February 2005

RFID als Technik des Ubiquitous Computing - Eine Gefahr für die Privatsphäre?

Jürgen Müller
Universität Kassel

Matthias Handy
Universität Rostock

In: Ferstl, Otto K, u.a. (Hg) 2005. *Wirtschaftsinformatik 2005: eEconomy, eGovernment, eSociety*; 7. Internationale Tagung Wirtschaftsinformatik 2005. Heidelberg: Physica-Verlag

ISBN: 3-7908-1574-8

RFID als Technik des Ubiquitous Computing – Eine Gefahr für die Privatsphäre?

Jürgen Müller
Universität Kassel

Matthias Handy
Universität Rostock

Zusammenfassung: In dem folgenden Beitrag werden in einer interdisziplinären Betrachtung rechtliche und technische Aspekte des Einsatzes von Funketiketten bzw. RFID-Systemen als wichtige Technik des „Ubiquitous Business" beleuchtet. An Hand von Anwendungskonstellationen wird die Einordnung von RFID-Systemen ins Telekommunikations-, Multimedia- und Datenschutzrecht vorgenommen. In diesem Beitrag werden mögliche Risiken des Einsatzes von RFID-Systemen aufgezeigt, um auf die datenschutzrechtlichen Prinzipien bezogenen Schutzbedarf abzuleiten. Zur Sicherung der datenschutzrechtlichen Zweckbindung werden unter anderem eine Anwendungskennung (AK) und eine Verwendungskennung (VK) vorgeschlagen, die bestimmte Verarbeitungsbeschränkungen von Daten gegenüber verantwortlichen Stellen deutlich machen.

Schlüsselworte: RFID-Techniken, Funketiketten, Datenschutzrecht, Risikoanalyse, Schutzbedarf, Ubiquitous Computing, Ubiquitous Business.

1 Einleitung

RFID-Systeme sind nur ein Aspekt einer größeren Entwicklung der Mikroelektronik und Informationstechnik hin zu einer Welt der allgegenwärtigen Rechnertechnik oder des Ubiquitous Computing. Ubiquitous Computing ist eine Technikvision, so Marc Weiser bereits 1991, deren Kernidee es ist, dass Mikroelektronik nach und nach in Gegenstände des täglichen Lebens eindringt und deren Funktionalität beträchtlich erweitert [Weis91]. Ziel des Ubiquitous Computing ist die „nachhaltige Unterstützung des Menschen sowie eine durchgängige Optimierung wirtschaftlicher Prozesse durch eine Vielzahl von in die Umgebung eingebrachter Mikroprozessoren und Sensoren" [LaMa03].

RFID-Systeme können einerseits als Basistechnologie des Ubiquitous Computing angesehen werden. Andererseits gelten sie auch als Wegbereiter einer derart in-

formatisierten Welt, da sie keine Extrapolation heute verfügbarer Technologien sind, sondern sich vielmehr bereits heute in unterschiedlichen Anwendungen einsetzen lassen.

Bei zunehmender Miniaturisierung, Verbesserung noch bestehender technischer Schwierigkeiten, Erhöhung der Speicherkapazität und Ergänzung weiterer Funktionalitäten sowie vor allem zunehmender Kostenreduzierung wird ein massenhafter Einsatz in vielen Alltagsfeldern erwartet. RFID-Systeme werden bereits heute beispielsweise zur Verfolgung von Ersatzteilen in der Montagereihe, zur Sortierung von Kleidungsstücken in Großwäschereien oder zur Identifikation von Kunden mit Hilfe von Kundenkarten eingesetzt. Ein größerer Einsatz von RFID-Systemen ist in Deutschland zur Fußball-Weltmeisterschaft 2006 geplant.

Die Einsatzmöglichkeiten von Funketiketten oder Radio-Frequency-Identification-Technik (RFID) werden von Verbraucher- und Datenschützern weltweit kritisch diskutiert. Auf der einen Seite verspricht sich die Industrie durch den Einsatz von RFID-Systemen, besonders im Logistikbereich, neue Möglichkeiten der kontaktlosen Produkterfassung, -verfolgung von Waren und von neuen Vertriebskonzepten, wie produktbezogene Kundeninformationssysteme, sowie Kostenersparnisse durch Effizienzsteigerungen. Auf der anderen Seite wird befürchtet, dass die informationelle Selbstbestimmung des Kunden durch versteckt angebrachte RFID-Marken an Gegenständen oder versteckt aufgestellte Lesegeräte beeinträchtigt würde.

2 Methodisches Vorgehen

Der vorliegende Beitrag verfolgt das Ziel, erste Ansätze zur verfassungsverträglichen Gestaltung der neuen RFID-Technik zu erarbeiten. Dabei werden Vorgehensweisen der Methode KORA zur Konkretisierung von rechtlichen Gestaltungsanforderungen [Roßn93] aufgegriffen und in die hier verwendete Methode zur rechtlichen Analyse neuer Technikentwicklungen überführt.

Nach einer Subsumtion der RFID-Systeme am geltenden Recht werden die sich hieraus ergebenden Rechtsfolgen hinsichtlich ihrer Tragfähigkeit für die neue RFID-Technik untersucht. Um erste technische und normative Gestaltungsvorschläge ableiten zu können, werden mit dem Einsatz von RFID-Systemen verbundene Risiken und bestehender Schutzbedarf in Rückbindung an Prinzipien und verfassungsmäßige Werte der Rechtsordnung diskutiert. Nicht alle fünf Schritte können im folgenden Beitrag in gleicher Ausführlichkeit dargestellt werden.

3 Grundlegendes zu RFID-Systemen

Ein RFID-System besteht in seiner einfachsten Form aus einem Lesegerät und aktiven bzw. passiven Transpondern (RFID-Marken). RFID-Lesegeräte setzen sich aus einer Steuerungseinheit und einer Hochfrequenzeinheit zusammen. Die Steuerungseinheit koordiniert und überwacht den Kommunikationsablauf mit dem Transponder, ist für die Signalcodierung und -decodierung verantwortlich und kommuniziert bei Bedarf mit einer Applikationssoftware auf einem angeschlossenen PC. Überdies wird die Steuerungseinheit zur Durchführung von Sicherheits- und Antikollisionsverfahren verwendet. Das HF-Interface erzeugt eine hochfrequente Trägerfrequenz und übernimmt die Aufgabe der Modulation bzw. Demodulation.

Eine passive RFID-Marke besteht üblicherweise aus einem Mikrochip (RFID-Chip) und einem Koppelelement (z.B. Antennenspule und Kondensator). Die erforderliche Energie wird bei passiven induktiv gekoppelten RFID-Marken dem magnetischen Wechselfeld des Lesegerätes entzogen. Handelsübliche passive RFID-Marken in Etikettenform sind zum Beispiel die von Texas Instruments angebotenen Tag-it HF-I Inlays [Texa02] oder die I-Code-SLI-Familie von Philips [Phil03]. Bei diesen auch als Smart Label bezeichneten Transpondern sind Koppelelement und Mikrochip (RFID-Chip) auf einer PET-Folie aufgebracht.

Weltweit federführend bei der Entwicklung von RFID-basierter Produktkennzeichnung ist EPCglobal, ein Gemeinschaftsunternehmen der europäischen EAN international und des US-amerikanischen Uniform Code Council (UCC). EPCglobal soll einen weltweiten Standard zur Produktkennzeichnung per RFID entwickeln. Kern dieser Produktkennzeichnung ist der Elektronische Produkt-Code (EPC), eine weltweit eindeutige Nummer, die einem Produkt zugewiesen wird und anhand derer es auf der gesamten Versorgungskette identifizierbar ist. Der EPC ist auf einem RFID-Chip gespeichert und kann von kompatiblen Lesegeräten ausgelesen werden. Der EPC ist eingebettet in das so genannte EPCglobal Network, einer Sammelbezeichnung für verschiedene Technologien, die mit der elektronischen Produktkennzeichnung verbunden sind (EPC tags, Lesegeräte, Object Name Service (ONS), Physical Markup Language (PML), Savant). Der Object Name Service gibt Auskunft darüber, wo Informationen zu dem entsprechenden Produktcode zu finden sind. Die Physical Markup Language ist eine standardisierte Form zur Beschreibung von Produktinformationen. Savant ist das zentrale Nervensystem des EPCglobal Network und verwaltet und transportiert sämtliche Informationen des Systems. Aktuell ist die Version 1 der EPC-Spezifikation verfügbar [Epcs04].

In den folgenden Ausführungen wird bei den auf der RFID-Marke gespeicherten Daten zwischen der Markenkennung (auch Kennung) und sonstigen Daten unterschieden. Dabei ist zu beachten, dass nicht alle RFID-Marken in der Lage sind, über die Kennung hinaus Daten zu speichern.

4 Rechtlich relevante Anwendungskonstellationen

Die derzeit diskutierten Anwendungsszenarien für Transpondertechnik lassen sich in verschiedene Kategorien von Anwendungen einordnen. So dienen an Produkten angebrachte RFID-Marken bzw. Funketiketten dem Kunden im Einzelhandel als elektronisches Kundeninformationssystem (Fallgruppe 1). Eine Erweiterung der Fallgruppe 1 würde sich ergeben, wenn das Funketikett am Produkt nicht nur durch ein Lesegerät vom Kunden ausgelesen werden kann, sondern der Einzelhändler dem Kunden an seinen Lesegeräten eine Funkschnittstelle anbietet, über die er die Informationen bzw. Daten des Funketiketts an einen PDA des Kunden beispielsweise übermittelt.

Hingegen verwendet eine Wäscherei, die in die Kleidungsstücke des Kunden eingenähte RFID-Marken als Informations- und Kennzeichnungssystem für Prozesssteuerung im eigenen Betrieb, (gleich einer an den Kunden ausgegebene Kundenkarte) deren Beschreiben und Auslesen ausschließlich durch die ausgebende Wäscherei erfolgt (Fallgruppe 2). Hierbei ist wichtig, dass der Kunde bzw. Betroffene über den Gebrauch der RFID-Marke hinaus, keinen Einfluss auf die Daten verarbeitenden Vorgänge besitzt.

Als dritte Fallgruppe sind Konstellationen einzuordnen, in denen Montageunternehmen oder Groß- bzw. Einzelhändler die RFID-Marken bzw. Funketiketten, die Paletten und Einzelprodukte markieren, ebenfalls nur intern für ihre eigenen Aufgaben in der Montagereihe oder in der Warenlogistik nutzen und nicht dem Kunden als Dritten, wie in der ersten Fallgruppe, anbieten.

Für eine rechtliche Betrachtung erscheinen im Blick auf den heutigen Stand der Technik drei Hauptkonstellationen maßgeblich, die auch in den Eingangs beschriebenen Anwendungsbeispielen angelegt sind:

- Funketiketten als Informations- und Kennzeichnungssystem für die Verwendung durch Dritte (Konstellation 1)
- Funketiketten als Informations- und Kennzeichnungssystem für die eigene Verwendung, bei Ausgabe derselben an den Betroffenen (Konstellation 2)
- Funketiketten als Informations- und Kennzeichnungssystem für die Verwendung im internen oder im zweiseitigen Verhältnis (Konstellation 3)

5 Rechtliche Einordnung

5.1 RFID-Kommunikation als Telekommunikation

Funketiketten bzw. RFID-Marken und die zum Auslesen und Beschreiben benötigten Lesegeräte sind technische Systeme, die elektromagnetische Signale senden, empfangen und steuern, die als Nachrichten [Bgeh30][1] zu identifizieren sind. Sie stellen Telekommunikationsanlagen im Sinn des § 3 Nr. 23 TKG (Telekommunikationsgesetz) dar, zwischen denen Telekommunikation im Sinn des § 3 Nr. 22 TKG stattfindet. Allerdings wird zwischen RFID-Marke und dem Lesegerät kein Telekommunikationsdienst, also Telekommunikation für Dritte angeboten.

Dies würde sich anders darstellen, wenn beispielsweise das RFID-Lesegerät des Einzelhändlers mit einer drahtlosen Schnittstelle ausgestattet wäre und so die Funketikettendaten an das mobile Endgerät (PDA) des Kunden als Dritten weitergeleitet würde (vgl. Erweiterung der Fallgruppe 1). Dadurch erbrächte der Einzelhändler als Betreiber dieser Übertragungswege geschäftsmäßig Telekommunikationsdienste gemäß § 3 Nr. 10 TKG. In diesem Fall gälten dann weitergehende Pflichten des TKG.

5.2 RFID-System als Teledienst

Ein Teledienst wird gemäß § 2 Abs. 1 TDG als ein elektronischer Informationsdienst zur individuellen Nutzung von kombinierbaren Daten begriffen, der auf Übertragungsvorgänge der Telekommunikation beruht.

5.2.1 Grundintention des Teledienstegesetzes

Obwohl die Normierung des Teledienstegesetzes das sich verbreitende Internet mit seinen verschiedenen Anwendungen im Blick hatte, [Btds13], ist es von seiner Grundkonzeption technikoffen ausgestaltet. Mit dem Gesetz soll der tiefgreifende „Wandel zur Informationsgesellschaft aktiv gestaltet“ [Btds13] werden.

So erfasst das TDG die RFID-Technik als eine weitere Nutzungsmöglichkeit im sich entwickelnden elektronischen Markt.

5.2.2 Übermittlung mittels Telekommunikation

Die Übermittlung der Kennung und der weiteren auf der RFID-Marke abgelegten Daten erfolgt, wie festgestellt, mittels Telekommunikation, welche lediglich Mittel und nicht alleiniger Zweck des Angebots ist [Spin01].

---

[1] Der Begriff der Nachricht ist nach [Bgeh30] weit auszulegen.

5.2.3 Von kombinierbaren Daten: Wie Zeichen, Bilder oder Töne

Der § 2 Abs. 1 TDG beschreibt „elektronische“ Informationsdienste als Nutzung „von kombinierbaren Daten“. Durch diese Formulierung sollen Angebote mit multimedialem Charakter von monomedialen Diensten (z.B. klassische Sprachtelefonie) abgegrenzt werden. Dabei legt das Wort „kombinierbar“ nahe, dass es nicht auf die konkrete Realisierung der Multimedialität ankommt, sondern die Möglichkeit des Angebots maßgeblich sein soll. Um nun mit einer Auslegung aus einer rein technischen Sicht das Tatbestandsmerkmal nicht weitgehend bedeutungslos werden zu lassen, muss dieses funktional verstanden werden, weil digitale Daten von der Möglichkeit ihrer Abbildung grundsätzlich technisch jeder Darstellungsform zugänglich sind [Enge01]. Daher kann auf den gewöhnlichen Gebrauch eines Angebots, wie er in seiner Konzeption angelegt ist, abgestellt werden. So kommt den im Speicherbereich für sonstige Daten auf einer RFID-Marke abgelegten Daten die Eignung als Inhalt eines Teledienstes zu. Dies setzt aber voraus, dass die Nutzung dieser sonstigen Daten - was in einer mittelfristigen Entwicklungsperspektive möglich erscheint - multimedial gedacht ist.

Selbst wenn noch keine Multimedialität für Daten der RFID-Marke vorgesehen ist, würden diese unter § 2 Abs. 1 TDG einzuordnen sein, falls die RFID-Marke eine Art Sprung- oder Verknüpfungsadresse in ein Intra- oder Internet-Angebot trägt, das seinerseits einen Teledienst darstellt.

5.2.4 Zur Nutzung bestimmt

Zudem muss nach § 2 Abs. 1 TDG der elektronische Informationsdienst zur Nutzung bestimmt sein. Dies setzt ein Anbieter-Nutzer-Verhältnis voraus.

- Anwendbarkeit in geschlossenen Nutzergruppen

Ein Anbieter-Nutzer-Verhältnis ist nicht schon dadurch ausgeschlossen, dass der Informationsdienst in einer geschlossenen Benutzergruppe (Intranet) angeboten wird [Enge97, Wald00.1, Btds14]. So kann der Einsatz von RFID-Systemen innerhalb eines Betriebes oder zwischen Unternehmen (z.B. in der Lagerhaltung oder bei der Verfolgung von Gütern in der Logistikkette) gleichwohl ein Teledienst sein. Im Arbeitsverhältnis als einer der Hauptfälle eines internen Diensteangebots fehlt es jedoch an dem Anbieter-Nutzer-Verhältnis.

- Anbietereignung

Eine Person ist Anbieter (§ 3 Nr. 1 TDG), wenn sie einen Teledienst bereithält [Wald00.2], indem sie ihn als eigenen organisatorisch und technisch in seinem Machtbereich selbst erbringt oder einen fremden Teledienst speichert, und damit zur Nutzung vorhält. Hiernach würde beispielsweise der Einzelhändler im beschriebenen Einkaufsszenario zum Anbieter, der in seinem Ladengeschäft abrufbare Inhalte auf den RFID-Marken, mit denen die bei ihm vorgehaltenen Produkte

markiert sind, anbietet. Dabei kann schlichter Besitz gemäß § 854 Abs. 1 BGB nicht genügen.

So bedarf es, neben dem tatsächlichen, an den Umstand der Funktionsherrschaft angeknüpften Angebot, was Anbieten schon begrifflich voraussetzt, eines Wissens- und Willenselementes auf Seiten des Anbieters, sonst würde er schon deshalb zum Anbieter von Telediensten, wenn diese in seinem Herrschaftsbereich benutzbar zur Verfügung stünden, obwohl er die Dienste nur zu seinen eigenen Zwecken, etwa für seine Logistikaufgaben einsetzt.

Neben Argumenten der Wortlautauslegung und der historischen Entwicklung sprechen auch Sinn und Zweck der Vorschrift dafür, die Verantwortlichkeit für Inhalte nicht an das Vorhandensein einer Art Zustandsverantwortlichkeit [Fria99], sondern an ein zurechenbares Handeln anzuknüpfen.

Das Erfordernis eines subjektiven Elements als Voraussetzung für die Anbieterstellung muss beim Einsatz von RFID-Technik gesondert festgestellt werden, da anders als bei Angeboten im Internet, die durch das Bereitstellen einer HTML-Seite mittels aktiven Tuns in die abgeschlossene, virtuelle Welt des Netzes, also zwangsläufig willentlich eingestellt wurden, RFID-Marken in der körperlichen Welt eingebracht werden und zunächst einfach vorhanden sind.

- An eine Person ausgegebene RFID-Marken

Bei RFID-Marken, mittels derer als digitale Legitimations-, Zugangsberechtigungs- oder Kundenkarten Daten für die Geschäftsbeziehung ausgetauscht werden, fehlt es an einem Anbieter-Nutzer-Verhältnis, wenn dem Karteninhaber über den bloßen Gebrauch hinaus, die Möglichkeit entzogen ist, Einfluss auf die Daten verarbeitenden Vorgänge beispielsweise durch Löschung oder Änderung der abgespeicherten Informationen zu nehmen.

Anders beurteilt sich die Verwendung von ausgegebenen RFID-Marken, wenn der Inhaber die Verarbeitungsvorgänge auf der Marke kontrollieren kann. Dabei kann der Karteninhaber nach § 3 Nr. 1 TDG auch für Inhalte der ausgebenden Stelle Anbieter eines dann „fremden Teledienstes“ (§ 11 TDG) sein. Insoweit kommt ihm sachgerecht die Haftungsfreistellung des § 8 Abs. 2 TDG in Verbindung mit § 11 TDG zugute.

5.2.5 Ergebnis

Im Ergebnis wird ein Teledienst angeboten, wenn Daten von Funketiketten bzw. RFID-Marken als Informations- und Kennzeichnungssystem gegenüber Dritten mit multimedialem Charakter bereitgehalten werden. RFID-Marken, die an Betroffene ohne ihren Einfluss auf Funktion ausgegeben werden oder die nur im internen und zweiseitigen Verhältnis Verwendung finden, werden vom TDG nicht erfasst. Allerdings ergibt sich, anders als in einer rein virtuellen Welt, die Schwie-

rigkeit, wie dieser zunächst inwendige Willen zum Angebot nach außen erkennbar wird.

5.3 Anforderungen des Telekommunikations-, Multimedia- und Datenschutzrechts

In allen Anwendungskonstellationen bleibt im Telekommunikationsrecht § 89 TKG anwendbar, der jede Funkkommunikation vor dem Abhören durch Dritte unabhängig vom Vorliegen eines Telekommunikationsdienstes schützt. Obwohl der Kommunikationsvorgang vom Lesegerät initiiert und gesteuert wird, steht das unbefugte Auslesen und Beschreiben einer RFID-Marke unter Strafe (§ 148 Abs. 1 Nr. 1 TKG) [Müll04].

Für Teledienste wurden zur Wahrung von schutzwürdigen Interessen der Nutzer vornehmlich besondere Informationspflichten (§ 6, § 7 TDG, § 312e BGB) und Haftungspriviligierungen für fremde Inhalte (§§ 8 Abs. 2, 9 ff TDG) normiert. Diese passen auf RFID-Systeme nur in Einzelpunkten. Zwar wäre die Anbieterkennzeichnung (AKZ) nach § 6 TDG beispielsweise wegen des Angebots von Daten in elektronischer Form über Telekommunikation und der dadurch bestehenden Flüchtigkeit der Informationen und räumlichen Distanz zum Angebot angezeigt. Aber weil RFID-Marken an Gegenständen angeheftet sind, erscheint das mit § 6 TDG verfolgte Ziel lebensfremd, zumal dieser durch entsprechende Aufdrucke auf der Verpackung oder am Warenregal zweckmäßig erfüllt wird. Abgesehen davon würde die Speicherkapazität heutiger RFID-Marken für eine AKZ nicht ausreichen.

Für personenbezogene Daten sieht das bereichsspezifische Teledienstedatenschutzgesetz (TDDSG) besondere Zulassungstatbestände für Bestands- und Nutzungsdaten (§ 5, § 6 TDDSG) sowie besondere Zweckbindungsregeln vor. Diese gehen vielfach ins Leere. Begründet liegt das in dem Umstand, dass durch das TDG und TDDSG der Anbieter als Normadressat verpflichtet wird, wobei der Nutzer die RFID-Kommunikation über das Lesegerät initiiert. Zudem finden auf einer RFID-Marke neben Speichern (§ 3 Abs. 4 Nr. 1 BDSG [Bundesdatenschutzgesetz]) und Übermitteln in Form des Bereithaltens (§ 3 Abs. 4 Nr. 3 BDSG) keine weiteren Daten verarbeitenden Vorgänge, wie Erheben (§ 3 Abs. 3 BDSG) und Nutzen (§ 3 Abs. 5 BDSG) statt. Ebenso tragen die Anforderungen des BDSG den spezifischen Bedingungen von RFID-Systemen keine Rechnung. Insbesondere § 6c BDSG, der besondere Pflichten für „mobile personenbezogene Speicher- und Verarbeitungsmedien“, also für Chip-Karten (§ 3 Abs. 10 BDSG) vorsieht, findet auf RFID-Marken keine Anwendung, weil gemäß § 3 Abs. 10 Nr.2 BDSG auf

dem Medium eine über die Speicherung hinausgehende Verarbeitung[2] erfolgen muss [Horn04].

Merkmal	TK-Recht	Multimediarecht	Datenschutzrecht
Konstellation 1[3]	kein TKG[4] , aber § 89 TKG.	kein TDG für RFID-Kennung; jedoch für sonstige Daten im Speicher	BDSG für RFID-Kennung
Konstellation 2	kein TKG, außer § 89 TKG	kein TDG für RFID-Kennung u. sonstige Daten im Speicher	BDSG für RFID-Kennung und für sonstige Daten im Speicher (aber derzeit kein §6c BDSG)
Konstellation 3	kein TKG, aber § 89 TKG	kein TDG für RFID-Kennung und kein TDG für sonstige Daten im Speicher	BDSG für RFID-Kennung und für sonstige Daten im RFID-Speicher

Tabelle 1: Überblick über anwendbares Recht

6 Risiken von RFID-Systemen

6.1 Möglichkeiten auf Grund der technischen Bedingungen

Nachdem das geltende Recht RFID-Systeme nur unvollständig erfasst, gilt es die Risiken durch den Einsatz von RFID-Systemen zu analysieren und hieraus einen Schutzbedarf abzuleiten. Auf Grund der technischen Bedingungen lassen sich für RFID-Systeme vornehmlich als technische Bedingungen festhalten, dass sie in extrem kleinen Baugrößen mit einer Funkschnittstelle auf verschiedenen flexiblen Trägermaterialien[5] aufgebracht werden können und alle RFID-Marken mittels Antikollisionsverfahren in der Reichweite des Lesegerätfeldes erfasst werden. Hieraus ergibt sich die Möglichkeit, RFID-Marken nicht nur sichtkontaktlos auszulesen, sondern auch mit Gegenständen unlösbar zu verbinden, unsichtbar zu platzie-

2 Hier wird auf den weiteren Begriff des § 3 Abs. 2 BDSG zur automatisierten Verarbeitung Bezug genommen.

3 Vorausgesetzt wird, dass die sonstigen Daten in der Anwendungskonstellation 1 auch für eine multimediale Verwendung vorgesehen sind.

4 außer bei Kommunikationsschnittstelle an nutzerfremdem Lesegerät.

5 Als Bestandteil von Verpackungsfolien, Aufdruck auf Polymerbasis möglich.

ren und fast an und in jeden Gegenstand einzubringen. Dabei erfolgt die Erfassung verhältnismäßig einfach, schnell und nahezu gleichzeitig.

RFID-Technik zeichnet sich daneben dadurch aus, dass die RFID-Marken mit einer weltweit eindeutigen Kennung und optional mit einem zusätzlichen Speicher für sonstige Daten ausgestattet sind sowie in ein Hintergrundsystem[6] mit weiterführenden Daten eingebunden werden können. Dies bedeutet die Identifizierbarkeit der RFID-Marke mit einer Art mehr oder weniger aussagekräftigen inhaltlichen Identität, je nach Umfang und Güte der auf der Marke selbst oder im ergänzenden Hintergrundsystem nachgewiesenen Daten.

Allerdings fehlt es bei RFID-Marken neben dem Lesegerät an einem direkten Ein- und Ausgabemedium, was keine Registrierbarkeit der Daten verarbeitenden Vorgänge im aktuellen Zeitpunkt erlaubt. Ebenso findet auf derzeitigen Marken keine Zugangs-[7] und Zugriffskontrolle[8] oder wenigstens eine Zugriffsprotokollierung statt. Dies bedeutet, dass die auf einer RFID-Marke abgelegten Daten hinsichtlich Auslesbarkeit und Manipulation offen zugänglich sind und keine Kontrolle über die Daten weder präventiv noch nachträglich ermöglichen.

Gleiches gilt für die Übertragung oder Kommunikation mit dem Lesegerät, die ebenfalls ungeschützt in Ermangelung kryptografischer Sicherungen abgewickelt wird. Diese Funkkommunikation ist aber in ihrer Reichweite sehr begrenzt, wodurch im Kreis der Reichweite eine gewisse Überschaubarkeit gewahrt bleibt.

6.2 Folgen der Möglichkeiten von RFID-Technik

Die Möglichkeit der sichtkontaktlosen Kommunikation führt zu Unmerklichkeit der Technik und zu einer gewissen räumlichen Distanz von der RFID-Marke zum Verwender derselben, wie bei elektronischen Informations- und Kommunikationsangeboten in der virtuellen Welt.

Ebenso wird die Unmerklichkeit der aktuell stattfindenden und erfolgten Daten verarbeitenden Vorgänge durch die fehlenden Möglichkeiten begünstigt, diese Vorgänge präventiv oder nachträglich zu registrieren. Damit vermag eine Person als RFID-Marken-Inhaber auf Markenzugriffe unter Berücksichtigung der aktuellen Situation, in der gerade ein solcher Auslese- oder Schreibvorgang stattfindet, nicht zu reagieren oder einzuschreiten. Ihm fehlt auch das Wissen, ob und auf welche Weise in einem bestimmten, zurückliegenden Zeitraum Zugriffe auf die RFID-Marke erfolgten.

Neben der Unmerklichkeit entstehen durch die Verbindung der RFID-Marken mit Gegenständen Kontextdaten, die zwangsläufig einen Gegenstandsbezug aufwei-

---

6 Vgl. Ausführungen zum Object Name Service (ONS).

7 Authentifikation des Lesegeräts.

8 Verwaltung von Lese- und Schreibrechten.

sen. Hinzu tritt die Unlösbarkeit der RFID-Marke vom Gegenstand, sodass sich diese in das mit dem betreffenden Gegenstand verbundene Handeln der Menschen integriert, aber auch ein Kontrollverlust über die RFID-Technik durch ihre Verwendung eintritt. Dagegen liegt in der Möglichkeit der schnellen, einfachen und quasi gleichzeitigen Erfassung die Voraussetzung eines allgegenwärtigen Einsatzes.

Das wichtigste Kennzeichen der RFID-Technik, die Identifizierbarkeit der Marken, hat zur Folge, dass die RFID-Marken durch das RFID-System wiedererkannt, zu Gegenständen und Personen zugeordnet, zu anderen, ebenfalls markierten Gegenständen in Beziehung gesetzt und aus einer Zusammenschau Muster erkannt werden können. Die Art inhaltliche Identität bringt ein markenimmanentes Kontextwissen und bessere Einordenbarkeit beim Wiedererkennen einer RFID-Marke und beim Erkennen von Mustern mit sich. Verschärft wird dies durch die Möglichkeit über Hintergrundsysteme weiterführende Daten über die RFID-Marke und damit über den markierten Gegenstand gleich eines Gedächtnisses abzufragen, wobei hierdurch zusätzlich Datenspuren, insbesondere über Bewegungsprofil der einzelnen RFID-Marke über den Standort des abfragenden Lesegeräts entstehen.

Nachdem die Daten auf der RFID-Marke und die Funkkommunikation zum Lesegerät ungeschützt zugänglich sind, lässt sich ein unbefugtes Auslesen und Abhören der gespeicherten bzw. übermittelten Daten nicht verhindern. Dies birgt zudem die Gefahr der Manipulation der Daten auf der Marke in sich.

6.3 Verletzungspotentiale von Rechtsgütern

Die RFID-Technik ist eine Informations- und Kommunikationstechnik, die auf der einen Seite im virtuellen Sozialraum angesiedelt ist und auf der anderen Seite durch die Verknüpfung zu einem körperlichen Gegenstand im realen Sozialraum präsent ist. Dadurch sind nicht nur das Eigentumsrecht (Art. 14 GG) und die Handlungsfreiheit (Art. 2 Abs. 1 GG), sondern vor allem auch das Brief-, Post- und Fernmeldegeheimnis (Art. 10 GG) und das Grundrecht der informationellen Selbstbestimmung (Art. 1 Abs. 1, Art. 2 Abs. 1 GG) betroffen.

6.3.1 Grundrecht des Fernmeldegeheimnisses

Das Grundrecht des Brief-, Post- und Fernmeldegeheimnisses schützt die Vertraulichkeit der Kommunikation. Das in § 89 TKG normierte Abhörverbot trägt diesem Grundrecht Rechnung.

Im praktischen Umgang besteht die Schwierigkeit für den Verwender einer RFID-Marke, die subjektive Bestimmung der abgefragten und/oder empfangenen Daten durch den Markeninhaber, also das Befugtsein des RFID-Marken-Verwenders erkennen zu können.

6.3.2 Recht der informationellen Selbstbestimmung

Personenbezogene Daten[9] und deren Erhebung (§ 3 Abs. 3 BDSG), Verarbeitung (§ 3 Abs. 4 BDSG) und Nutzung (§ 3 Abs. 5 BDSG) werden durch das Grundrecht der informationellen Selbstbestimmung [Bveg65] (Art. 1 Abs. 1 GG i. V. m. Art. 2 Abs. 1 GG) geschützt, welches durch das Datenschutzrecht konkretisiert wird [Podl04].

Dabei entsteht bei dem Einsatz der zunächst datenschutzrechtlich neutralen RFID-Technik eine datenschutzrechtliche Relevanz dann, wenn auf dem RFID-Speicher selbst personenbezogene Daten abgelegt werden oder wenn die RFID-Marke mit ihrer Kennung (UID) oder den sonstigen abgespeicherten Daten (ggf. über den sie tragenden Gegenstand) einer Person zugeordnet werden kann. Für die Anwendbarkeit des Datenschutzrechts reicht aus, wenn die Person, auf die die zu schützenden Daten bezogen sind, lediglich bestimmbar [Damm03], also die Ermittelung auch unter Zuhilfenahme von Zusatzwissen nach allgemeiner Lebenserfahrung nicht ausgeschlossen ist.

7 Überlegungen zum Schutzbedarf

Durch den Einsatz von RFID-Systemen entstehen qualitativ neue Risiken. Zur Gewährleistung des Fernmeldegeheimnisses und der informationellen Selbstbestimmung bedarf es der Umsetzung von Schutzanforderungen.

Die Auswahl der Anforderungen ist nach den Rechten oder Prinzipien gegliedert, aus denen sich diese ableiten lassen.

- Eigentums- und Besitzrecht

Rechte, wie etwa §§ 985, 903 BGB oder §§ 858 Abs. 1, 862 Abs. 1BGB, die sich aus einer Eigentumsposition (§ 903 BGB) oder einer Besitzposition (§ 862 Abs. 1 BGB) ergeben, würden das Entfernen und Deaktivieren einer an einem Gegenstand angehefteten RFID-Marke erlauben. Bei Fremdbesitz (e contrario § 872 BGB), wenn zum Beispiel ein Kunde ein RFID-markiertes Fahrrad mietet, kann ein Deaktivierungsverlangen nicht auf § 858 BGB gestützt werden, da keine Störung in dem eingeräumten Besitzrecht vorliegt.

[9] Gemäß § 3 Abs. 1 BDSG Angaben über Verhältnisse einer zumindest bestimmbaren Person.

- Datensparsamkeit

Dem präventiven Gestaltungsgebot der Datensparsamkeit nach § 3a BDSG lässt sich die Forderung entnehmen, dass RFID-Systeme datenschutzgerecht zu gestalten sind und damit als ein potentieller Gegenstand von Datenverarbeitung deaktivierbar sein müssen.

- Technisch-organisatorischer Schutz

Auf Grund von § 9 BDSG, der zur Durchsetzung der im Datenschutzrecht niedergelegten Anforderungen technisch organisatorische Maßnahmen verlangt, sind Schutzmaßnamen zu implementieren, die die RFID-Kommunikation gegen Kenntnisnahme durch Dritte und die personenbezogenen Daten auf den RFID-Marken vor unbefugtem Zugang und Manipulation sichern.

- Transparenzprinzip

Um dem Betroffenen die Verwirklichung seiner informationellen Selbstbestimmung zu ermöglichen, bedarf es an Transparenz der Daten verarbeitenden Vorgänge. Daher muss zum einen hinsichtlich des Einsatzes von RFID-Systemen ein Wissen um Art, Umfang und Struktur der Daten verarbeitenden Vorgänge, insbesondere die Weise der Einbindung in ein Hintergrundinformationssystem (z.B. ONS) sicher gestellt werden. Zum anderen muss die Verwendung der personenbezogenen Daten sowie ihre Art und ihr Inhalt von der verantwortlichen Stelle dargelegt werden. Daneben gilt es, die erfolgenden Daten verarbeitenden Vorgänge auf der RFID-Marke sowie die stattfindende Kommunikation zwischen Marke und Lesegerät erkennbar zu machen.

Als ein Problem grundsätzlicherer Natur stellt sich das Erfordernis dar, einmal die Zweckbindung und zum anderen die Adressatenbestimmung der personenbezogenen Daten erkennbar zu machen.

- Zweckbestimmung und Zweckbindung

Die datenschutzrechtliche Zweckbindung soll sicherstellen, dass der Einzelne darauf vertrauen kann, dass die Datenverarbeitung nur zu dem von ihm oder dem Gesetz erlaubten Zweck erfolgt. Ein besonderes Risiko für die personenbezogenen Daten entsteht, wenn diese über die Erhebung von der RFID-Marke hinaus gespeichert und vor allem genutzt werden. Deutlich wird das am Beispiel einer verantwortlichen Stelle, die ein gewerbliches Interesse an den Daten hat. Daher muss, wenn schon technisch das Auslesen einer RFID-Marke nur schwer markenseitig gesteuert werden kann, zumindest die Weiterverarbeitung und zweckwidrige Verwertung ausgeschlossen werden. Bei dem technischen Stand derzeitiger RFID-

Systeme bietet sich als Behelfslösung[10] an, die vorgesehenen Verarbeitungszwecke durch Klassifizierungen zu steuern.

- Informationelle Gewaltenteilung

Durch die informationelle Gewaltenteilung [Bveg65] sollen bereichsspezifisch unterschiedliche Datenflüsse und -bestände gemäß des Zweckbindungsprinzips streng getrennt gehalten werden. Manche Spezifikationen von RFID-Marken sehen in der Kennung neben der Seriennummer vor, auch Daten inhaltlicher Natur abzulegen (vgl. Funketiketten nach dem EPC-Standard). Bei der ersten Anfrage des Lesegeräts (mit dem „Inventory-Befehl“) wird aber die Kennung in Gänze ausgelesen. So sollten innerhalb der RFID-Kennung Daten mit Seriennummernfunktion und Daten mit inhaltlicher Bestimmung getrennt sein.

8 Gestaltungsvorschläge

8.1 Vorüberlegungen

In diesem Abschnitt werden Möglichkeiten zur Eindämmung der bestehenden Risiken beschrieben. Dabei wird auf drei der angesprochenen Problembereiche eingegangen. Zunächst werden die Gefährdungslage beim Eigentumsübergang von mit RFID markierten Produkten sowie bereits existierende und neue Lösungsideen diskutiert. Weiterhin werden in diesem Abschnitt Gestaltungsideen vorgestellt, mit denen das Einsatzfeld und die angedachte Verwendung von RFID-Marken angezeigt werden können, um unerwünschte Auslesevorgänge zu vermeiden bzw. zu verhindern.

Prinzipiell lässt sich ein RFID-System bestehend aus Marken und Lesegeräten mit herkömmlichen kryptografischen Verfahren gegen Angriffe sichern. Die besonderen Eigenschaften solcher Systeme erschweren jedoch die direkte Übertragung von Verfahren, wie sie beispielsweise bei Smart Cards zum Einsatz kommen. Dies ist zum einen bedingt durch den drahtlosen Kommunikationskanal eines RFID-Systems, der den Schutz des Systems vor Abhörangriffen erschwert. Überdies sind kryptografische Verfahren auf (für RFID-Systeme) verhältnismäßig viel Speicher angewiesen. Auch die Energieversorgung und die Taktfrequenz sind oft nicht ausreichend um aufwändige Verschlüsselungsverfahren durchzuführen.

[10] Aber auch mit dem Vorteil, die Komplexität von Verarbeitungsvorgängen reduzieren zu helfen und dadurch verloren gegangene Transparenz wiederzugewinnen.

Für viele Anwendungen sind kryptografische Verfahren, wie Authentifizierung oder Verschlüsselung, einfach nicht erforderlich beziehungsweise nicht erwünscht. Es macht zum Beispiel wenig Sinn, in einem innerbetrieblichen Produktionsprozess, bei dem Einzelteile und Baugruppen mit RFID-Marken versehen sind und so auf ihrem Weg durch das Unternehmen genau verfolgt werden können, derartige Mechanismen einzusetzen. Die Gefahr des unerlaubten Auslesens der Marken ist dort als eher gering einzuschätzen. Außerdem besteht bei den verwendeten Daten (noch) kein Personenbezug, der als schützenswert einzustufen wäre.

Schließlich erhöht die Integration kryptografischer Verfahren in RFID-Systeme den Preis solcher Systeme, vor allem den aus ökonomischen Gesichtspunkten kritischen Preis je RFID-Marke. Für einen weiträumigen Einsatz von RFID-Systemen beispielsweise im Einzelhandel ist jedoch ein möglichst niedriger Stückpreis entscheidend.

Bei allen hier präsentierten Gestaltungsvorschlägen ist zu berücksichtigen, dass für RFID-Systeme kein einheitlicher Standard existiert. Vielmehr gibt es eine Vielzahl von Normen und Standards für RFID-Systeme mit unterschiedlichen Charakteristika und Einsatzzwecken.[11] Die präsentierten Gestaltungsideen sind möglichst generisch verfasst und sollen als Grundstein für eine derzeit noch hypothetische Meta-Norm für alle RFID-Systeme dienen, die Problembereiche der informationellen Selbstbestimmung und des Datenschutzes berühren.

8.2 Übergabe von Artikeln mit RFID-Marken

Eine besondere Problemlage entsteht beim Eigentumsübergang von mit RFID-Marken ausgestatteten Produkten, beispielsweise an der Kasse eines Supermarktes. Die RFID-Marke, die auf ihrem bisherigen Weg durch die Lieferkette ihre Dienste verrichtet hat, wird nun zur Gefahr für die Privatsphäre des neuen Eigentümers, wenn er anhand der Markenkennung identifiziert werden kann. Vorstellbar wäre dies durch eine Verknüpfung der Markenkennung mit der Person des Käufers durch ein identifizierendes Bezahlungssystem, zum Beispiel bei Bezahlung mit einer Kundenkarte.

Um dieser Gefährdung zu begegnen, wurden bereits verschiedene Verfahren entwickelt. Diese lassen sich in zwei große Gruppen einteilen. In der ersten Gruppe sind Verfahren angesiedelt, die ein Auslesen der RFID-Marken durch fremde, d.h. nicht autorisierte Lesegeräte unterbinden oder stören. Dazu gehören das Jamming

[11] Für Logistikanwendungen existieren unter anderem die Normen ISO/IEC 18000, ISO/IEC 15961-15963 sowie ISO/IEC 15418. Die Normen ISO 11784, 11785 sowie 14223 befassen sich mit der automatischen Identifikation von Nutztieren. Normen für kontaktlose Identifikationskarten werden in ISO/IEC 10373, 10536, 14443 sowie 15693 beschrieben.

und der so genannte Blocker-Tag [Jue+03]. Das Jamming verwendet einen Störsender der die Kommunikation zwischen Lesegerät und RFID-Marke komplett unterbindet. Das Blocker-Tag stört diese Kommunikation nur dann, wenn das Lesegerät spezielle, als privat gekennzeichnete, Markenkennungen abfragen will. Im einfachsten Fall könnte der Adressraum von RFID-Marken in eine private und eine öffentliche Zone aufgeteilt werden. Alle privaten RFID-Marken haben eine Kennung beginnend mit einer 0, alle öffentlichen RFID-Markenkennungen beginnen mit einer 1. Sobald ein Lesegerät versucht, im privaten Adressbereich nach RFID-Marken zu suchen, wird das Blocker-Tag aktiv und stört diesen Vorgang, indem es dem Lesegerät vorgaukelt, es wären Millionen von RFID-Marken vorhanden. Das Lesegerät kann daraufhin real vorhandene RFID-Marken nicht mehr erkennen. Beim Eigentumsübergang muss bei diesem Verfahren die Kennung der RFID-Marke angepasst werden.

Verfahren, die wie beim Jamming oder beim Blocker-Tag die Kommunikation zwischen Lesegerät und RFID-Marke aktiv stören, sind als rechtlich bedenklich einzustufen. Zwar fallen sie nicht unter § 317 StGB (Störung von TK-Anlagen), sie sind jedoch gegebenenfalls als Ordnungswidrigkeit nach FTEG einzuordnen.

Eine zweite große Gruppe verändert die Markenkennung beim Eigentumsübergang. Beim Meta-ID-Verfahren antwortet die RFID-Marke nach einem Sperrvorgang nicht mehr mit ihrer originären Kennung, sondern mit einer so genannten Meta-ID [Sar+02]. Die eigentliche Kennung der RFID Marke erfährt nur derjenige, der den geheimen Schlüssel kennt, mit der die Meta-ID erzeugt wurde, und diesen an die RFID-Marke sendet. Die RFID-Marke bildet aus dem empfangenen Schlüssel die dazugehörige Meta-ID und vergleicht diese mit der gespeicherten Meta-ID. Bei Gleichheit wird die RFID-Marke entsperrt und die Klardaten werden an das Lesegerät übertragen. Dieses Verfahren nutzt das Prinzip der Einweg-Hashfunktionen: aus dem geheimen Schlüssel lässt sich problemlos die dazugehörige Meta-ID berechnen, es ist jedoch sehr schwierig, aus der Meta-ID den geheimen Schlüssel zu berechnen [Schn96].

Beim Kill-Tag-Ansatz wird die RFID-Marke durch einen speziellen Befehl des Lesegerätes komplett und unwiederbringlich deaktiviert [Epcs04]. Problematisch wird dieses Verfahren, wenn der Kunde einen gekauften Artikel wieder in den Laden zurückbringt. Der Artikel muss dann wieder in das Warenwirtschaftssystem eingegliedert werden, wozu das Anbringen einer neuen Marke erforderlich wäre. Der Artikel bekäme dann praktisch eine neue Identität. Bei Regressansprüchen ist man jedoch auf Informationen der „vergangenen“ Identität des Artikels angewiesen. Überdies kann der Käufer eines Artikels mit deaktivierter RFID-Marke den Mehrwert dieses Kennzeichnungsverfahrens nicht für private Zwecke nutzen. Der „intelligente Kühlschrank“ würde dann nicht mehr funktionieren.

Wir schlagen als Gestaltungsidee einen modifizierten Kill-Befehl vor, der anders als das bisherige Verfahren nicht die komplette Markenkennung löscht, sondern nur den eindeutig identifizierenden Teil dieser Kennung. Die eindeutige Serien-

nummer eines Artikels wird gelöscht oder gegebenenfalls durch eine private Inventarnummer ersetzt, die Objektklasse des Artikels bleibt jedoch erhalten. Dies beschränkt die Aussagekraft der RFID-Marke auf die eines Barcodes. Beim EPC setzt sich eine Kennung nach SGTIN-96 (Serialized Global Trade Identification Number) unter anderem aus einer Herstellerkennung (Company Prefix), einer Artikelreferenz (Item Reference) und einer 38-bit langen Seriennummer zusammen. Unser Ansatz deaktiviert die Seriennummer; Herstellerkennung und Artikelreferenz (Objektklasse) bleiben erhalten. Damit lassen sich RFID-Marken auch nach dem Kauf nutzen.

Ein zweiter Gestaltungsvorschlag betrifft die Infrastruktur eines serverbasierten, überregional vernetzten RFID-Systems, wie es vom ECPGlobal-Konsortium vorgeschlagen wird [Epcs04]. Dabei geht es um die Auflösung des Zusammenhangs zwischen RFID-Marke und eindeutig identifizierbarem Gegenstand. Eine RFID-Marke speichert eine Objektidentität gewöhnlich als Bit-Serie, beim EPC zum Beispiel mit einer Länge von 64 oder 96 bit. Die wahre Identität und ein möglicher Personenbezug lassen sich jedoch erst nach einer Decodierung dieser Bitserie herstellen. Dies geschieht beim EPC durch Anfrage bei einem ONS-Server (Object Name Service), der Zugriff auf eine verteilte Datenbank hat, die zu einer EPC-Nummer weiterführende Informationen abspeichert. Ein ONS-Server kann überdies zur Aufzeichnung eines Bewegungsprofils verwendet werden, indem er Orte und Zeiten von Auslesevorgängen einer RFID-Marke abspeichert.

Wir schlagen eine Löschung des ONS-Eintrages (oder des Eintrages in einer vergleichbaren Datenbank eines anderen Systems) vor, um die Privatsphäre des Eigentümers eines Produktes mit RFID-Marke besser zu schützen. Es lässt sich zwar weiterhin die RFID-Marke mit jedem Lesegerät auslesen, weiterführende Informationen eventuell mit Personenbezug können damit jedoch nicht erlangt werden. Alternativ zu einer Löschung des ONS-Eintrages könnte eine Zugangsbeschränkung zu einem derartigen System eingeführt werden. Es kann dann zwar jeder eine Anfrage an das ONS-System stellen, Antworten erhält jedoch nur, wer sich vorher als berechtigt authentifiziert hat.

8.3 Kennzeichnung der Zielanwendung und des Verwendungszwecks einer RFID-Marke

Wie kann ein Lesegerät erkennen, für welche Anwendung eine bestimmte RFID-Marke arbeitet? Eine Waschmaschine, die ihr Waschprogramm anhand der erkannten RFID-Marken der in ihr enthaltenen Kleidungsstücke auswählt, sollte auch nur diejenigen Marken auslesen, die zu dieser speziellen Anwendung gehören. Wir schlagen dafür die Einführung einer *Anwendungskennung* (AK) vor, für die ein Speicherabschnitt auf der RFID-Marke reserviert ist. Dabei wird gefordert, dass eine Anfrage des Lesegerätes immer in Kombination mit einer AK ausgesendet werden muss, die genau eine Anwendung spezifiziert. Eine RFID-Marke ant-

wortet nur dann auf die Anfrage des Lesegerätes, wenn dessen AK mit der eigenen Anwendungskennung übereinstimmt. Dies erfordert implizit, dass auf einer RFID-Marke gegebenenfalls Platz für mehrere Anwendungskennungen reserviert werden muss, wenn der damit verbundene Artikel in mehreren Anwendungen eingesetzt werden kann. Die Anwendungskennung sollte vom Nutzer gegen Änderungen gesperrt werden können. Ein Entsperren sollte nur mittels eines geheimen Schlüssels möglich sein.

Ein ähnliches Verfahren ist bereits in ISO/IEC 15693 spezifiziert. Dort ist jede Marke mit einer AFI (Application Family Identifier) ausgestattet. Das Lesegerät sendet eine AFI zusammen mit dem Inventory-Befehl. Dieses mit einer AFI versehene Kommando lässt nur diejenigen RFID-Marken in der Umgebung antworten, die die gleiche AFI haben. Marken mit ungleicher AFI bleiben hingegen stumm. Die ISO 15693 spezifiziert weiterhin, dass eine Anfrage des Lesegerätes ohne AFI von allen RFID-Marken beantwortet werden muss. Dies unterscheidet diesen Ansatz von unserem Gestaltungsvorschlag. Wir fordern, dass jede Anfrage eines Lesegerätes mit einer AFI versehen werden muss. Andernfalls darf keine der vorhandenen RFID-Marken antworten.

Wie kann ein Lesegerät erkennen, für welchen Zweck die Daten auf einer RFID-Marke bestimmt sind? Angenommen, die Kennung der RFID-Marke ist nur bedingt aussagekräftig und mit ihr allein ist kein Personenbezug herstellbar. Nur, wenn neben der Kennung auch der sonstige Speicher auf der RFID-Marke ausgelesen wird, kann ein Datenschutz-Problem erst entstehen. Wir schlagen für diesen Fall die Einführung einer *Verwendungskennung* (VK) vor. Wie die Anwendungskennung ist auch die VK auf der RFID-Marke gespeichert und kann gegen Veränderung gesperrt werden. Das Lesegerät fragt RFID-Marken in der gewohnten Weise ab. Die RFID-Marken antworten mit ihrer Markenkennung und der Verwendungskennung. Die Verwendungskennung spezifiziert dabei die Möglichkeit der Verwendung der Daten, womit eine Zweckbindung von RFID-Daten erreicht werden kann. So können beispielsweise gewerbliche Daten eine andere VK haben als private Daten. Ein Lesegerät erfährt dadurch zunächst nur die Markenkennung und den angedachten Verwendungszweck der auf der RFID-Marke gespeicherten sonstigen Daten. Diese sonstigen Daten sollten nur dann ausgelesen werden, wenn sie für den Zweck, den das Lesegerät vertritt, gedacht sind.

Eine ähnliche Kennung ist auch in der ISO/IEC 15693 spezifiziert. Der darin beschriebene DSFID (Data Storage Format Identifier) arbeitet ähnlich wie die Verwendungskennung, spezifiziert jedoch nicht den Verwendungszweck der Daten sondern deren Speicherformat.

9 Schlussbemerkung

Zusammenfassend lässt sich festhalten, dass RFID-Systeme per se nicht datenschutzfeindlich sind. Viele Regeln des Telekommunikations-, Multimedia- und Datenschutzrechts erfassen RFID-Anwendungen.

Zur Kompensation der aufgezeigten Defizite sollte eine Pflicht zum Deaktivieren und sollten erweiterte Transparenzregeln im Multimedia- und Datenschutzrecht normiert werden. Diese können durch Erweiterungen und Veränderungen der Spezifikationen für RFID-Systeme, wie diskutiert, technisch unterstützt werden.

Allerdings sind viele der Risiken, die mit dem Einsatz von RFID-Systemen in Verbindung gebracht werden, Kennzeichen einer Welt der allgegenwärtigen Rechnertechnik, in der viele der Alltagsgegenstände mit Rechner-, Sensor- und Kommunikationstechnik ausgestattet sowie vernetzt im Hintergrund in allen Lebensbereichen präsent sein werden.

Daher gilt es den neuen Risiken mit vorsorgender Technikgestaltung zu begegnen und das Datenschutzrecht unter dem Gedanken der Vorsorge fortzuentwickeln. Deutlich wird dies bei der RFID-Technik, bei der mit zunehmender Verwendung einer RFID-Marke die Gefahr der Personenbeziehbarkeit größer wird und auf einen Schlag alle bisherigen Profildaten zu einem feingranularen Muster zusammengeführt werden könnten.

Nur in einer Kombination von Recht und Technik lassen sich die Herausforderungen für Werte und Prinzipien durch technische Entwicklungen der Informationsgesellschaft meistern, die als zivilisatorische Errungenschaft in unserer Verfassungs- und Rechtsordnung niedergelegt sind.

Literatur

[Bgeh30] Entscheidungen des Bundesgerichtshof in Strafsachen, Band 30, S. 19 f.

[Btds13] Bundestagsdrucksache, Legislaturperiode 13, Nr. 7385, S. 16.

[Btds14] Bundestagsdrucksache, Legislaturperiode 14, Nr. 1191, S. 9.

[Bveg65] Entscheidungen des Bundesverfassungsgerichts, Band 65, Seite 1 ff.

[Damm03] Dammann, U. in: Simitis, S., Kommentar zum Bundesdatenschutzgesetz, 5. Auflage 2003, § 3 Rn. 22.

[Enge01] Engel-Flechsig, S. in: Engel-Flechsig, S.; Maennel, F.A.; Tettenborn, A., Beck'scher IuKDG-Kommentar, 1. Auflage 2001, § 2 Rn. 41.

[Enge97] Engel-Flechsig, S.; Maennel, F.A.; Tettenborn, A., Das neue Informations- und Kommunikationsdienstegesetz, Neue Juristische Wochenschrift 1997, 2981 ff.

[Epcs04] EPC Specification 1.0, http://www.epcglobalinc.org/standards_technology/specifications.html, 2004, Abruf am 2004-10-05.

[Fria99] Friauf, K.H. in Schmidt-Aßmann, E., Besonderes Verwaltungsrecht, 11. Auflage 1999, Abschnitt 2, Rn. 86 ff.

[Horn04] Hornung, G., Datenschutz für Chipkarten. Die Anwendung des § 6c BDSG auf Signatur- und Biometriekarten. Datenschutz und Datensicherheit 2004, S. 16.

[Jue+03] Juels, A.; Rivest, R.L.; Szydlo, M.: The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In: V. Atluri (Hrsg.), 8th ACM Conference on Computer and Communications Security, ACM Press, 2003, S. 103-111.

[LaMa03] Langheinrich, M.; Mattern, F., Digitalisierung des Alltags. Was ist Pervasive Computing, in: Aus Politik und Zeitgeschichte (B42/2003), Oktober 2003.

[Müll04] Müller, J., Ist das Auslesen von RFID-Tags zulässig?, Datenschutz und Datensicherheit 2004, S. 215.

[Phil03] Philips Icode SLI Product Specification, http://www.semiconductors.philips.com/acrobat/other/identification/SL058030.pdf, 2003, Abruf am 2004-10-05.

[Podl04] Podlech, A. in: Denninger, E., u.a., Kommentar zum Grundgesetz für die Bundesrepublik Deutschland, 2004, Art. 2 Abs. 1 GG, Rn. 78 ff.

[Roßn93] Roßnagel, A., KORA - Eine Methode zur Konkretisierung rechtlicher Anforderungen zu technischen Gestaltungsvorschlägen für Informations- und Kommunikationssysteme (zus. m. Hammer, V. und Pordesch, U.), InfoTech, 5. Jg. (1993), Heft 1, S. 21 - 24.

[Sar+02] Sarma, S.; Weis, S.; Engels, D.: RFID systems and security and privacy implications. In: Burton Kaliski, Cetin Kaya Co, and Christof Paar (Hrsg.), Cryptographic Hardware and Embedded Systems - CHES 2002, LNCS Band 2523, Springer: Berlin et al., 2002, S. 454-469.

[Schn96] Schneier, B.: Angewandte Kryptographie. Addison-Wesley. Bonn et al., 1996.

[Spin01] Spindler, G. in: Roßnagel, A., Recht der Multimediadienste, 2001, § 2 TDG Rn. 17, 19.

[Texa02] Texas Instruments Tag-it HF-I Transponder Inlays Reference Guide, Texas Instruments, Mai 2002.

[Wald00.1] Waldenberg, A. in: Roßnagel, A., Recht der Multimediadienste, 2000, §3 TDG Rn. 14.

[Wald00.2] Waldenberg, A. in: Roßnagel, A., Recht der Multimediadienste, 2000, §3 TDG Rn. 22.

[Weis91] Weiser, M.: The Computer for the 21st Century. Scientific American 265, 1991: S. 94 ff.