für

⁴³⁸ Näher dazu *Oertel u.a.* 2004, 44 ff.

⁴³⁹ Auch Betreiber der Internetseite <http://www.spychips.com>.

⁴⁴⁰ CASPIAN 2003.

⁴⁴¹ CASPIAN 2003.

⁴⁴² Zwar bezieht sich die Publikation zuerst alleinig auf das Verhältnis Verbraucher/Unternehmer, doch werden im Abschnitt „VI. Conclusion“ die Wertungen auch auf die Verwaltung übertragen.

wirtschaftliche Zusammenarbeit und Entwicklung (OECD) orientieren sollte. Abschließend wären drittens bestimmte Anwendungen gänzlich zu verbieten. Darunter fielen beispielsweise die Einbindung von RFID in Geld oder Kleidung sowie die gesamte Überwachung und Verfolgung von Betroffenen. Außerdem muss eine Deaktivierung der Marke möglich sein.

Als akzeptable Nutzungen präsentierte CASPIAN die Verwendung von RFID-Marken im Zusammenhang mit pharmazeutischen Produkten sowie Rückverfolgung von Gütern und Auffindung von Gefahrgut, wie auch die Abfallvernichtung. Gefordert wurde aber die wirksame dauerhafte Deaktivierung oder Entfernung der Marke vor Abgabe an den Endkunden.

In der zweiten Anlage dieser Publikation wendete sich CASPIAN unter anderem gegen die isolierte Methode der Deaktivierung von RFID-Marken (nach Abrechnung an der Kasse). Diese wäre einerseits unzureichend, weil sie zu spät die weitere Informationssammlung verhindere, andererseits ist sie auch rückgängig zu machen. Zu einer Zwei-Klassen-Struktur führte es daneben, diese Entscheidung den Konsumenten zu überlassen. Der (freiwillige) Einsatz von „Blocking Tags“ wurde darüber hinaus mit vergleichbarer Argumentation abgelehnt.

2.5.2 Digitalcourage e.V.

Im November 2003 erstellte der Verein Digitalcourage⁴⁴³, der damals noch den Namen FoeBud⁴⁴⁴ e.V. trug, sein „Positionspapier über den Gebrauch von RFID in Konsumgütern“.⁴⁴⁵ FoeBud e.V. war bekannt für die jährliche Verleihung des „BigBrotherAwards“.⁴⁴⁶

Der Verein sah die Privatsphäre, die Bürgerrechte und den Datenschutz durch versteckte RFID-Marken, versteckte Lesegeräte, massenhafte Datenzusammenführung und durch die Personenverfolgung mittels Erstellung von Profilen in Gefahr. Deshalb verlangte er in seinen „Leitlinien für Rechte und Pflichten im Zusammenhang mit RFID“ eine Technikfolgenabschätzung durch eine neutrale Stelle, ähnlich dem amerikanischen, von CASPIAN vorgestellten Modell. In ihrer Forderung nach einer fairen Informationspraxis sahen sie die Privacy-Richtlinien der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) ebenfalls als empfehlenswert an.

⁴⁴³ Seit November 2012 heißt *FoeBud e.V. Digitalcourage e.V.*

⁴⁴⁴ Der Verein nannte sich in seiner Langform „Förderung des öffentlichen bewegten und unbewegten Datenverkehrs“.

⁴⁴⁵ *FoeBud* 2003, 1-3.

⁴⁴⁶ Ziel von *BigBrotherAwards Deutschland* ist es, die öffentliche Diskussion um Privatsphäre und Datenschutz zu fördern, und den missbräuchlichen Umgang mit Technik und Informationen aufzuzeigen. So wurde 2003 die Metro-Gruppe für ihre „Future Store Initiative“ (Einsatz von RFID-Marken), 2005 das WM-Organisationskomitee des DFB (Nutzung von RFID-Schnüffelpchips in WM-Tickets) und 2011 die Modemarke Peuterey (verdeckt integrierte RFID-Marken in Kleidung) ausgezeichnet – s. auch <http://www.bigbrotherawards.de/2003>.

FoeBud e.V. verlangte die Einhaltung folgender Prinzipien:

- Offenheit und Transparenz: Anwender von RFID dürfen keine geheimen Datenbanken anlegen und müssen ihre Praktiken in Bezug auf die Nutzung und Instandhaltung der Technik offen darlegen.
- Zweckangabe: Der Anwender muss angeben, zu welchem Zweck RFID-Marken und –Lesegeräte eingesetzt werden.
- Sammelbegrenzung: Das Sammeln von Informationen soll auf die Daten beschränkt bleiben, die für den jeweiligen Zweck erforderlich sind.
- Verantwortung: RFID-Anwender tragen die Verantwortung bei dem Einsatz der Technik und müssen zur Rechenschaft gezogen werden, wenn die Prinzipien nicht eingehalten werden.
- Sicherheitsstandards: Integrität und Sicherheit müssen bei dem Zugriff auf Datenbanken, dem System und bei der Datenübermittlung gewährleistet sein. Neutrale Instanzen haben eine Sicherheitsbeurteilung vorzunehmen und zu veröffentlichen.

Der Verein FoeBud e.V. sprach sich für ein striktes Verbot von RFID-Anwendungen aus, die die Anonymität des Bürgers nicht garantieren können. Zu akzeptieren sei aber der Einsatz von RFID-Technik bei der Rückverfolgung von Medikamenten und industriellen Gütern, insbesondere wenn diese toxische Substanzen enthalten.

2.5.3 Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre

Die Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre forderte in einer Resolution, die vom ULD⁴⁴⁷ „mitgestaltet wurde“, bereits im November 2003, dass personenbezogene Daten aus RFID-Marken nur in einer offenen und transparenten Weise erhoben werden dürfen, um einen ungerechtfertigten Eingriff in die Privatsphäre zu verhindern.⁴⁴⁸

So sollten folgende Grundsätze bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden:

- Jeder Verarbeiter von Daten soll vor Einführung von RFID-Marken, die mit personenbezogenen Daten verknüpfbar sind oder die zur Bildung von Konsumprofilen führen, zunächst andere Möglichkeiten in Betracht ziehen, die das gleiche Ziel – ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen – erreichen.
- Der Betroffene muss über die beabsichtigte Erhebung und die weitere Verwendung von personenbezogenen Daten informiert werden. Eine

⁴⁴⁷ S. unten.

⁴⁴⁸ Internationale Konferenz der Datenschutzbeauftragten, Entschließung 2003.

Speicherung von Daten darf nur erfolgen, wenn sie unverzichtbar ist, unbemerkte Datenerhebung ist verboten.

- Personenbezogene Daten dürfen nur für den Zweck verwendet werden, für den sie erhoben werden. Sie dürfen nur solange aufgehoben werden, wie es zur Erreichung des Zweckes erforderlich ist.
- Daten von RFID-Marken aus verschiedenen Produkten müssen getrennt verarbeitet werden, sodass keine Verhaltens-, Nutzungs- und Bewegungsprofile erstellt werden können.

2.5.4 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) betrachtete in seiner Stellungnahme 2004 die RFID-Technik als Vorteil im Bereich der Logistik, aber als Gefahr für die Privatsphäre, insbesondere durch Bildung von personalisierten Einkaufs- und Nutzungsprofilen.⁴⁴⁹ Es erwartete in absehbarer Zeit unsichtbare RFID-Marken in beinahe allen Alltagsgegenständen. Darüber hinaus wies es auf eine neue Marken-Generation hin, die nicht nur durch spezielle Lesegeräte auszulesen wären, sondern ohne ein solches Lesegerät mit anderen Marken in Verbindung treten könnten.

Um dem Grundrecht der informationellen Selbstbestimmung gerecht zu werden, forderte das ULD, personenbezogene Daten offen und transparent zu erheben. Dabei wies es darauf hin, dass nicht nur die Vorteile, darunter auch ein Gewinn an Komfort für Verbraucher zu beachten wären, sondern auch die benannten Nachteile in den Blick genommen und verhindert werden müssten. Dies könnte insbesondere durch technische Maßnahmen erfolgen.

2.5.5 Stellungnahme der Bundesregierung der 15. Legislaturperiode

Im Zuge der Diskussion um die Einführung der RFID-Technik stellte die Fraktion der FDP im Bundestag eine kleine Anfrage, mit der sie von der Bundesregierung wissen wollte, wie sie den RFID-Einsatz aus datenschutzrechtlicher Sicht beurteile und welche Missbrauchsgefahren für den Einzelnen, insbesondere hinsichtlich der Erstellung von Bewegungsprofilen, zu erwarten wären.⁴⁵⁰

In ihrer Stellungnahme vom Mai 2004 teilte die Bundesregierung mit, dass bei dem gegenwärtigen Entwicklungsstand der RFID-Technik kein ergänzender Regelungsbedarf erkennbar wäre.⁴⁵¹

Die Erhebung und Verwendung von personenbezogenen Daten durch RFID-Systeme, sei es als Zeiterfassungs- oder Eintrittskarten zur Kontrolle der Zutrittsberechtigung oder sei es als Produkt- oder Bauteilkennzeichnung zur Logistik- und Prozesssteuerung, würden durch das geltende Datenschutzrecht

⁴⁴⁹ ULD 2004.

⁴⁵⁰ BT-Drs. 15/3025.

⁴⁵¹ BT-Drs. 15/3190, 2 f.

abgedeckt. Missbrauchsgefahren wären, insbesondere wegen der geringen Reichweite der RFID-Systeme, die personenbezogene Daten verwenden, praktisch ausgeschlossen, zumal nach Kenntnis der Bundesregierung in Deutschland keine Systeme eingesetzt würden, die Kundendaten mit RFID-markierten Produkten verknüpfen und Bewegungsprofile erstellen.

Die Bundesregierung betonte für den Einsatz von RFID-Technik die Bedeutung der Transparenz, besonders die Information des Betroffenen über den Umgang von personenbezogenen Daten durch die eingesetzte RFID-Technik. Auskunftsrechte des Betroffenen sowie besondere Unterrichtungspflichten nach § 6c BDSG bei der Verwendung von leistungsfähigen RFID-Marken regelte allerdings das Datenschutzrecht bereits. Auch verpflichtete das geltende Datenschutzrecht zum Schutz vor unbefugtem Auslesen von Daten zu entsprechenden organisatorischen und technischen Schutzmaßnahmen gemäß § 9 BDSG.

2.5.6 Unternehmen Microsoft

Der weltweit führende Hersteller von Betriebssystemen und anderer Software, Microsoft, verwies in seinem Positionspapier vom September 2004 „Microsoft und RFID, White Paper“⁴⁵² neben den Risiken für die Privatsphäre der Verbraucher auf mögliche Verbesserungen für das tägliche Leben sowie für Unternehmen. Ziel müsste es daher sein, die RFID-Technik verantwortlich zu entwickeln. Ausgehend von der Darstellung der veränderten und gesteigerten Gefährdungslage empfahl Microsoft gemäß seiner Vorstellung einer verantwortlichen Entwicklung, die Implementierung von Sicherheitsmethoden in die RFID-Technik. Unternehmen, die RFID-Technik verwenden, müssten sich an festgelegte Vorschriften halten.

2.5.7 Artikel-29-Datenschutzgruppe

Gemäß dem Art. 29 der Richtlinie 95/46/EG (DSRL)⁴⁵³ wurde ein unabhängiges Beratungsgremium der Europäischen Gemeinschaft für Datenschutzfragen „Artikel-29-Datenschutzgruppe“ eingesetzt. Ihre Aufgaben sind in Art. 30 der Richtlinie 95/46/EG sowie in Art. 15 Abs. 3 der Richtlinie 2002/58/EG⁴⁵⁴ festgelegt.

Diese Gruppe verabschiedete am 19. Januar 2005 als ersten Situationsbericht ein Arbeitspapier „Datenschutzfragen im Zusammenhang mit der RFID-Technik“,⁴⁵⁵ indem sie auf europäischer Ebene eine Bewertung datenschutzrechtlicher Belange des Einsatzes von RFID-Systemen vornahm. Ohne die mit den möglichen RFID-Anwendungen verbundenen Vorteile verkennen zu wollen, sah die Artikel-29-Datenschutzgruppe bei RFID-Systemen technisch bedingt,

⁴⁵² Microsoft 2004.

⁴⁵³ Richtlinie 95/46/EG v. 24.10.1995, EG-ABl. L 281/48 v. 23.11.1995.

⁴⁵⁴ Richtlinie 2002/58/EG v. 12.7.2002, EG-ABl. L 201/46 v. 31.7.2002.

⁴⁵⁵ Artikel-29-Datenschutzgruppe, WP 105/2005.

eine hohe Verletzlichkeit durch Angriffe gegeben und befürchtete durch ihren Einsatz schwerwiegende Eingriffe in die informationelle Selbstbestimmung und Menschenwürde.

Ausgehend von der Anwendbarkeit des Datenschutzrechts für den Großteil der bislang geplanten RFID-Anwendungen,⁴⁵⁶ wies die Gruppe auf die im Datenschutz geltenden Grundsätze und konkreten Anforderungen hin, die auch beim Einsatz von RFID-Systemen zu beachten wären. Insbesondere war sie der Meinung, dass gegenüber dem Betroffenen eine Informationspflicht besteht, ihm die Existenz von RFID-Marken und RFID-Lesegeräten und ihren Verwendungszusammenhang erkennbar zu machen.⁴⁵⁷ Daneben sollten geeignete Verfahren über Aktivierbarkeit und Echtzeitaktivierung des RFID-Systems informieren.⁴⁵⁸ Außerdem sah die Artikel-29-Datenschutzgruppe die Bereitstellung technischer Lösungen als Geboten an, um dem Betroffenen die Löschung oder Deaktivierung zu ermöglichen.⁴⁵⁹ Schließlich betonte die Arbeitsgruppe, dass im Feld der RFID-Technik Forschungs- und Entwicklungsbedarf bestehe und eine weitere Diskussion über rechtliche und technische Fragen geführt werden müsse.⁴⁶⁰

Im Mai 2009 veröffentlichte die Artikel-29-Datenschutzgruppe eine Empfehlung, die vorsieht, dass die RFID-Branche vor Einführung von RFID-Anwendungen eine „Datenschutz-Folgenabschätzung“ durchführt und die erhaltenen Ergebnisse an die zuständigen Stellen weiterleitet.⁴⁶¹ Ein zunächst von der Artikel-29-Datenschutzgruppe abgelehntes Konzept zur Prüfung der Datenschutzverträglichkeit von einzuführenden RFID-Anwendungen, das die RFID-Anwendungsbetreiber im März 2010 vorschlugen, wurde nach seiner Überarbeitung von ihr positiv bewertet.⁴⁶²

2.5.8 Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BitKom)

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BitKom), der als Branchenverband über 700 Unternehmen der Geräte-, Software- und Medienindustrie vertritt, veröffentlichte eine Stellungnahme zum Einsatz von RFID-Systemen. In dieser kritisierte BitKom die Forderungen der Artikel-29-Datenschutzgruppe und stellte in der beigefügten Anlage⁴⁶³ vom 21. März 2005 seine Bewertung datenschutzrechtlicher Implikationen dar. Sei-

⁴⁵⁶ Artikel-29-Datenschutzgruppe, WP 105/2005, 8 f.

⁴⁵⁷ Artikel-29-Datenschutzgruppe, WP 105/2005, 12, 15.

⁴⁵⁸ Artikel-29-Datenschutzgruppe, WP 105/2005, 15.

⁴⁵⁹ Artikel-29-Datenschutzgruppe, WP 105/2005, 17 f.

⁴⁶⁰ Artikel-29-Datenschutzgruppe, WP 105/2005, 18.

⁴⁶¹ Artikel-29-Datenschutzgruppe, WP 175/2009, 4.

⁴⁶² Artikel-29-Datenschutzgruppe, WP 180/2011, 3 und 6; näher Abschnitt 2.5.16.

⁴⁶³ BitKom 2005, 4 ff.

ner Ansicht nach entstanden durch den Einsatz der RFID-Technik keine neuen datenschutzrechtlichen Herausforderungen. Er sah den, durch das geltende Datenschutzrecht gewährten Schutz, als weitgehend ausreichend an. Es ließe sich auch aus dem geltenden Datenschutzrecht keine Lösungs- und Deaktivierungspflicht sowie weitere Informationspflichten über Aktivierungsstatus der RFID-Marken gegenüber dem Betroffenen ableiten. Auch Vorschriften des Strafgesetzbuchs kämen beim RFID-Einsatz nicht zum Tragen.

2.5.9 Deutscher Fußball-Bund (DFB) zur Fußballweltmeisterschaft 2006

Kontrovers wurde die Zutrittskontrolle zu den Fußballstadien der Weltmeisterschaft 2006 in Deutschland diskutiert. Die Fédération Internationale de Football Association (FIFA) und der Deutsche Fußball-Bund (DFB) gaben Eintrittskarten aus, die mit einer RFID-Marke versehen waren.⁴⁶⁴ Der Zuteilung der Eintrittskarten vorgeschaltet war ein mehrstufiger Bestellvorgang, bei dem der Eintrittskarteninteressent neben Namen und Fußballspielwunsch, auch Wohnanschrift, Geburtsdatum und Personalausweisnummer angeben musste.

Damit versprachen sich die Verantwortlichen eine zügige Abwicklung des Einlasses sowie größere Fälschungssicherheit gegenüber dem Handel von Eintrittskarten auf dem Schwarzmarkt. Begründet wurde die Einführung insbesondere auch mit dem Erfordernis hoher Sicherheit in den Stadien, die mittels eines solchen Zutrittskontrollsystems besser gewährleistet werden könnte. Daneben sollte sich Deutschland als innovativer Veranstalter präsentieren.

Dieses Konzept der Einlasskontrolle stieß auf heftige Kritik durch Verbraucherschutzorganisationen und Datenschutzbehörden.⁴⁶⁵ In dem Zukunftsgespräch des Instituts für Zukunftsstudien und Technologiebewertung (IZT) vom 9. Oktober 2005 stellten Datenschützer die Erforderlichkeit und Koppelung der Datenerhebung infrage und beklagten nicht zuletzt die Intransparenz der geplanten Verarbeitungsvorgänge.⁴⁶⁶ Befürchtet wurde, dass dieses Zutrittskontrollsystem nicht nur für den Ausnahmefall der Fußballweltmeisterschaft, sondern künftig auch für den Regelbetrieb der Ligaspiele Verwendung finden sollte. Sorge bestand zudem, dass mit seiner Einführung und der Personalisierung der Eintrittskarten wertvolle Kundendaten gewonnen werden sollten, um diese gewinnbringend in der Werbeindustrie weiter nutzen zu können. Die Kontroverse führte zu Nachbesserungen an dem ursprünglichen Konzept des Bestellvorgangs.

⁴⁶⁴ Vgl. Abschnitt 2.1.3.3.

⁴⁶⁵ S. z.B. Pressemitteilung der Verbraucherzentrale Bundesverband v. 1.12.2005, abrufbar unter: <http://www.verbaende.com/news.phph/WM-2006-vzbv-vzbv-klagt-gegen-ticketbedingungen>. Auch-EU-Kommission-prueft-Zulaessigkeit-vzbv-DFB-agiert-planlos?m=34995; Stellungnahme *FoeBuD*, abrufbar unter: http://www.foebud.org/rfid/pe-wm2006-21-01-2005/ULD_Schleswig-Holstein, abrufbar unter: http://www.datenschutzzentrum.de/polizei/Weichert_wm.htm; s. auch *Conrad*, CR 2005, 537 ff.

⁴⁶⁶ S. <http://www.heise/newsticker/meldung/65449>.

2.5.10 Organisation EPCglobal

EPCglobal ist eine nicht gewinnorientierte Organisation, um die Normung und den branchenübergreifenden Einsatz der RFID-Technik entlang der gesamten Wertschöpfungskette zu unterstützen.⁴⁶⁷ Sie informiert auf der eigenen Internetseite über die RFID-Technik, ihre Möglichkeiten und inzwischen auch über ihre Risiken für die Privatsphäre.⁴⁶⁸

In seinen Stellungnahmen von 2006 reagierte EPCglobal auf die Bedenken zum RFID-Einsatz im Handel. Sie versprach diese sehr ernst zu nehmen und strebte technische Lösungen sowie Lösungen auf politischer Ebene an.⁴⁶⁹ EPCglobal wehrte sich im „Implementation Cookbook“⁴⁷⁰ gegen die Kritik und wollte durch gezielte Aufklärung der Desinformation entgegenwirken. Daher wurden spezielle Leitlinien („Guidelines“) für Konsumenten entwickelt, die über die konkrete Verwendung von RFID-Marken an Produkten informierten sowie dem Verbraucher die Möglichkeit gewährte, die Marken auf erworbenen Produkten zu deaktivieren.⁴⁷¹

2.5.11 Konferenzen der Datenschutzbeauftragten des Bundes und der Länder

Die Datenschutzbeauftragten des Bundes und der Länder schlossen sich vorbehaltlos der Position der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre 2004 an.⁴⁷² Auf ihrer Konferenz im Oktober 2006⁴⁷³ bekräftigten sie, dass der Schutz der Persönlichkeitsrechte von Betroffenen nur gewährleistet werden könne, wenn die zum Einsatz der RFID-Technik formulierten Grundsätze⁴⁷⁴ eingehalten würden.

Im Hinblick auf die Weiterentwicklung der IuK-Technik und das Angebot neuer, sich dieser Technik bedienender Anwendungen, legten die Datenschutzbeauftragten des Bundes und der Länder auf ihrer Konferenz im März 2010⁴⁷⁵ ein Eckpunktepapier zu einem modernen Datenschutzrecht für das 21. Jahrhundert vor,⁴⁷⁶ das als Diskussionsgrundlage für eine Reform des Datenschutzrechts dienen sollte. Hierin betonte sie, dass die wichtigsten Grundsätze des Datenschutzes, trotz der neuen Technologien und der Globalisierung, nach wie vor gültig wären. Allerdings sollten anhand der Schutzziele sanktionsbe-

⁴⁶⁷ Vgl. auch Abschnitt 2.2.6.1.

⁴⁶⁸ S. <http://epcglobalinc.org> oder <http://gs1.org/epcglobal>.

⁴⁶⁹ EPCglobal 2006a.

⁴⁷⁰ S. <http://www.epcglobalinc.org/what/cookbook>.

⁴⁷¹ EPCglobal 2006b.

⁴⁷² Konferenz der Datenschutzbeauftragten, Entschließung 2004.

⁴⁷³ Konferenz der Datenschutzbeauftragten, Entschließung 2006.

⁴⁷⁴ S. oben.

⁴⁷⁵ Konferenz der Datenschutzbeauftragten, Entschließung 2010.

⁴⁷⁶ BfDI, 2010.

wehrte Grundsatznormen erarbeitet werden, die für alle Formen der Datenverarbeitung gelten.

2.5.12 Organisation European Expert Group for IT-Security (EICAR)

EICAR, deren RFID-Task-Force neben Microsoft Corporation, IBM, Metro Group und anderen renommierten Unternehmen, der Bundesdatenschutzbeauftragte, das Bundesamt für Sicherheit in der Informationstechnik und die NATO angehören, bewertete in einem kurz gefassten „Management-Leitfaden für den Einsatz von RFID-Systemen“⁴⁷⁷ die möglichen mit der RFID-Technologie verbundenen datenschutzrelevanten Probleme als wichtigen Faktor. Selbstverpflichtungen der Industrie sah sie jedoch insbesondere unter Berücksichtigung der potenziellen unsichtbaren Allgegenwärtigkeit der Technologie nicht als ausreichenden Garanten zur Wahrung der Privatsphäre der Kunden und forderten dementsprechend technische Schutzmechanismen. Außerdem stellte EICAR technische Schutzmechanismen für Marken und Lesegeräte vor, betonte aber, dass auch die Hintergrundinformationssysteme entsprechend abzusichern seien.⁴⁷⁸

Ein zuletzt im März 2006 aktualisierter „Leitfaden: RFID und Datenschutz“ klärt nicht nur technische Fragen und zeigt Anwendungsmöglichkeiten für Unternehmer auf, sondern bilanziert auch datenschutzrechtliche Anforderungen des Bundesdatenschutzgesetzes. Hierbei werden insbesondere Informations- und Hinweispflichten erörtert. Eine umfassende Profilerstellung sei aber in jedem Fall nur mit Einwilligung des jeweiligen Kunden möglich.⁴⁷⁹

2.5.13 Center for Democracy and Technology (CDT)

Die RFID-Arbeitsgruppe am Center for Democracy und Technology (CDT) stellte im Mai 2006 eine Richtlinie⁴⁸⁰ vor, an der sich u.a. Cisco System Inc., Microsoft Corporation, IBM, Visa und Procter & Gamble Company beteiligten. Hierin wurden die Vorzüge der RFID-Technologie für Konsumenten, die Wirtschaft, das Gesundheitswesen und auch für Regierungen gepriesen. Gefahr bestände hinsichtlich der Verknüpfung von personenbezogenen Daten mit den RFID-Systemen.

Die Arbeitsgruppe wandte sich insbesondere gegen verborgen angebrachte Marken, heimliche Auslesevorgänge und forderte eine Zugangsmöglichkeit der Verbraucher zu den über sie gewonnenen Informationen. Insgesamt wurde größtmögliche Transparenz verlangt, wozu es gehöre, den Bürger über und bei Verwendung von RFID umfassend zu informieren. Des Weiteren sollte die Ent-

⁴⁷⁷ EICAR 2006a.

⁴⁷⁸ Autor 2006, 28 f.; s. auch EICAR 2006, 7 ff.

⁴⁷⁹ EICAR 2006b.

⁴⁸⁰ CDT 2006.

scheidung über die Verwendung beim Verbraucher verbleiben. Eine ablehnende Haltung sollte auch nicht zu Nachteilen führen (beispielsweise hinsichtlich der Warengarantie). Auch sollte der Datenschutz bereits bei der Entwicklung der RFID-Systeme Beachtung finden, um nicht erst später nachgerüstet werden zu müssen.

2.5.14 US – National Institute of Standards and Technology (NIST)

Das, dem Wirtschaftsministerium der Vereinigten Staaten von Amerika (USA) nachgeordnete Institute of Standards and Technology (NIST) veröffentlichte seine Leitlinien „Guidelines for Securing Radio Frequency Identification (RFID) Systems“⁴⁸¹ im April 2007. Dieser Leitfaden wurde unter Mitwirkung des Information Technology Laboratory (ITL) erarbeitet und stellt die RFID-Technologie vor, nannte ihre Anwendungsmöglichkeiten und ihre Risiken und wies auf mögliche schützende Sicherheitskontrollen und datenschutzrechtliche Komplikationen hin. Des Weiteren stellte dieses - an Unternehmen gerichtete Papier - zwei Fallstudien⁴⁸² vor. Die Studien beschrieben die Möglichkeiten des Einsatzes von RFID Technologie im Gesundheitswesen und im Umgang mit Gefahrgut (z.B. Atommüll).

Bereits in der einleitenden Zusammenfassung („Executive Summary“) wurden die Risiken des RFID-Einsatzes genannt. Diese Risiken wären durch organisatorische und technische Maßnahmen zu minimieren. Entsprechend wurden umfassende Sicherheitsmaßnahmen empfohlen. Hinsichtlich der vorgestellten Anwendungsmöglichkeiten und -umgebungen beschränkte sich der Leitfaden allerdings auf Nachverfolgungsszenarien (Tracking-Szenarien) und ging nicht auf die spezifischen Risiken ein, die durch den Einsatz von Smart-Cards zur Identifizierung im Zusammenhang mit Zugangsberechtigungsnachweisen oder auch beim Bezahlen entstehen können.⁴⁸³

Um die benannten Risiken handhaben zu können, wären Vorkehrungen auf der Managementebene, im operativen Geschäft sowie auf Ebene der technischen Entwicklung notwendig. Seitens der strategischen Führung wurden allgemein verpflichtende Leitlinien hinsichtlich des Einsatzes der RFID-Technologie verlangt. Zudem wären Maßnahmen zu treffen, um die Daten auf der RFID-Marke selbst zu minimieren.⁴⁸⁴ Die Vorgaben könnten einerseits organisatorisch beispielsweise durch Zugangskontrollen zu sensiblen Bereichen, durch Zerstörung nicht mehr benötigter RFID-Marken, Schulungen oder durch Verteilung der Verantwortlichkeiten zur Verringerung der Schädigungsmöglichkeiten umgesetzt werden.⁴⁸⁵ Andererseits wären technische Schutzvorkehrun-

⁴⁸¹ Nist 2007.

⁴⁸² Nist 2007, Kap. 8.

⁴⁸³ S. <http://www.heise.de/newsticker/meldung/89030>; s. auch Nist, 2007, Kap. 1.2 und 5.

⁴⁸⁴ Nist 2007, Kap. 5.1.

⁴⁸⁵ Nist 2007, Kap. 5.2.

gen zu treffen, indem beispielsweise kryptographische Mechanismen in RFID-Komponenten implementiert werden.⁴⁸⁶

2.5.15 Metro-Gruppe

Nach Angaben der Metro-Gruppe werden seit 2008 RFID-Marken in allen Metro-Konzernen – weltweit – eingesetzt. Dadurch konnten die Logistik, das Lagermanagement, die Warenverfügbarkeit für den Konsumenten und die Arbeitsabläufe optimiert werden.

In der Broschüre „Die Metro-Group und RFID“⁴⁸⁷ wurden die Vorzüge eines mit RFID-Technologie ausgestatteten Einkaufsladens angepriesen. Beispielsweise wies der Konzern auf eine schnelle Kaufabwicklung an der „Selbstzahlkasse“, Terminals mit Informationen, automatisch überwachte Regale, intelligente Umkleidekabinen und einen unterstützenden Computer am Einkaufswagen hin.⁴⁸⁸ Das Unternehmen arbeite mit seinen Partnern an einem kundenfreundlichen Einsatz von RFID-Marken. Weiter wurde in dieser Informationsschrift darauf hingewiesen, dass die Datenschutzbestimmungen eingehalten würden. Neben der Befolgung gesetzlicher Vorschriften, existiere ein freiwilliger Kodex. Dieser sehe neben der Bereitstellung von Marken-Deaktivatoren vor, dass die Kunden stets umfassend informiert würden.⁴⁸⁹

2.5.16 Kommission der Europäischen Union

Im Mai 2009 veröffentlichte die EU-Kommission eine „Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen“.⁴⁹⁰ Kern der Empfehlung war die Aufforderung an „die Mitgliedsstaaten dafür Sorge zu tragen, dass die Branche in Zusammenarbeit mit den jeweiligen Beteiligten aus der Zivilgesellschaft einen Rahmen für Datenschutz-Folgenabschätzungen“ (Privacy Impact Assessment, PIA) aufstellt.⁴⁹¹

Weiter forderte die Kommission im Einzelhandel eine transparente und möglichst unentgeltliche Möglichkeit für den Verbraucher, RFID-Marken deaktivieren oder entfernen zu lassen.⁴⁹² Schließlich wurde weiterer Entwicklungs- und Aufklärungsbedarf gesehen, um einerseits die Umsetzung von datenschutzfördernden Techniken in RFID-Anwendungen zu unterstützen und andererseits

⁴⁸⁶ Nist 2007, Kap. 5.3.

⁴⁸⁷ Metro Gruppe 2008; vgl. Abschnitt 2.1.3.1.

⁴⁸⁸ Metro Gruppe 2008, 25 ff.

⁴⁸⁹ Metro Gruppe 2008, 29 f.

⁴⁹⁰ EU-Kommission, Empfehlung, (2009/387/EG), L 122, 47.

⁴⁹¹ EU-Kommission, Empfehlung, (2009/387/EG), L 122, 50, Nr. 4, 5, 10.

⁴⁹² EU-Kommission, Empfehlung, (2009/387/EG), L 122, 51, Nr. 11, 12.

das Bewusstsein aller Beteiligten für die Chancen und Risiken zu stärken.⁴⁹³ Interessant ist die in den Erwägungsgründen getroffene Feststellung, dass RFID-gestützte Anwendungen unter den Anwendungsbereich der allgemeinen Datenschutzrichtlinie (Richtlinie 95/46/EG) sowie unter den der Datenschutzrichtlinie für die elektronische Kommunikation (Richtlinie 2002/58/EG) fallen.

Im April 2011 wurde nach Ablehnung des ersten Entwurfs durch die Artikel-29-Datenschutzgruppe ein Rahmen für die Datenschutz-Folgenabschätzung (PIA-Framework) von Vertretern der Zivilgesellschaft, Vertretern der Industrie und Datenschützern unter der Teilnahme der EU-Kommissarin Neelie Kroes unterzeichnet.⁴⁹⁴ Darin ist vorgesehen, dass der jeweilige Anwender vor der Einführung der RFID-Technik eine „Datenschutz-Folgenabschätzung“ durchführt, die in eine Vor-Bewertungsphase und die eigentlich wichtige Risikobewertungsphase unterteilt ist.⁴⁹⁵ Damit sollen europaweit gleiche Ausgangsbedingungen bei Herstellern und Anwendern geschaffen werden. Dieser neue Ansatz verlangt von der Industrie und den Anwendern die „Durchführung von Datenschutz-Verträglichkeitsprüfungen, insbesondere für bestimmte Datenverarbeitungsvorgänge, von denen angenommen wird, dass sie (...) besondere Risiken für die Rechte und Freiheiten der Betroffenen darstellen.“⁴⁹⁶

Entsprechend der Forderungen der Europäischen Kommission sieht der Rahmen für eine Datenschutz-Folgenabschätzung (PIA-Framework) zudem vor, dass RFID-Marken im Falle einer möglichen Bedrohung der Privatsphäre oder dem Schutz personenbezogener Daten standardmäßig („per Default“) deaktiviert werden müssen – es sei denn, es liegt eine explizite Einwilligung des Verbrauchers vor.

2.5.17 Verbraucherzentrale Bundesverband (vzbv)

Die Verbraucherzentrale Bundesverband (VZBV) begrüßt in ihrer Stellungnahme vom 6. April 2011 den europäischen Selbstverpflichtungsrahmen für Datenschutz-Folgenabschätzung (PIA-Framework), mahnt aber gleichzeitig eine konsequente Umsetzung an.

Für die weitere Vorgehensweise nennt der VZBV folgende Anforderungen⁴⁹⁷:

- Scharfe und wirksame Sanktionsmöglichkeiten, die definiert sein müssen, bei Nichteinhaltung der Datenfolgenabschätzungen gemäß dem PIA-Framework.

⁴⁹³ *EU-Kommission*, Empfehlung, (2009/387/EG), L 122, 51, Nr. 15 ff., Erwägungsgrund 24, 26.

⁴⁹⁴ *Artikel-29-Datenschutzgruppe*, WP 175/2010.

⁴⁹⁵ *Artikel-29-Datenschutzgruppe*, WP 180/2011, 5.

⁴⁹⁶ *Artikel-29-Datenschutzgruppe*, WP 168/2009, 23.

⁴⁹⁷ Näher dazu *Verbraucherzentrale Bundesverband* 2011.

- Unbedingte Kennzeichnungspflicht, wo RFID drin ist, muss auch RFID drauf stehen. Diese Kennzeichnung muss zusätzlich den Namen des Betreibers und eine Kontaktmöglichkeit (Hotline-Telefonnummer oder Internetadresse) enthalten.
- Erhöhung der Transparenz durch Informationen auf dem Produkt über die Risiken einer Anwendung, außerdem Zugang zu vollständigen Prüfungsergebnissen der Datenschutz-Folgenabschätzung durch Bereitstellung im Internet.
- Der VZBV fordert grundsätzlich die physische Entfernung der RFID-Marke am Verkaufsort oder vor Versand im Fernabsatz. Dem Verbraucher dürfen keine Nachteile auch nach dem Kauf (bei Umtausch, Garantieleistungen) durch nicht aktivierte Marken entstehen. Sollte ein Verbraucher sich bewusst gegen die Deaktivierung entscheiden, müssen die Einwilligungserklärungen klar, verständlich und an die Alltagsrealität angepasst sein.
- Wirtschaft, Datenschutzbeauftragte von Bund und Ländern und Verbraucherverbände haben die Verpflichtung die Öffentlichkeit über die Gefahren beim Einsatz von RFID aufzuklären.
- Der VZBV verlangt zusätzliches Personal für die Datenschutzbehörden, um die Datenschutz-Folgenabschätzungen konsequent und nachhaltig durchführen zu können.

2.5.18 Bundesbeauftragter für Datenschutz und Informationsfreiheit

Der Bundesbeauftragte für Datenschutz und Informationsfreiheit (BfDI) geht von einer zunehmenden Verbreitung der RFID-Technik aus. Wenn die „kleinen Funkchips“ die Welt erobern, sieht er die Gefahr einer mit der realen Welt verbundenen allgegenwärtigen Datenverarbeitung.⁴⁹⁸

Als Maßnahmen, begleitend zur großflächigen Einführung und Nutzung der RFID-Technik, werden Aufklärung und Schutzmechanismen gefordert. Demnach ist die Wirtschaft gehalten, die Verbraucher über die konkreten Verarbeitungs- und Nutzungsvorgänge zu informieren und Möglichkeiten zur Deaktivierung der Marken oder zur Löschung ihrer Inhalte zu schaffen. Daneben sollen Mechanismen treten, anonymes Kaufen zu ermöglichen und auch (Selbst-)Verpflichtungen der Industrie, Daten sparsam und sicher zu verarbeiten. Bloße Absichtserklärungen von Seiten der Industrie hält der Bundesbeauftragte für nicht ausreichend. Notfalls muss es verbindliche Regelungen für den Einsatz der RFID-Technik geben.⁴⁹⁹

⁴⁹⁸ S. BfDI 2012.

⁴⁹⁹ S. <http://www.heise.de/newsticker/meldungen/98659.htm>.

2.5.19 Fazit zur gesellschaftlichen Diskussion

Inzwischen wird die Auseinandersetzung weniger aufgeregt geführt und die Diskussion um die Risiken des Einsatzes hat sich versachlicht.

Der zu Beginn enge Fokus auf die Technikkomponente der RFID-Marke hat sich geweitet. Mittlerweile wird die RFID-Technik als System wahrgenommen und die Diskussion bezieht andere Auto-ID-Verfahren mit ein. Zum anderen sind in die Betrachtung mehr die Anwendungen gerückt, die auf diese Verfahren zurückgreifen. Einbezogen werden nicht nur die durch die Auto-ID-Technik bedingten Risiken, sondern der Datenumgang, der gerade in Verknüpfung mit den weiteren Datenverarbeitungsanwendungen eines Unternehmens oder der Akteure einer Prozesskette eine neue Qualität erfahren kann.

Grund hierfür dürfte in der Vertiefung der Diskussion, aber auch in der medialen Abnutzung des Themas liegen. Im Diskussionsprozess wurden den Beteiligten zum einen die Funktionsweise der RFID-Technik und den mit ihr verbundenen Möglichkeiten und Grenzen zunehmend vertrauter, wodurch die Auseinandersetzung mit zunehmender Sachkompetenz geführt werden kann. Zum anderen dürften die Bemühungen um Transparenz und Risikobegrenzung zu einer Entschärfung der Auseinandersetzung beigetragen haben, zu denen sich die Interessenprotagonisten aus Wirtschaft und Politik als Reaktion auf die zum Teil recht öffentlichkeitswirksam geführte Auseinandersetzung gezwungen sahen. Auch führte die Präsenz des Themas in den Medien zu einer gewissen Gewöhnung. Verbraucher empfinden die RFID-Technik weniger bedrohlich als diese für sie noch neu und unbekannt war. Zur Beruhigung trug sicherlich auch bei, dass die Einführung der RFID-Technik weniger schnell und umfassend kam, wie prognostiziert oder befürchtet.

Auto-ID-Verfahren im Kontext allgegenwärtiger
Datenverarbeitung
Datenschutzrechtliche Betrachtung des Einsatzes von
RFID-Systemen
Müller, J.
2018, XXXI, 652 S. 6 Abb., 4 Abb. in Farbe., Softcover
ISBN: 978-3-658-19124-5