INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG

ITA manu:script

# Die Veröffentlichung des Privaten

## Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip

Andreas Krisch



ÖSTERREICHISCHE AKADEMIE DER WISSENSCHAFTEN

Wien, Jänner/2005
ITA-05-01
ISSN 1681-9187

http://www.oeaw.ac.at/ita/pdf/ita_05_01.pdf

**Jänner/2005**
**(ITA-05-01)**

# Die Veröffentlichung des Privaten

## Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip

**Andreas Krisch**

VIBE!AT – Verein für Internet-Benutzer Österreichs

### *Keywords*

Privatsphäre, Datenschutz, Radio Frequency Identification, RFID, eindeutige Produktkennzeichnung, EPC Network

### *Zusammenfassung/Abstract*

Kleine elektronische Speichermedien, auch Intelligente Etiketten oder RFID-Tags genannt, deren Daten per Funkübertragung abgerufen werden können, sollen, an Produkten angebracht oder in diese integriert, zur Produktkennzeichnung verwendet werden. Auf diesen RFID-Tags soll der Electronic Product Code eines Produktes, eine weltweit eindeutige Identifikationsnummer für dieses Produkt, gespeichert werden. Mittels dieser eindeutigen Kennzeichnung sollen Informationen zu dem betreffenden Produkt in einem global verfügbaren, Internet-basierten Informationssystem gespeichert und zum Abruf bereit gehalten werden. Auf diese Art soll es möglich werden, den Lebenszyklus eines Produktes von der Produktion bis zur Entsorgung zu überwachen. Besondere Vorteile werden von dieser Art der Produktüberwachung im Bereich des Handels und des Supply Chain Managements erwartet. Diese Arbeit beschäftigt sich mit den möglichen Auswirkungen der Produktüberwachung mittels RFID-Systemen auf die Privatsphäre der betroffenen Konsumenten.

Small electronic storage-devices, also known as Smart Labels or RFID-Tags, that emit the information they hold via radio signals, are intended to be mounted on or integrated in products to serve as means of product identification. These RFID-Tags shall store a product's Electronic Product Code, a worldwide unique identifier of a single product. Based on this identifier information on the product is to be stored and kept available in an Internet-based, globally available information system. This information system shall provide the possibility to monitor the whole life-cycle of any product from production to disposal. Special benefits of this product surveillance system are expected in wholesale and retail businesses and supply chain management. This paper discusses the potential effects of product surveillance via RFID systems on consumers' privacy.



ISSN 1681-9187

## Inhalt



*Dieses ITA manu:script ist die ausgearbeitete Fassung eines Vortrags, der auf der Tagung "TA'04: Exklusive Technik? Neue Technologien zwischen erweiterten Handlungsspielräumen und eingeschränktem Zugang", veranstaltet vom ITA, am 7. Juni 2004 in Wien gehalten wurde.*

# 1 Einleitung

Intelligente Etiketten, auch Smart Tags, Smart Labels oder RFID-Tags (Radio Frequency Identification) genannt, sollen künftig die allgegenwärtigen Strichcodes als Mittel zur Kennzeichnung von Produkten ersetzen und mittels der Zuordnung weltweit eindeutiger Seriennummern die Verarbeitung und Bereitstellung von umfangreichen Informationen zu jedem Produkt ermöglichen.

Diese Arbeit erläutert den Aufbau eines zum Teil bereits realisierten globalen Produktinformationssystems und beschäftigt sich darauf aufbauend mit den Auswirkungen einer solchen umfangreichen Datenverarbeitung in Verbindung mit der eindeutigen Kennzeichnung von Produkten mittels RFID-Tags auf die Privatsphäre der betroffenen Konsumenten.

Ein einfaches RFID-System besteht aus drei Komponenten: einer Antenne, einem Empfänger und einem Transponder oder RFID-Etikett als Informationsträger.

Die Antenne strahlt elektromagnetische Funksignale aus, um das Etikett zu aktivieren und anschließend Daten vom Tag zu lesen oder auf diesen zu schreiben. Sie stellt die Verbindung zwischen den Tags und dem Empfänger her, der die Datenerfassung und die Kommunikationsabläufe des Systems kontrolliert. Antennen sind in unterschiedlichsten Größen und Formen erhältlich; sie können in Türrahmen eingebaut werden, um Daten von passierenden Personen oder Gegenständen zu empfangen, oder auf Gerüsten über Autobahnen montiert werden, um den Verkehr zu überwachen. Das elektromagnetische Feld einer Antenne kann permanent aktiv sein oder über einen Sensor bei Bedarf aufgebaut werden (dazu und im Folgenden: AIM, 2004).

Oft wird die Antenne mit dem Empfänger zu einem tragbaren oder stationären Lesegerät verbunden. Wenn ein RFID-Tag vom elektromagnetischen Feld erfasst wird, erkennt er das Aktivierungssignal der Antenne und das Lesegerät dekodiert die am Etikett gespeicherten Daten und gibt sie an einen Computer zur weiteren Verarbeitung weiter.

Es werden aktive und passive RFID-Tags unterschieden. Aktive Tags werden durch eine interne Batterie mit Strom versorgt und unterstützen üblicherweise sowohl Lese- als auch Schreibzugriffe. Ihre Speicherkapazität kann je nach Anwendungsgebiet bis zu 1 MB betragen. Durch die eigenständige Stromversorgung verfügen aktive Tags über eine größere Kommunikationsreichweite als passive Tags. Demgegenüber wirkt sich die Batterie negativ auf die Größe, die Produktionskosten und die Lebensdauer des Tags aus. Die Lebensdauer eines aktiven Tags beträgt in Abhängigkeit von Betriebstemperatur und Batterietyp bis zu 10 Jahre.

Passive Tags kommen ohne interne Stromversorgung aus und beziehen ihre Energie aus dem elektromagnetischen Feld des Lesegeräts. Sie sind daher um einiges leichter als aktive Tags, deutlich billiger als diese und verfügen über eine nahezu unlimitierte Lebensdauer. Im Gegenzug verfügen sie über eine geringere Kommunikationsreichweite und benötigen ein leistungsfähigeres Lesegerät. Üblicherweise können passive Tags nur ein einziges Mal beschrieben werden und unterstützen im laufenden Betrieb nur Lesezugriffe auf die gespeicherten Daten. Passive Tags dienen oft zur Speicherung eindeutiger Schlüssel (z. B. einer Produktnummer) für Datenbankeinträge.

RFID-Systeme werden auch nach den verwendeten Frequenzbereichen unterschieden. Niedrigfrequente Systeme (30–500 kHz) verfügen über kürzere Kommunikationsreichweiten und verursachen dafür geringere Kosten. Sie werden hauptsächlich für Zutrittskontroll-, Produktverfolgungs- und Tieridentifikationssysteme verwendet. Hochfrequente Systeme (850–950 MHz und 2,4–2,5 GHz) verfügen über hohe Reichweiten (über 25 Meter) und Zugriffsgeschwindigkeiten, verursachen jedoch auch höhere Systemkosten. Sie werden vor allem zur Verfolgung von Eisenbahnwaggons und in automatischen Mautsystemen verwendet.

Der bedeutendste Vorteil aller Typen von RFID-Systemen ist, dass ohne direkten Kontakt und ohne direkte Sichtverbindung zum RFID-Tag auf die darauf gespeicherten Informationen zugegriffen werden kann. Auf RFID-Tags kann durch Schnee, Nebel, Eis, Lacke und andere Materialien hindurch zugegriffen werden, bei denen Strichcode- und andere optische Systeme versagen. In den meisten Anwendungsfällen können selbst unter widrigen Umständen Zugriffszeiten von unter 100 Millisekunden erreicht werden (AIM, 2004).

Die möglichen Anwendungsgebiete von RFID-Systemen sind mannigfach. Mattern beschreibt deren Potential folgendermaßen: „Interessant an solchen fernabfragbaren elektronischen Markern ist, dass sich dadurch Objekte der realen Welt eindeutig erkennen lassen und so in Echtzeit mit einem im Internet oder einer entfernten Datenbank residierenden zugehörigen Datensatz verknüpft werden können, wodurch letztendlich beliebigen Dingen spezifische Informationen und Methoden zur Informationsverarbeitung zugeordnet werden können. Lassen sich Alltagsgegenstände aus der Ferne identifizieren und mit Information behaften, eröffnet dies aber weit über den ursprünglichen Zweck der automatisierten Lagerhaltung oder des kassenlosen Supermarktes hinausgehende Anwendungsmöglichkeiten, ...“ (Mattern, 2002, S. 2 f.).

Zu diesen weiteren Anwendungsbereichen gehört der elektronische Kleiderschrank, der seinem Benutzer Ratschläge zur optisch ansprechenden Kombination der vorhandenen Kleidungsstücke erteilt und zusätzlich als Werbeplattform für Bekleidungshändler dienen soll (Wan, 2000), ebenso wie Konzepte zur effizienteren Abfallverwertung durch detailliertere Informationen über die Zusammensetzung der zu entsorgenden Produkte, die mittels RFID-Kennzeichnung verfügbar gemacht werden sollen.

Kernelement all dieser Anwendungsvisionen ist die weltweit eindeutige Kennzeichnung von Produkten. Diese Kennzeichnung soll mittels des Electronic Product Code (EPC) erfolgen, der einen der vier wesentlichen Bestandteile des EPC Networks zur dezentralen Sammlung und Verwaltung von Produktinformationen darstellt. Im folgenden Abschnitt wird das EPC Network mit seinen Komponenten vorgestellt.

# 2 Das EPC Network zur Produktüberwachung

Das EPC Network, ein System zur weltweit eindeutigen Produktkennzeichnung und dezentralen Speicherung und Verfügbarmachung von produktbezogenen Informationen im Internet, wurde vom Auto-ID Center des Massachusetts Institute of Technology (MIT Auto-ID Center) unter Mitwirkung eines Konsortiums namhafter Unternehmen und Forschungseinrichtungen entwickelt. Es setzt sich aus folgenden Komponenten zusammen:

## *2.1 Der Electronic Product Code*

Der Electronic Product Code (EPC) soll als weltweit eindeutige Identifikationsnummer die bisher als Strichcodes gebräuchlichen EAN.UCC Identifikationsnummern ersetzen. Die in bisherigen Codes enthaltene Herkunftsland-Nummer, Teilnehmernummer und Artikelnummer werden im EPC um

eine Seriennummer ergänzt. Dadurch wird über die bisherige Kennzeichnung von Artikelgruppen eine eindeutige Kennzeichnung von einzelnen Produkten möglich (EAN Austria, 2004).

Der vom MIT Auto-ID Center dafür vorgeschlagene 96-Bit-Code setzt sich aus einem 8 Bit großen Header zur Kennzeichnung des Nummerierungsschemas, 28 Bit zur Kennzeichnung des Herstellers, 24 Bit zur Angabe der Objektklasse und 36 Bit für die Nutzung als Seriennummer zusammen.

Bei dieser Aufteilung der verfügbaren Stellen können rund 238 Millionen Hersteller mit jeweils ungefähr 16 Millionen Objektklassen zu je ca. 68 Milliarden Objekten ausgestattet werden. Daraus ergeben sich für jeden Hersteller rund 1.152 Billiarden eindeutige Produktkennzeichen (Brock, 2001, S. 19 f.).

Zum Vergleich: Bei jährlich rund 13 Billiarden produzierten Reiskörnern weltweit (Brock, 2001, S. 12) würden die Seriennummern eines einzigen Herstellers ungefähr 88 Jahre ausreichen, um jedes einzelne Reiskorn mit einer eindeutigen Nummer zu versehen.

## 2.2 Die Physical Markup Language

Die Bereitstellung der Produktinformationen zu den mittels EPC gekennzeichneten Objekten soll mittels der Physical Markup Language (PML) erfolgen. Dabei handelt es sich im wesentlichen um ein XML-Schema zur Beschreibung von physischen Objekten.

Die vom MIT Auto-ID Center vorgelegte PML-Spezifikation sieht neben der Beschreibung von Produkt- und Umwelteigenschaften (beispielsweise Inhaltsstoffen, Haltbarkeit, Gewicht, Temperatur) vor, Objekte anderen Objekten hierarchisch zuzuordnen (beispielsweise können einzelne Produkte einer Palette zugeordnet werden, diese könnte wiederum einem LKW zugeordnet werden usw.) und Verbindungen zu anderen PML-Dateien anzugeben. Der derzeitige und frühere Aufenthaltsorte (entweder relativ zu einem anderen Objekt oder absolut mittels GPS-Koordinaten) können ebenso angegeben werden wie Informationen über Personen und Organisationen, die im Zeitablauf in einer Verbindung zu dem Objekt standen (z. B. Eigentümer oder Lieferanten). Verbindungen zwischen Personen bzw. Organisationen und Orten (z. B. „Herr W arbeitet im Lager X der Firma Y, das sich in der Straße Z befindet“) können ebenso festgehalten werden, wie genaue Zeitpunkte zu denen gewisse Ereignisse eingetreten sind (z. B. Lieferdatum und -uhrzeit) (Brock et al., 2001, S. 7 ff.).

Derart formatierte Informationen können von jedem Teilnehmer am EPC Network auf seinen eigenen Servern (dem so genannten EPC Information Service (EPC IS)) zum Abruf bereitgestellt werden. Die Auffindbarkeit der zahlreichen dezentral angebotenen Informationen zu einem Produkt wird dabei durch das Object Naming Service und das EPC Discovery Service gewährleistet.

## 2.3 Das Object Naming Service und EPC Discovery Service

Das Object Naming Service (ONS) baut sowohl technisch als auch funktional auf den Konzepten des für die Zuordnung von Domainnamen zu IP-Adressen im Internet gebräuchlichen Domain Name System (DNS) auf. Das ONS dient als Verzeichnis aller EPC Informationssysteme. Nach Übermittlung eines Produktcodes liefert das ONS eine oder mehrere Internetadressen zurück, an denen der Hersteller Informationen zu diesem Produkt bereit hält.

Das EPC Discovery Service liefert ein Verzeichnis aller EPC Informationssysteme, die Daten über ein bestimmtes Produkt enthalten. Es ermöglicht allen Teilnehmern der Logistikkette, die auf ihren

EPC-Informationssystemen abgelegten Informationen zu einem Produkt im Netzwerk zur Verfügung zu stellen. Ist ein Netzwerkteilnehmer an den bisher gesammelten Informationen zu einem Produkt interessiert, kann er vom EPC Discovery Service eine Liste aller EPC-Informationssysteme abrufen, die entsprechende Informationen anbieten und diese Daten in weiterer Folge zu einem umfassenden Gesamtbild des Produktlebenszyklusses zusammenführen (VeriSign, 2004).

## 2.4 Funktionsweise und Verfügbarkeit

Anhand der schematischen Darstellung des EPC Network in Abbildung 1 lassen sich die Informationsflüsse im System wie folgt zusammenfassen:

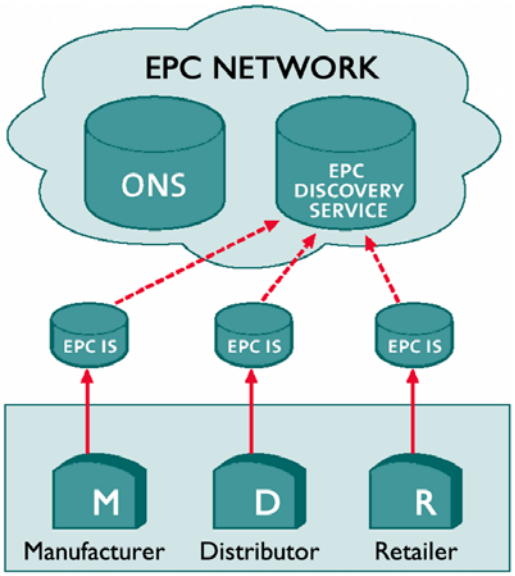


*Abbildung 1: Das EPC Network (VeriSign, 2004)*

*Bereitstellen von Informationen:* Der Hersteller eines Produktes kennzeichnet dieses mit einem auf einem RFID-Tag gespeicherten Electronic Product Code und speichert produktbezogene Daten zu diesem EPC in seinem EPC IS. Die Verfügbarkeit dieser Informationen teilt er dem EPC Discovery Service mit. Jeder weitere Teilnehmer an der Lieferkette kann weitere Informationen zu demselben Produkt in seinem EPC IS speichern und dies ebenfalls dem EPC Discovery Service melden.

*Abrufen von Informationen:* Für den Abruf von Informationen sind im System zwei Möglichkeiten vorgesehen. Werden lediglich Herstellerinformationen benötigt, kann der abfragende Teilnehmer den EPC an das ONS übermitteln und erhält daraufhin die Adresse des EPC IS des Herstellers, von wo er die gewünschten Informationen beziehen kann. Werden über die Herstellerinformationen hinaus Daten benötigt, die im Laufe des Produktlebenszyklus an verschiedenen Stellen gespeichert wurden, übermittelt der Anfrager den EPC an das EPC Discovery Service, woraufhin er eine Liste aller EPC IS erhält, die Daten zu diesem Produkt bereithalten. Aus diesen im Netzwerk verteilten Datenquellen kann in weiterer Folge eine Gesamtbeschreibung des bisherigen Produktlebenszyklusses erstellt werden.

## 2.5 Erhoffte Vorteile des Technikeinsatzes

Die größten wirtschaftlichen Vorteile des Einsatzes von RFID-Kennzeichnungen in der Konsumgüterindustrie werden gemäß einer Studie des MIT Auto-ID Centers (Agarval, 2001) in der Optimierung der Produktverfügbarkeit in den Regalen der Einzelhändler vermutet. Die Studie zitiert, allerdings ohne genauere Quellenangaben, Analysen von Anderson Consulting, Roland Berger und ECR France aus den Jahren 1996, 1999 bzw. 2000 laut derer der durchschnittliche Anteil von nicht verfügbaren Produkten zwischen 8,2 % und 10,9 % mit Spitzenwerten bis zu 17,5 % liegen soll. Die Ursachen dafür werden in inadäquaten Bestellabläufen und verspäteter Regal-Nachbestückung aus den vorhandenen Lagerbeständen gesehen.

Durch den Einsatz von RFID-Systemen könnte der jeweilige Warenbestand in den Regalen und Lagern permanent überwacht und auf bevorstehende Engpässe automatisch hingewiesen werden. Die dadurch erreichte rechtzeitige Nachbestellung und Nachbestückung der Regale würde – so die Studie – die Nichtverfügbarkeit von Produkten um ungefähr 80 % reduzieren, woraus Verkaufssteigerungen von durchschnittlich 2 – 3 % resultieren sollen.

Weitere Vorteile im Supply Chain Management und der Lagerverwaltung sollen in der automatischen Erstellung von Liefernachweisen auf Basis der bei der Warenübernahme erkannten EPC-Kennungen liegen. Dadurch sollen Verluste durch fehlerhafte Erfassungen minimiert und der Arbeitsaufwand für Warenübernahme und Reklamation reduziert werden.

Darüber hinaus sollen dank des RFID-Einsatzes in der Lagerverwaltung Inventurarbeiten auf ein Minimum reduziert werden können, da der aktuelle Lagerbestand jederzeit automationsunterstützt festgestellt werden könne. Ebenso wäre es möglich, verderbliche Güter stets so in den Verkaufsregalen anzuordnen, dass jeweils die ältesten Produkte zuerst entnommen werden und somit Verluste aufgrund der Überschreitung des Mindesthaltbarkeitsdatums reduziert werden könnten.

Durch die verbesserte Überwachung der Lagerbestände wären darüber hinaus Einsparungen durch kürzere Bestellzyklen und einer damit verbundenen Verringerung der Lagerbestände erzielbar.

Zusätzliche Vorteile würde der Einsatz von RFID-Tags zur Produktkennzeichnung in den Bereichen der Diebstahlsbekämpfung, dem „Rückgabe-Betrug“ und der Produktfälschung bieten. Die Diebstahlsbekämpfung wäre durch den Technikeinsatz nicht nur auf den Verkaufsbereich beschränkt sondern es wäre darüber hinaus ebenfalls möglich gestohlene Produkte am Schwarzmarkt zu identifizieren und dem legitimen Eigentümer zurückzuerstatten. Darüber hinaus könnten RFID-Systeme auch verwendet werden, um Produktfälschungen anhand fehlender RFID-Etiketten oder gefälschter bzw. duplizierter Seriennummern zu erkennen und aus dem Verkehr zu ziehen, was in weiterer Folge eine Steigerung der Verkaufserlöse nach sich ziehen soll.

## 2.6 Erwartete Kosten des Technikeinsatzes

Bezüglich der zu erwartenden Kosten des Einsatzes von RFID Systemen sind bisher nur wenig konkrete Zahlen veröffentlicht worden. Während Agarval (2001) lediglich einige Kostenbereiche aufzählt und sich einer weiteren Behandlung dieses Bereichs mit einem Hinweis auf ständig sinkende Kosten enthält, veröffentlichte A. T. Kearney (2003) eine Analyse der Kosten und Vorteile aus dem Einsatz in der Konsumgüterindustrie.

Diese Analyse ortet die Vorteile aus dem RFID-Einsatz vor allem bei den Handelsunternehmen und nur zu einem geringeren Teil bei den Produzenten. Während im Handel vorwiegend einmalige Kosten für Hardware- und Softwareanschaffungen sowie Integration der Systeme in die bestehenden

Strukturen anfallen, hätten die Hersteller über diese einmaligen Anschaffungskosten mit den hohen laufenden Kosten der Produktkennzeichnung zu kämpfen. Hersteller, die geringere Stückzahlen hochpreisiger Produkte verkaufen, würden aufgrund der Reduktion von Schwund und Nichtverfügbarkeit ihrer Produkte stärker profitieren und hätten aufgrund der geringeren Anzahl der hergestellten Produkte auch geringere Kosten für die Produktkennzeichnung mittels RFID-Etiketten zu tragen. Im Gegensatz dazu wären Hersteller niedrigpreisiger Produkte aufgrund der höheren Stückzahlen verkaufter Produkte auch mit deutlich höheren Kosten für die Produktkennzeichnung konfrontiert. Vor allem für die zweite Gruppe von Produzenten würde sich ein Einsatz von RFID-Etiketten zur Produktkennzeichnung am ehesten dann rechnen, wenn sie von den Handelsunternehmen Zugriff auf die jeweils aktuellen Verkaufs- und Lagerstandszahlen erhalten und sie dadurch die Möglichkeit bekommen, ihre Produktionsprozesse besser an die Marktlage anzupassen.

## 2.7 Realisierungsgrad

Während die Konzeption des EPC Networks unter der Leitung des MIT Auto-ID Centers erfolgte, wurde die praxisgerechte Umsetzung bereits an kommerziell orientierte Betriebe übertragen. Die Administration des Electronic Product Code wurde an die EPCglobal, Inc., ein eigens dafür ins Leben gerufenes Joint Venture von EAN International und dem Uniform Code Council (UCC), vergeben. Dieses hat die Spezifikation des Electronic Product Code in der Version 1.0 verabschiedet. Der Electronic Product Code ist in Europa über die Mitgliedsbetriebe von EAN International bereits weitestgehend verfügbar. Der Betrieb des EPC Networks wurde von VeriSign, einem Unternehmen mit umfangreichen Erfahrungen im Bereich der Domainnamen-Verwaltung, übernommen.

In den USA haben die Handelskette WalMart und das Verteidigungsministerium ihre größten 100 Zulieferbetriebe verpflichtet, ab 2005, vorerst auf Verpackungsebene, mit dem Einsatz der RFID-Etikettierung zu beginnen.

In Deutschland betreibt die Metro Group mit dem Future Store in der Stadt Rheinberg einen Supermarkt, in dem Produkte mit RFID-Kennzeichnungen zum Verkauf angeboten werden. Die mit RFID-Tags bestückten Kundenkarten des Future Store wurde nach zahlreichen kritischen Medienberichten wieder eingezogen.

In Österreich werden bereits vereinzelt Produkte mit RFID-Kennzeichnungen im Einzelhandel vertrieben.

Neben Pilotprojekten in weiteren Einzelhandelsketten (z. B. Rewe) sind Anwendungen in zahlreichen anderen Bereichen bekannt. In Wien sind beispielsweise alle Medien der Hauptbibliothek mit RFID-Tags gekennzeichnet. Ebenso kommen in Wien RFID-Tags zur Kennzeichnung von Haustieren zum Einsatz.

Reisepässe von EU-Bürgern werden in Zukunft biometrische Daten ihrer Inhaber auf RFID-Tags zum Abruf bereithalten. Derzeit ist die Speicherung von Fingerabdrücken und eines Bildes auf diesen Tags geplant.

# 3 Grundsätze im Schutz der Privatsphäre

Beschäftigt man sich mit den Auswirkungen von RFID-Systemen auf die Privatsphäre und somit mit den Grundsätzen im Schutz der Privatsphäre, so ist vorerst die Frage zu beantworten, was unter Privatsphäre verstanden werden soll und weshalb der Schutz derselben von Bedeutung ist.

Bei der Beantwortung dieser Frage soll vorrangig den Ausführungen von Beate Rössler (2001) gefolgt werden, die in ihrem Buch „Der Wert des Privaten" nicht nur eine zusätzliche Definition des Begriffs der Privatsphäre anbietet, sondern darüber hinaus auf eine Definition abzielt, die möglichst viele der in den diversen Diskursen zur Privatsphäre bisher behandelten Teilaspekte des Privaten zu integrieren sucht.

Rössler unterscheidet dabei drei Arten von Privatheit: Von *dezisionaler Privatheit* spricht sie, wenn wir den Anspruch haben, vor unerwünschtem Zutritt im Sinne von Hineinreden, Fremdbestimmen bei Entscheidungen und Handlungen geschützt zu sein. *Informationelle Privatheit* meint den Anspruch, vor unerwünschtem Zugang im Sinne eines Eingriffs in die persönlichen Daten über sich geschützt zu werden, also vor dem Zugang zu Informationen über sich. Unter *lokaler Privatheit* schließlich versteht sie den Anspruch, vor dem Zutritt anderer in Räume oder Bereiche geschützt zu werden.

Rössler argumentiert weiters, dass wir Privatheit deshalb für wertvoll halten, weil wir Freiheit und damit Autonomie für wertvoll halten und weil nur aufgrund der Rahmenbedingungen von Privatheit und der Rechte und Ansprüche auf Privatheit Autonomie in all ihren Aspekten lebbar und artikulierbar ist. „Begreift man als das *telos* von Freiheit, ein autonomes Leben führen zu können, dann kann man, in der Ausbuchstabierung der Bedingungen eines solchen autonomen Lebens, sehen, dass für den Schutz von Autonomie Freiheitsrechte selbst nicht ausreichend sind, sondern dass Autonomie angewiesen ist auf die Substantialisierung dieser Freiheitsrechte in Rechten und Ansprüchen auf den Schutz des Privaten. Denn die Autonomie einer Person kann verletzt, beschädigt werden auf Weisen, die die Freiheitsrechte selbst gar nicht unmittelbar berühren: und um ebendieser Möglichkeiten willen sind Personen, in ihrer Autonomie, angewiesen auf den Schutz des Privaten" (Rössler, 2001, S. 26).

Dementsprechend dienen die drei oben definierten Dimensionen des Privaten dem Schutz unterschiedlicher Aspekte: „Die Dimension der dezisionalen Privatheit dient der Sicherung von Entscheidungs- und Handlungsspielräumen eines Subjekts in all seinen sozialen Bezügen; die Dimension der informationellen Privatheit dient der Sicherung eines für seine Autonomie notwendigen gesicherten Erwartungshorizonts an das Wissen anderer über es selbst; die Dimension der lokalen Privatheit dient dem Schutz von räumlichen Rückzugsmöglichkeiten, auf die ein Subjekt um seiner Autonomie willen angewiesen ist" (Rössler, 2001, S. 40).

Ähnlich auch die Argumentation des deutschen Bundesverfassungsgerichts (1983) zum sogenannten Volkszählungsurteil, das den Begriff „informationelle Selbstbestimmung" geprägt hat. Dort heißt es:

> „Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit

über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Im Kontext der elektronischen Datenverarbeitung stehen bei der Beschäftigung mit dem Themenbereich Privatsphäre vor allem die Aspekte der informationellen Privatheit im Mittelpunkt. In diesem Zusammenhang sind auch die folgenden Ausführungen bezüglich der grundlegenden Kriterien zu verstehen, die im Bereich der Datenverarbeitung für die Aufrechterhaltung der Privatsphäre erfüllt sein müssen. Bezüglich der lokalen und dezisionalen Privatheit wären jedenfalls noch weitere Kriterien hinzuzufügen, um einen umfassenden Kriterienkatalog für die generelle Gewährleistung der Privatsphäre zu erhalten.

In der Literatur und den einschlägigen Normen finden sich unterschiedliche Definitionen der für die informationelle Privatheit relevanten Daten. Die EU-Datenschutzrichtlinie beispielsweise definiert als ihren Gegenstand „insbesondere den Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten", wobei personenbezogene Daten „alle Informationen über eine bestimmte oder bestimmbare natürliche Person ('betroffene Person')" umfassen. „[A]ls bestimmbar wird eine Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kenn-Nummer oder zu einem oder mehreren spezifischen Elementen, die Ausdruck ihrer physischen, physiologischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität sind" (Europäisches Parlament und Rat, 1995, S. 10).

Der Schutz bezieht sich also auch auf Daten, die keinen unmittelbaren Personenbezug aufweisen, sondern erst durch Verknüpfung mit anderen Daten oder in einem anderen Kontext einer konkreten Person zugeordnet werden können. Ebenso fordert Rössler, dass „[d]er Schutz der immer schon identifizierten Person wie auch der potentiell zu identifizierenden [...] gleichermaßen Thema der informationellen Privatheit sein" muss (Rössler, 2001, S. 223). Sie unterscheidet insgesamt aber vier Gruppen von Daten, die – je nach Kontext – als schützenswert, als zur informationellen Privatheit gehörend, angesehen werden müssen:

Als Erstes müsse man „die *Privatheit von Gedanken und mentalen Zuständen* nennen, von Gefühlen und Einstellungen generell, Daten, deren Wichtigkeit für die Identität, die Persönlichkeit ganz aus der Innenperspektive bestimmt werden können: was wichtig ist für eine Person, was sie als besonders intim und privat empfindet, ist auch ihre eigene Entscheidung und kann nämlich nur in Grenzen verallgemeinert und objektiviert werden" (Rössler, 2001, S. 224).

Dieser Umstand, dass nicht objektiviert werden kann, was Menschen als besonders intim oder privat empfinden, ist – nebenbei bemerkt – neben der Verknüpfbarkeit mit anderen Daten und dem Verwendungszusammenhang mit ein Grund für die oft erhobene Forderung nach Datensparsamkeit und Zweckbindung der gesammelten Daten.

Als zweite Gruppe von Daten nennt Rössler die *„personenbezogenen Daten"* – wie sie etwa in der EU-Richtlinie beschrieben werden – „die dazu dienen können, nicht nur eine Person unter allen anderen möglichen zu identifizieren, sondern auch die Vorlieben, Eigenheiten, Gewohnheiten von Personen zu bestimmen: hier geht es dann um das weite Spektrum von computergestützten Daten, zu denen dann auch etwa Daten über das *browser-behavior* einer Person gehören, aber auch um traditionelle Daten wie persönliche Aufzeichnungen (Tagebücher), Briefe, Dokumente usf." (Rössler, 2001, S. 224).

Die dritte Gruppe von Daten umfasst nach Rösslers Ausführungen alles, *„was Personen zu Hause (legitimerweise) tun"*. Verhaltensweisen, die Personen zu Hause an den Tag legen, können nach ihrer Ansicht „informationell" genannt werden, „weil Personen ein Interesse daran haben, dass unbestimmte andere hiervon nichts 'wissen'" (Rössler, 2001, S. 224 f.).

Die vierte und letzte Datengruppe beinhaltet schließlich *„außerhäusige Bewegungen und Gewohnheiten* und [Daten, die sich] auf die *raum-zeitlichen Gegebenheiten* einer Person beziehen: Videoüberwachungen auf öffentlichen Plätzen und in Geschäften wären solche Fälle der Sammlung von Daten, die eine Person prinzipiell identifizierbar machen und mit deren Hilfe Personen überwacht werden können" (Rössler, S. 225).

Wichtig für die Beurteilung der Sensibilität von Daten ist aber jedenfalls auch der Verwendungszusammenhang und die Verknüpfbarkeit mit anderen Daten. So stellte das deutsche Bundesverfassungsgericht (1983) in seinem Volkszählungsurteil fest: „Dabei kann nicht allein auf die Art der [im Rahmen der Volkszählung vom Bürger verlangten] Angaben abgestellt werden. Entscheidend sind ihre Nutzbarkeit und Verwendungsmöglichkeit. Diese hängen einerseits von dem Zweck, dem die Erhebung dient, und andererseits von den der Informationstechnologie eigenen Verarbeitungsmöglichkeiten und Verknüpfungsmöglichkeiten ab. Dadurch kann ein für sich gesehen belangloses Datum einen neuen Stellenwert bekommen; insoweit gibt es unter den Bedingungen der automatischen Datenverarbeitung kein 'belangloses' Datum mehr."

So führen auch Mattern und Langheinrich (2001, S. 7) im Bezug auf Ubiquitous Computing und die damit einhergehende Verwischung der Grenzen zwischen Offline und Online – die bei den derzeitigen Formen der Internetnutzung noch feststellbar sind – aus: „Besonders kritisch erscheint, dass die Grenze zwischen „personenbezogenen" und „anonymen" Daten bei einer derart stark zunehmenden Datenmenge verschwimmt, da immer leistungsfähigere Rechner und Verfahren die nachträgliche Korrelation solcher Informationen erleichtern. Die zunehmende Personalisierung, vor allem auch bei der Angebots- und Preisgestaltung, verstärkt diesen Effekt noch, da anonyme Spuren immer individueller werden".

Vor diesem Hintergrund ist jedenfalls die *Datensparsamkeit und Zweckbindung* der gesammelten Daten als wesentliches Kriterium für die Gewährleistung der Privatsphäre zu betrachten. Als weitere wichtige Kriterien nennen Mattern und Langheinrich, aber in ähnlicher Form auch andere Quellen (vgl. beispielsweise die OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD, 1980):

- *Anonymität und Pseudonymität*
  Wie kann man seinen Namen und andere personenbezogene Daten über sich verbergen oder nur selektiv preisgeben?
- *Vertraulichkeit*
  Wie kann sichergestellt werden, dass unbefugten Dritten sowohl während der Übertragung als auch danach kein Zugriff auf die persönlichen Daten möglich ist?
- *Transparenz*
  Wie kann man sich darüber im Klaren sein, welcher Aspekt seiner Person (Bewegungsmuster, Diskussionsbeiträge, etc.) zu irgendeinem Zeitpunkt überwacht wird, und unter welchen Umständen (Grund der Überwachung, Dauer der Datenspeicherung, Empfänger der Daten, etc.) dies geschieht?
- *Vertrauen und Absicherung*
  Wem kann man vertrauen, dass Abmachungen über Grund und Umfang der Datensammlung und deren Empfänger eingehalten werden, und wer kann einem im Konfliktfall helfen? (in enger Anlehnung an: Mattern, Langheinrich, 2001, S. 8).

# 4 Auswirkungen

Der Einsatz von RFID-Systemen bringt eine Reihe von Auswirkungen auf die betroffenen Konsumenten mit sich. Diese umfassen einerseits die Einbindung in Datenverarbeitungsprozesse ohne das Wissen und die Zustimmung der Betroffenen und andererseits den Ausschluss bzw. die Benachteiligung von unterschiedlichen Personengruppen. Gemeinsam ist diesen Auswirkungen das Potential zur Gefährdung der Privatsphäre.

## 4.1 Inklusion durch den Technikeinsatz

Das vorgestellte System zur Kennzeichnung und Überwachung von Produkten ermöglicht auch die Erfassung von umfangreichen Informationen über die Umwelt eines Produktes. Neben geographischer Position, Umwelt-Temperatur und benachbarten Produkten oder der Zuordnung zu einer Verpackungseinheit können ebenso Daten über handelnde Personen und Eigentumsverhältnisse verarbeitet werden.

Der Detaillierungsgrad der erfassten Informationen hängt dabei vor allem von der Anzahl und Position der eingesetzten Lesegeräte ab und kann entsprechend den Wünschen der Betreiber angepasst werden. Im Folgenden einige wenige Beispiele möglicher Szenarien im Einzelhandel:

Durch die Kennzeichnung von Produkten mit RFID-Tags und darauf gespeichertem Electronic Product Code kann durch in den Regalen montierte Lesegeräte das Verhalten der Konsumenten innerhalb des Geschäftslokales detailliert erfasst werden. Auf diese Art könnte festgestellt werden, welchem Weg Konsumenten durch das Geschäft folgen, vor welchen Regalen sie länger verweilen und an welchen sie zügig vorbeigehen. Daraus wäre leicht ein Interesse oder Desinteresse für bestimmte Produktgruppen ableitbar. Darüber hinaus wären auch detailliertere Auswertungen möglich. Beispielsweise könnte analysiert werden, welche Produkte Konsumenten aus dem Regal nehmen und anschließend wieder zurücklegen. Aus diesen Informationen kann man im Anschluss ableiten, dass ein Konsument an einer bestimmten Produktgruppe interessiert ist und dieses Interesse in weiterer Folge mit gezielter Werbung ansprechen.

Diese Informationen können beispielsweise durch die Zuordnung zu einer personalisierten Rabattkarte dauerhaft mit den Daten des Kunden verknüpft werden. Der Einsatz von RFID-Systemen eröffnet aber darüber hinausgehend noch weitere Zuordnungsmöglichkeiten:

Werden Produkte mit RFID-Tags und EPC eindeutig gekennzeichnet und bleiben die RFID-Tags auch nach dem Verkauf am Produkt befestigt und nicht deaktiviert, so kann der darauf gespeicherte Produktcode jederzeit von jedem beliebigen Lesegerät empfangen und verarbeitet werden. Jede Person würde auf diese Art ständig eine Reihe von eindeutigen Kennungen aussenden, anhand derer sie ohne ihr Wissen und Zutun eindeutig wiedererkannt werden könnte.

Bleiben RFID-Tags auch nach dem Verkauf eines Produktes aktiv, so wäre eine Erfassung der darauf gespeicherten Produktcodes und der Abruf von Informationen zu diesem Produktcode bei einem neuerlichen Besuch dieses oder eines anderen Geschäftslokales nicht nur möglich sondern sogar technisch notwendig. Da passive RFID-Tags in der Regel nur Lesezugriffe erlauben, können sie nicht als „verkauft“ markiert werden wie dies bei herkömmlichen Warensicherungssystemen geschieht. Informationen über die Eigentumsverhältnisse müssten daher in den Datenbanken des EPC Networks abgelegt und bei jeder Erfassung des entsprechenden Produktcodes dort abgerufen werden. Bereits aus diesen Abfragen beim EPC Network ließe sich anhand der bekannten Positionen der Lesegeräte eine umfangreiche Analyse über die geographischen Bewegungen von Konsumenten erstellen.

Neben diesen Bewegungsprofilen könnten aber durch die gegenseitige Zuordnung der Produktcodes eines Konsumenten auch Analysen über dessen Konsumgewohnheiten erstellt werden. Aufgrund der im EPC Network abrufbaren Produktdaten wären weiters Rückschlüsse auf die Kaufkraft der Konsumenten möglich.

Da es den Konsumenten nicht möglich ist festzustellen, wann und von wem die von ihnen in diversen Produkten mitgeführten RFID-Tags abgerufen werden, würden derartige Datenverarbeitungen in der Regel ohne Wissen und ohne Zustimmung der Betroffenen stattfinden.

Handelsbetriebe, die RFID-Systeme einsetzen, hätten den Vorteil, dass sie mittelfristig auf die Ausgabe von Kundenkarten als Maßnahme zur Datensammlung verzichten und somit zusätzliche Einsparungen erzielen könnten.

Aus Sicht der Datenschutzinteressen der Konsumenten wäre ein zusätzlicher Nachteil dadurch gegeben, dass die gesammelten und verknüpften Daten dem einzelnen Konsumenten aufgrund der Produktcodes, die er mit sich führt, leicht zugeordnet werden können, auch ohne dass dem Datenverarbeiter sein Name bekannt ist. Dies ist deshalb als Nachteil zu bewerten, da der Konsument die auf seinen Produkten gespeicherten Codes kennen und bekannt geben müsste, um von den Datenverarbeitern Auskunft zu den über ihn gespeicherten Daten erhalten zu können.

Die Konsumenten finden sich beim Einsatz von RFID-Systemen also in einer Situation wieder, in der sie über keine Möglichkeit verfügen festzustellen, wer wann welche Daten über sie verarbeitet. Selbst wenn das EPC Network in der derzeit geplanten Form nicht realisiert werden sollte, steht dennoch jedem Betreiber von RFID-Lesegeräten die Möglichkeit offen, RFID-Tags, die in den Aktionsbereich seiner Lesegeräte geraten, abzufragen, die empfangenen Daten auf beliebige Art zu speichern und mit beliebigen anderen Informationen zu verknüpfen.

## 4.2 Exklusion durch den Technikeinsatz

Neben dieser unkontrollierbaren Einbindung in Datenverarbeitungsprozesse eröffnen RFID-Systeme auch Ausschließungsmöglichkeiten.

Ein Beispiel für derartige Exklusions-Szenarien ist die weitere Verfeinerung einer Preisdiskriminierungsstrategie. Darunter wird die Verwendung unterschiedlicher Preise für gleiche Produkte in unterschiedlichen Märkten verstanden, sofern diese Preisunterschiede nicht durch unterschiedlich hohe Selbstkosten begründet sind.

In der „virtuellen Tour“ des Metro Future Store (Metro Group, 2004) wird der Einsatz von RFID-Systemen für diese Zwecke anschaulich präsentiert: Eine Konsumentin nähert sich mit ihrem intelligenten Einkaufswagen einem Regal, daraufhin verändert das elektronische Preisschild automatisch seine Anzeige und zeigt einen offenbar nur für diese Konsumentin gültigen „Special Price“ an. Diese Konsumentin kommt also offenbar in den Genuss von Rabatten, von denen andere Konsumenten ausgeschlossen werden.

Ein weiteres Beispiel für den Ausschluss von Leistungen kann in den Plänen gesehen werden, sogenannten „Service-Betrug“ zu verhindern. Darunter wird die unrechtmäßige Geltendmachung von Service- oder Gewährleistungsansprüchen verstanden. Auf Basis der eindeutigen Produktkennzeichnung mit RFID-Systemen soll sichergestellt werden, dass derartige Leistungen nur dann erbracht werden, wenn ein Produkt auch tatsächlich bei dem Einzelhändler erworben wurde, bei dem die Ansprüche geltend gemacht werden. Entfernen Konsumenten RFID-Tags von den von ihnen erworbenen Produkten, schließen sie sich in diesem Szenario selbst von der Inanspruchnahme jeglicher weiterer Leistungen aus.

Auch Überlegungen, die Echtheit von Produkten anhand der daran befestigten RFID-Tags nachzuweisen und Produktfälschungen somit zu erschweren, weisen in die Richtung, dass ein eigenmächtiges Entfernen von RFID-Tags künftig dazu führen könnte, des Erwerbs von Produktfälschungen verdächtigt zu werden.

In Bezug auf die mittels RFID-Systemen gesammelten Daten und die umfangreichen Möglichkeiten für Unternehmen, wertvolle Informationen daraus abzuleiten, sind ausschließende Wirkungen aber auch im Hinblick auf den Zugriff auf die gespeicherten Daten und die Verwertung derselben zu erwarten. Die Zugriffsrechte zu den jeweiligen EPC-Informationssystemen werden für große Handelskonzerne voraussichtlich einen lukrativen Geschäftszweig eröffnen.

Werden RFID-Etiketten für derartige Zwecke verwendet könnten sich die betroffenen Konsumenten alsbald vor die Wahl gestellt sehen, entweder durch Entfernung der Etiketten ihre Privatsphäre zu schützen und dafür im Gegenzug konkrete Nachteile bis hin zum Verdacht der Produktfälschung zu erleiden, oder aber sich den Sicherheitsvorstellungen der involvierten Unternehmen zu unterwerfen und einer strafbaren Handlung unverdächtigt bei jedem RFID-Lesegerät in dessen Nähe sie geraten wertvolle Informationen über ihre Privatsphäre zu hinterlassen.

## 4.3 Privatsphäre

Hinsichtlich der Gewährleistung der Privatsphäre ergeben sich vor dem Hintergrund der im Abschnitt 3 vorgestellten Grundsätze aus der eindeutigen Produktkennzeichnung mittels RFID und der Nutzung des EPC Network eine Reihe von Problemfeldern, auf die im Folgenden näher eingegangen wird.

### 4.3.1 Datensammlung

Als Zielsetzung der eindeutigen Produktkennzeichnung und der darauf aufbauenden RFID-Systeme kann betrachtet werden, möglichst jedes Objekt unserer Umwelt mit einer eindeutigen Kennzeichnung auszustatten, Informationen über diese Objekte und deren Umgebung zu speichern sowie diese Daten zur weiteren Nutzung zur Verfügung zu stellen. Damit soll ermöglicht werden, anhand der kontinuierlich gesammelten Daten die gesamte Lebensdauer eines Objektes, Umwelteinflüsse, die auf dieses gewirkt haben, Änderungen in den Besitz- und Ortsverhältnissen und vieles mehr nachvollziehen zu können. Im Zuge dieser umfangreichen Datensammlung werden aber auch eine Reihe von Informationen gespeichert, die Auskunft über die näheren Lebensumstände derjenigen geben können, in deren Besitz sich die betreffenden Objekte befinden.

Mit zunehmender Verbreitung der elektronischen Produktkennzeichnung geht auch eine Steigerung der Anzahl der RFID-Lesegeräte und der dazugehörigen Datenverarbeitungen einher. Während beispielsweise eine RFID-Lösung für eine einzelne Bibliothek noch als relativ unkritisch bezüglich Ihrer Auswirkungen auf die Privatsphäre zu bewerten ist, so ändert sich dies drastisch, sobald etwa in anderen Anwendungsbereichen wie in Supermärkten oder öffentlichen Verkehrsmitteln kompatible RFID-Systeme eingesetzt werden.

Die für die Privatsphäre ursprünglich relativ unbedenkliche Verwaltung der Bibliotheksbestände mittels RFID-Kennzeichnung hat sodann zur Folge, dass die EPCs der mitgeführten Bücher an jedes beliebige RFID-Lesegerät weitergegeben werden, in dessen Aktionsbereich sie gelangen. Wie die Datenverarbeitungssysteme hinter diesen fremden Lesegeräten auf diese Produktcodes reagieren, entzieht sich vollkommen der Einflussmöglichkeit der Bibliothek, die ebenso wie der Entlehner des Buches weder Kenntnis von noch Kontrolle über diese Datenverarbeitungen hat.

Es liegt in weiterer Folge also daran, welche Interessen die Betreiber der einzelnen Datenverarbeitungen verfolgen, ob sie die Informationen, die sie beim zufälligen Erfassen dieser fremden Produktcodes sammeln können, speichern und Dritten zur Verfügung stellen. Für derartige allfällige Datensammlungen ist eine Teilnahme am EPC Network aber nicht Voraussetzung. Da es sich bei Electronic Product Codes um weltweit eindeutige Nummern handelt, kann jeder Betreiber eines Lesegerätes auf Basis dieser Nummern seine ganz persönliche Datensammlung entsprechend seinen spezifischen Interessen anlegen und diese gesammelten Informationen bei Bedarf abrufen und auswerten oder zu einem späteren Zeitpunkt doch noch in das EPC Network einbringen.

Die zuvor genannten Kriterien zur Gewährleistung der Privatsphäre sind im Bereich der möglichen Datensammlungen allesamt als verletzt zu betrachten. Die jederzeitige Möglichkeit zum Abruf des gespeicherten EPC ohne wirksame Zugriffsbeschränkung macht Datensparsamkeit ebenso wie eine Zweckbindung der Daten unmöglich, da nicht bekannt ist, wer auf die am RFID-Tag gespeicherten und im Internet abgelegten Daten zugegriffen hat. Anonymität oder Pseudonymität sind ebenfalls nicht gewährleistet, da ein Personenbezug beim Empfang des EPC, etwa durch Koppelung mit Kameras, Kunden- oder Kreditkarten, problemlos hergestellt werden kann. Das Kriterium der Vertraulichkeit der gesammelten Daten ist ebenso wie das Kriterium der Transparenz dadurch verletzt, dass der Betroffene im Regelfall keine Kenntnis vom Vorhandensein der Datensammlung hat. Dadurch ist schließlich auch das Kriterium des Vertrauens und der Absicherung als verletzt zu betrachten, da unbekannten Datenverarbeitern wohl kaum ernsthaft Vertrauen entgegengebracht werden kann und eine der Absicherung dienende Wahrnehmung von Auskunfts-, Korrektur- und Löschungsrechten ebenfalls nur gegenüber bekannten Datenverarbeitern wirksam ist. Ein Begehren nach Auskunft über die zum EPC eines in meinem Besitz befindlichen Gegenstandes gesammelten Daten, adressiert an „alle RFID-Lesegerätebetreiber meiner Stadt“, wird als undurchführbar gelten müssen.

### 4.3.2 Datenauswertung

Aufgrund der umfangreichen Möglichkeiten zur dezentralen Datensammlung durch eine unbekannte Anzahl in unserer Lebensumwelt angebrachter RFID-Lesegeräte sind die Möglichkeiten zur Datenauswertung natürlich von besonderer Bedeutung. Durch die Allgegenwärtigkeit der Datenverarbeitung in Form von Lesegeräten und Objekten, die von diesen „wahrgenommen“ werden, entsteht eine Fülle von Informationen über Objekte, Personen, Orte, Umweltbedingungen und die Zusammenhänge zwischen diesen. Für den Schutz der Privatsphäre ist in diesem Zusammenhang die Frage von Bedeutung, welche Daten wie einfach miteinander verknüpft werden können. Je leichter auf gesammelte Daten zugegriffen werden kann, und je einfacher eine Verknüpfung zwischen ihnen möglich ist, umso problematischer sind die möglichen Auswirkungen auf die Privatsphäre.

Auf Basis der Möglichkeiten des EPC Discovery Service ist die Verknüpfung der Daten zahlreicher Informationsquellen zu einem umfassenden Bericht über den bisherigen Lebenszyklus eines Objektes nicht nur vorstellbar sondern ausgewiesenes Ziel dieses Dienstes. Zurecht wird das Discovery Service von den Betreibern auch ausdrücklich als „die wertvollste aller Komponenten“ des EPC Networks bezeichnet, die viele Anwendungsmöglichkeiten für die verbesserten Produktinformationen eröffnet (VeriSign, 2004, S. 2).

Im Hinblick auf die Privatsphäre der Betroffenen ist diese Verknüpfbarkeit von Informationen ausgesprochen problematisch. So können jederzeit anhand der EPCs, die eine Person bei sich trägt, Daten zu den zugehörigen Gegenständen und somit dem Besitzer der Gegenstände abgerufen und zu einem Gesamtbild zusammengeführt werden. Auf diese Art ließe sich anhand der gespeicherten Orts- und Zeitangaben ein Bewegungsprofil der betroffenen Person erstellen. Die in der Physical Markup Language vorgesehenen Querverweise zu anderen Produktcodes ermöglichen die Einbeziehung von Informationen zu anderen Gegenständen, die der betroffene Benutzer zwar zum Zeitpunkt des Abrufs nicht bei sich trägt, die so aber dennoch mit ihm in Verbindung gebracht werden und weitere Informationen über ihn enthüllen können.

Auf diese Weise könnte ein weitläufiges Netzwerk von miteinander in Beziehung stehenden Gegenständen bei Bedarf Auskunft über eine Person, ihre Vorlieben, ihre finanzielle Lage – abgeleitet vom Wert und dem Alter der mit den EPCs gekennzeichneten Produkte – und andere private Einzelheiten geben, während für die betroffene Person kaum eine Möglichkeit besteht, die Existenz einer derartigen Datensammlung überhaupt wahrzunehmen oder eine solche gar zu verhindern.

Die Kriterien der Datensparsamkeit und Zweckbindung wären durch derartige Datensammlungen auf Vorrat ohne vorher klar definierten Verwendungszweck ganz klar verletzt. Findet die Auswertung der Datensammlung zum Zeitpunkt des Empfanges der Produktcodes statt, ist das Anonymitäts- und Pseudonymitätskriterium ebenfalls verletzt, da zu diesem Zeitpunkt ja problemlos feststellbar ist, wer die betreffenden Produktcodes bei sich trägt. Das Transparenzkriterium ist auch im Bezug auf die Datenauswertung nicht erfüllt, da die betroffene Person keine Kenntnis davon erlangen kann, wer wann Daten zu in ihrem Besitz befindlichen Produkten abruft oder gar zu umfangreichen Profilen aggregiert.

### 4.3.3 Schutzmöglichkeiten

Im Hinblick auf die Möglichkeiten, sich und seine Daten vor unerwünschten Datensammlungen zu schützen, erweist sich eine in vielen Anwendungsbereichen positiv bewertete Eigenschaft von RFID-Systemen als wesentlicher Nachteil: die Möglichkeit zur Datenerfassung ohne Berührung und direkten Sichtkontakt zum Datenträger.

Während das Scannen von Barcode-Etiketten auf Produkten aufgrund des nötigen Sichtkontaktes zwischen Lesegerät und Etikett im Regelfall nicht ohne das Wissen und Zutun des Konsumenten möglich ist, bieten RFID-Systeme die Möglichkeit eine Reihe von Etiketten sozusagen „im Vorbeigehen“ ohne weitere menschliche Mithilfe zu erfassen. Darüber hinaus bestehen zahlreiche Möglichkeiten, Lesegeräte unaufdringlich zu positionieren und durchaus unauffällig in ihre Umgebung zu integrieren und damit der Wahrnehmung der Betroffenen weitgehend zu entziehen.

Die geringen Abmessungen der RFID-Tags fördern darüber hinaus eine unauffällige Kennzeichnung von Gegenständen, die es letztendlich den Betroffenen unmöglich macht, mit Sicherheit festzustellen, ob an einem bestimmten Objekt RFID-Tags angebracht sind oder nicht. Genau diese verbleibende Unsicherheit stellt jedoch eines der wesentlichen Probleme der eindeutigen Produktkennzeichnung mittels RFID-Tags in Bezug auf die Privatsphäre dar.

Wie bereits zuvor ausgeführt, formulierte das deutsche Bundesverfassungsgericht (1983) in der Begründung des Volkszählungsurteils: „Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.“

Eine allgemeine Bekanntheit von RFID-Systemen vorausgesetzt – die bei entsprechender Verbreitung der Technologie als gegeben angenommen werden kann – führt die Unmöglichkeit mit absoluter Sicherheit festzustellen, ob ein Gegenstand mit einem RFID-Tag gekennzeichnet ist oder nicht, dazu, dass es den betroffenen Personen nicht mehr möglich ist, mit hinreichender Sicherheit zu überschauen, welche sie betreffenden Informationen in bestimmten Bereichen ihrer sozialen Umwelt bekannt sind und welche nicht. Dies hätte aber wiederum zur Folge, dass Personen auch dann in ihrer Privatsphäre beeinträchtigt sein können, wenn kein einziges Objekt in ihrem Umfeld mit einem RFID-Tag ausgestattet wäre, da sie mangels eigener Möglichkeiten zur Überprüfung generell von einer Präsenz solcher Tags ausgehen müssten.

Schutzmaßnahmen gegen eine ungewollte Datenübermittlung durch RFID-Tags scheitern in der Regel also bereits daran, dass sie auf das Vertrauen der betroffenen Personen in ihre Wirksamkeit an-

gewiesen sind. Besteht dieses Vertrauen nicht – was angesichts der bisherigen Vorgangsweisen der in diesem Bereich führenden Industrie- und Handelsunternehmen leider anzunehmen ist – sind technische Schutzmaßnahmen zur Wahrung der Privatsphäre als wirkungslos zu betrachten. Darüber hinaus versuchen die meisten der bisher vorgeschlagenen „Schutzmaßnahmen", wie beispielsweise der Blocker Tag (Juels, Rivest, Szydlo, 2004) oder das von Langheinrich (2002) vorgeschlagene Privacy Awareness System, die Verantwortung für den Datenschutz vom Datenverarbeiter weg zu den betroffenen Konsumenten zu verlagern.

„Lösungen", die eine Funkstörung durch Auskleidung des Einkaufskorbes mit Alufolie oder das ständige Mitführen eines unter gewissen Umständen wirksamen Blocker Tags, der bestimmte EPC-Nummernbereiche vor Lesezugriffen schützen soll, vorschlagen, versuchen ebenso die Datenverarbeiter von der Verantwortung für den Schutz der Privatsphäre der Konsumenten zu entbinden wie dies Vorschläge zur Deaktivierung der RFID-Tags „auf Wunsch des Konsumenten" am Ausgang des Geschäftslokales tun.

Werden diese Vorschläge aufgrund angeblich fehlender technischer Alternativen angenommen, wandelt sich der Schutz der Privatsphäre von einer grundsätzlich gewährleisteten und garantierten Sicherheit zu einer theoretischen Möglichkeit nach Maßgabe des persönlichen Informationsstandes, der persönlichen technischen Möglichkeiten und der Fähigkeit jedes Einzelnen, sich selbst vor unerwünschten Eingriffen in die Privatsphäre zu schützen.

# 5 Zusammenfassung

Wie in den vorliegenden Ausführungen gezeigt wurde, kann die eindeutige Kennzeichnung von Produkten mittels RFID-Tags zur drastischen Einschränkungen der Privatsphäre der Betroffenen führen. Dies ist insbesondere auch deshalb von Bedeutung, da die eindeutige Kennzeichnung von Produkten eine wichtige Grundlage für weitere RFID-Anwendungen (wie beispielsweise zur Abwicklung von Reklamationsfällen und Gewährleistungsforderungen) darstellt.

Für die Konsumenten ist ein Einsatz von RFID-Systemen nicht zuverlässig feststellbar, weshalb sie in der Regel auch nicht gegen die Sammlung und Nutzung ihrer Daten in derartigen Systemen protestieren und diese für sich ausschließen können. Eine Verweigerung der Nutzung von RFID-Systemen könnte darüber hinaus mit Nachteilen und Beschränkungen verbunden sein, wenn Service- und Gewährleistungsansprüche an eine Teilnahme an derartigen Systemen gebunden sind.

Soll ein möglichst hoher Nutzen aus den verfügbaren RFID-Technologien gezogen werden, so wird es unausweichlich sein, den Auswirkungen der Technologien auf die Privatsphäre der Betroffenen verstärkt Beachtung zu schenken und in einem gemeinsamen Bemühen zusammen mit den Betroffenen nach Lösungsmöglichkeiten zu suchen.

Bisher vorgestellte „Lösungen“ der Privatsphären-Problematik zielen meist auf eine Abwälzung der Verantwortung für den Schutz der personenbezogenen Daten auf die Konsumenten ab. Dies hätte eine Wandlung weg vom grundsätzlichen Schutz der Privatsphäre hin zum Selbstschutz-Prinzip zur Folge.

In seinem oft zitierten Artikel im Scientific American, mit dem Mark Weiser (1991) den Begriff des Ubiquitous Computing prägte, führte er – weniger oft zitiert – bezüglich des Schutzes der Privatsphäre folgendes aus, das der RFID-Entwicklung künftig als Ziel dienen sollte: *„If designed into systems from the outset, these techniques can ensure that private data does not become public. A well-implemented version of ubiquitous computing could even afford better privacy protection than exists today.“*

In diesem Sinne sind die Gestalter von RFID-Systemen aufgefordert, die legitimen Interessen der Betroffenen nach Schutz ihrer Privatsphäre angemessen zu honorieren und bereits in der Planungsphase ausreichend zu berücksichtigen. Unterstellt man, dass die legitimen Interessen der Konsumenten schlussendlich obsiegen, empfiehlt sich eine solche Vorgangsweise im übrigen auch aus rein wirtschaftlichen Überlegungen, wenn man bedenkt, dass grundlegende Systemänderungen umso teurer sind, je später in der Entwicklungsphase sie vorgenommen werden.

# 6 Literaturhinweise

Agarval, Vivek (2001), Report: Assessing the benefits of Auto-ID Technology in the Consumer Goods Industry. MIT AUTO-ID CENTER, 1. September, http://www.autoidlabs.com/whitepapers/CAM-WH-003.pdf, Abruf am 21.11.2004.

AIM – Association for Automatic Identification and Mobility (2004), What is Radio Frequency Identification (RFID)? http://www.aimglobal.org/technologies/rfid/what_is_rfid.asp, Abruf am 09.06.2004.

Brock, David L., Timothy P. Milne,Yun Y. Kang, and Brendon Lewis (2001), White Paper: The Physical Markup Language – Core Components: Time and Place. MIT AUTO-ID CENTER, 1. June. http://www.autoidlabs.com/whitepapers/MIT-AUTOID-WH-005.pdf, Abruf am 21.11.2004.

Brock, David L. (2001), White Paper The Electronic Product Code (EPC) A Naming Scheme for Physical Objects. MIT AUTO-ID CENTER, 1. January. http://www.autoidlabs.com/whitepapers/MIT-AUTOID-WH-002.pdf, Abruf am 21.11.2004.

Bundesrepublik Deutschland – Bundesverfassungsgericht (BVERFGE) (1983), 65,1; Urteil vom 15.12.1983, http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm, Abruf am 21.11. 2004.

EAN Austria (2004), Electronic Product Code.

Europäisches Parlament und Rat (1995), Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. http://www.dsk.gv.at/31995L0046d.htm, Abruf am 21.11.2004.

Juels, Ari, Ronald L. Rivest and Michael Szydlo (2004), The Blocker Tag – Selective Blocking of RFID Tags for Consumer Privacy, RSA Security Inc., http://www.rsasecurity.com/solutions/idmgt/whitepapers/RFID_WP_0404.pdf, Abruf am 21.11.2004.

Kearney A. T.(2003), Meeting the Retail RFID Mandate – A discussion of the issues facing CPG companies, November. http://www.atkearney.com/shared_res/pdf/Retail_RFID_S.pdf, Abruf am 21.11.2004.

Langheinrich, Marc (2002), A Privacy Awareness System for Ubiquitous Computing Environments. In Boriello, G. and L. E. Holmquist (editors), 4th International Conference on Ubiquitous Computing (UbiComp2002), September, Berlin: Springer Verlag, S. 237-245. http://www.inf.ethz.ch/vs/publ/papers/privacy-awareness.pdf, Abruf am 21.11.2004.

Mattern, Friedemann und Marc Langheinrich (2001), Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge. In: Müller, G. und M. Reichenbach (Hg): Sicherheitskonzepte für das Internet, S. 7–26. Berlin: Springer-Verlag.

Mattern, Friedemann (2002), Der Trend zur Vernetzung aller Dinge – Pervasive Computing und die Zukunft des Internets. In: Neue Kommunikationsanwendungen in modernen Netzen, S. 9–13. ITG-Fachtagung, Februar. http://www.inf.ethz.ch/vs/publ/papers/VernetzungAllerDinge.pdf, Abruf am 21.11.2004.

Metro Group (2004), Future Store Initiative, Virtual Tour trhough the Extra Future Store, http://www.future-store.org/multimedia/virtual_tour_mpg1.zip, Abruf am 21.11.2004.

OECD – Organisation for Economic Co-operation and Development (1980), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 23. September. http://www.oecd.org/EN/document/0,,EN-document-43-1-no-24-10255-43,00.h%tml, Abruf am 18.12.2002.

Rössler, Beate (2001), Der Wert des Privaten. Frankfurt/Main: Suhrkamp.

VeriSign (2004), The EPC Network: Enhancing the Supply Chain, 2004, http://www.verisign.com/nds/directory/epc/epc_whitepaper.pdf, Abruf am 12.07.2004.

Wan, Dadong (2000), Magic Wardrobe: Situated Shopping from Your Own Bedroom, Second International Symposium on Handheld and Ubiquitous Computing (HUC 2000), 25-27 September, Bristol, UK, http://www.accenture.com/xdoc/en/services/technology/publications/magicwardrobe-huc2000.pdf, Abruf am 21.11.2004.

Weiser, Mark (1991), The Computer for the 21st Century, Scientific American, September, S. 66-75.

## *Bisher erschienene* manu:scripte

ITA-01-01 Gunther Tichy, Walter Peissl (12/2001): Beeinträchtigung der Privatsphäre in der Informationsgesellschaft. <http://www.oeaw.ac.at/ita/pdf/ita_01_01.pdf>

ITA-01-02 Georg Aichholzer(12/2001): Delphi Austria: An Example of Tailoring Foresight to the Needs of a Small Country. <http://www.oeaw.ac.at/ita/pdf/ita_01_02.pdf>

ITA-01-03 Helge Torgersen, Jürgen Hampel (12/2001): The Gate-Resonance Model: The Interface of Policy, Media and the Public in Technology Conflicts. <http://www.oeaw.ac.at/ita/pdf/ita_01_03.pdf>

ITA-02-01 Georg Aichholzer (01/2002): Das ExpertInnen-Delphi: Methodische Grundlagen und Anwendungsfeld „Technology Foresight". <http://www.oeaw.ac.at/ita/pdf/ita_02_01.pdf>

ITA-02-02 Walter Peissl (01/2002): Surveillance and Security – A Dodgy Relationship. <http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf>

ITA-02-03 Gunther Tichy (02/2002): Informationsgesellschaft und flexiblere Arbeitsmärkte. <http://www.oeaw.ac.at/ita/pdf/ita_02_03.pdf>

ITA-02-04 Andreas Diekmann (06/2002): Diagnose von Fehlerquellen und methodische Qualität in der sozialwissenschaftlichen Forschung. <http://www.oeaw.ac.at/ita/pdf/ita_02_04.pdf>

ITA-02-05 Gunther Tichy (10/2002): Over-optimism Among Experts in Assessment and Foresight. <http://www.oeaw.ac.at/ita/pdf/ita_02_05.pdf>

ITA-02-06 Hilmar Westholm (12/2002): Mit eDemocracy zu deliberativer Politik? Zur Praxis und Anschlussfähigkeit eines neuen Mediums. <http://www.oeaw.ac.at/ita/pdf/ita_02_06.pdf>

ITA-03-01 Jörg Flecker und Sabine Kirschenhofer (01/2003): IT verleiht Flügel? Aktuelle Tendenzen der räumlichen Verlagerung von Arbeit. <http://www.oeaw.ac.at/ita/pdf/ita_03_01.pdf>

ITA-03-02 Gunther Tichy (11/2003): Die Risikogesellschaft – Ein vernachlässigtes Konzept in der europäischen Stagnationsdiskussion. <http://www.oeaw.ac.at/ita/pdf/ita_03_02.pdf>

ITA-03-03 Michael Nentwich (11/2003): Neue Kommunikationstechnologien und Wissenschaft – Veränderungspotentiale und Handlungsoptionen auf dem Weg zur Cyber-Wissenschaft. <http://www.oeaw.ac.at/ita/pdf/ita_03_03.pdf>

ITA-04-01 Gerd Schienstock (1/2004): Finnland auf dem Weg zur Wissensökonomie – Von Pfadabhängigkeit zu Pfadentwicklung. <http://www.oeaw.ac.at/ita/pdf/ita_04_01.pdf>

ITA-04-02 Gunther Tichy (6/2004): Technikfolgen-Abschätzung: Entscheidungshilfe in einer komplexen Welt. <http://www.oeaw.ac.at/ita/pdf/ita_04_02.pdf>

ITA-04-03 Johannes M. Bauer (11/2004): Governing the Networks of the Information Society – Prospects and limits of policy in a complex technical system. <http://www.oeaw.ac.at/ita/pdf/ita_04_03.pdf>

ITA-04-04 Ronald Leenes (12/2004): Local e-Government in the Netherlands: From Ambitious Policy Goals to Harsh Reality. <http://www.oeaw.ac.at/ita/pdf/ita_04_04.pdf>

ITA-05-01 Andreas Krisch (01/2005): Die Veröffentlichung des Privaten – Mit intelligenten Etiketten vom grundsätzlichen Schutz der Privatsphäre zum Selbstschutz-Prinzip. <http://www.oeaw.ac.at/ita/pdf/ita_05_01.pdf>