WISO Diskurs

Expertisen und Dokumentationen
zur Wirtschafts- und Sozialpolitik

September 2007

Auf dem Weg zum gläsernen Verbraucher?

Verbraucherschutz bei Kundenkarten und RFID-Chips

Gesprächskreis Verbraucherpolitik

FRIEDRICH EBERT STIFTUNG

Dokumentation einer Veranstaltung der Abteilung
Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung

Auf dem Weg zum gläsernen Verbraucher?

Verbraucherschutz bei Kundenkarten und RFID-Chips

Der Gesprächskreis „Verbraucherpolitik“

Der Gesprächskreis „Verbraucherpolitik“ der Friedrich-Ebert-Stiftung will den kontinuierlichen Dialog über aktuelle und grundsätzliche verbraucherpolitische Themen fördern. An ihm beteiligen sich Entscheidungsträger, Meinungsbildner und Experten aus Verbraucherverbänden, Politik, Administration, Wirtschaft, sonstigen Verbänden, Medien und Wissenschaft.

Ziel ist es, die Interessen von Verbraucherinnen und Verbrauchern gegenüber Politik, Wirtschaft und Gesellschaft zu unterstützen und den Stellenwert von Verbraucherpolitik – anhaltend – zu erhöhen. Der Gesprächskreis versteht Verbraucherpolitik nicht nur als defensive Schutzfunktion für den einzelnen Konsumenten, sondern als Wirtschaftspolitik von der Nachfrageseite und als gesamtgesellschaftliche Gestaltungsaufgabe.

Verbraucherpolitik ist eine Querschnittsaufgabe und muss in allen Politikbereichen – auf nationaler und internationaler Ebene – verankert und vernetzt werden. Zu den zu behandelnden Themenbereichen gehören:

- Verbraucherschutz im Bereich Gesundheit/Ernährung;
- Verbraucherschutz bei Finanzdienstleistungen;
- Verbraucherschutz im Bereich Bauen, Energie, Umwelt, Verkehr;
- Verbraucherschutz im Bereich Medien, Telekommunikation, Post;
- Verbraucherschutz in sonstigen Wirtschaftsfragen.

Die Ergebnisse der Veranstaltungen werden seit 2007 in der Schriftenreihe WISO Diskurs (zuvor in den Schriftenreihen „Gesprächskreis Verbraucherpolitik“ und „Wirtschaftspolitische Diskurse“) wiedergegeben.

Sprecher des Gesprächskreises ist *Manfred Zöllmer, MdB*, SPD-Bundestagsfraktion, Stellvertretender Vorsitzender des Bundestagsausschusses für Ernährung, Landwirtschaft und Verbraucherschutz.

http://www.fes.de/wiso/sets/s_verbr.htm

Inhalt

Die Dokumentation wird von der Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung veröffentlicht. Die Ausführungen und Schlussfolgerungen sind von der Autorin in eigener wissenschaftlicher Verantwortung vorgenommen worden.

Impressum: © Friedrich-Ebert-Stiftung | Herausgeber: Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung | Godesberger Allee 149 | 53175 Bonn | Fax 0228 883 398 | www.fes.de/wiso | Gestaltung: pellens.de | Druck: bub Bonner Universitäts-Buchdruckerei | ISBN: 978-3-89892-748-2

Vorwort

Über den Verbraucher werden immer mehr Informationen gesammelt. Datensammler des 21. Jahrhunderts ist dabei nicht mehr allein der Staat, Datensammler sind in immer stärkerem Maß auch die Unternehmen. Damit ist der Datenschutz eine zentrale Frage der wirtschaftlichen Verbraucherpolitik. Grund genug für den Gesprächskreis „Verbraucherpolitik" der Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung, dieses Thema in der Veranstaltung zum Thema: **„Verbraucherschutz bei Kundenkarten und RFID-Chips"** am 6.12.2006 in Wuppertal aufzugreifen.

Die Abkürzung RFID steht für Radiofrequenz-Identifikation. Sie ermöglicht – auf berührungslose Weise – eine automatische eindeutige Identifikation (Funkerkennung) und Lokalisierung von Objekten. Wenngleich in der Öffentlichkeit noch wenig bekannt, hält der Einsatz von RFID-Chips unaufhaltsam Einzug in die Wirtschaft, Wissenschaft und in öffentliche Einrichtungen, auch in den Alltag der Verbraucher.

Die neue Technik bietet viele Chancen, die auch Verbrauchern zugute kommen. Denn sie besitzt ein erhebliches Innovationspotenzial zur Effizienz- und Qualitätssteigerung in den unterschiedlichsten Branchen. Speziell in der Logistik, bei der Warenverfolgung und Prozesssteuerung, liegen ihre Vorteile auf der Hand.

Nicht nur Vorteile, sondern auch Risiken werden beim Einsatz von RFID-Chips bei verbrauchernahen Anwendungsfeldern gesehen: Im Einzelhandel, bei Eintrittskarten/Tickets, PKW-Wegfahrsperren, Bahncard und Fahrkarten, Ausweisen, Sport, Geldscheinen, bei der Einpflanzung unter die Haut oder in Büchern. Daten- und Verbraucherschützer befürchten hier die Gefahr einer umfassenden Verbraucherüberwachung und den Verlust der informationellen Selbstbestimmung, insbesondere wenn eine Verknüpfung mit personenbezogenen Daten erfolgt. Denn da die RFID-Systeme drahtlos arbeiten, kann das Auslesen der Daten ohne Wissen der Besitzer erfolgen.

Befürchtungen vor Missbrauch gibt es auch gegenüber Kundenkarten oder sonstigen Rabatt- und Bonussystemen, mit deren Hilfe Unternehmen eine Vielzahl persönlicher Daten und Informationen über das Kaufverhalten von Kunden erhalten können, wenn diese zustimmen, dass ihre Daten für Werbe- und Marktforschungszwecke verwendet werden dürfen. Immerhin gibt es in Deutschland inzwischen rund 100 Millionen Kundenkarten. Kritisiert wird die mangelnde Transparenz der Einwilligungserklärungen, so dass von freiwilliger Zustimmung und bewusster Entscheidung der Kunden für die Nutzung ihrer persönlichen sowie ihrer konsumbezogenen Daten keine Rede sein könne. Fast alle Kundenbindungssysteme würden mehr Daten sammeln, als für das Durchführen eines Bonussystems notwendig sei. Fragwürdig sei z. B. die Abfrage des vollständigen Geburtsdatums, des Berufs, des Einkommens oder von Hobbys.

Die gemeinsame Schnittmenge zwischen der Kundenkartenproblematik und der RFID-Anwendung ist der Datenschutz. Die Gefahr liegt in einer unzulässigen individualisierten Datenverknüpfung.

Um die zweifellos vorhandenen Potenziale der digitalen Technik zu entfalten, bedarf es einer höheren gesellschaftlichen Akzeptanz, die den Abbau von Ängsten vor Datenmissbrauch voraussetzt. Das Spektrum der vorgeschlagenen Lösungsmöglichkeiten, um einem denkbaren Datenmissbrauch Einhalt zu gebieten, ist breit: Selbstverpflichtungen der Wirtschaft, Einführung von Gütesiegeln, mehr Transparenz über den Ein-

satz, Verwendungszweck und Inhalt von Kundenkarten und RFID-Chips sowie über die Dauer der Speicherung von Daten, Kennzeichnungspflicht der Kommunikationsvorgänge, Deaktivierungsmöglichkeit der RFID-Chips, Schutz vor unbefugtem Auslesen der gespeicherten Daten, Verbot der Erstellung von Verhaltens-, Nutzungs- und Bewegungsprofilen aus Daten von Kundenkarten und RFID-Chips aus verschiedenen Produkten.

Auf der Veranstaltung wurde über das Spektrum der Risiken für Verbraucher, aber auch über die Vorteile des Einsatzes von Kundenkarten und RFID-Chips informiert und debattiert. Darauf aufbauend wurde über die angesprochenen Verbesserungsideen im Sinne der Verbraucher und einer höheren gesellschaftlichen Akzeptanz diskutiert. Während Verbraucher- und Datenschützer umfassende daten- bzw. verbraucherschutzrechtliche Regelungen im Zusammenhang mit der Nutzung von RFID-Chips forderten, sahen Anwender und Hersteller von RFID keinen Handlungsbedarf. In Deutschland seien die datenschutzrechtlichen Rahmenbestimmungen so eindeutig, dass eine missbräuchliche Verwendung der RFID-Technik zur Verletzung der informationellen Selbstbestimmung eigentlich ausgeschlossen sei.

Die Diskussionen und Ergebnisse der Tagung sind im vorliegenden Band themenstrukturiert und -zentriert zusammengefasst. Der Text der Dokumentation stammt aus der Feder von Johanna Maiwald, Politikwissenschaftlerin M.A. aus Berlin.

Hannelore Hausmann
Leiterin des
Gesprächskreises „Verbraucherpolitik“

Zusammenfassung und Politikempfehlungen

Funketiketten oder -chips und Kundenkarten sind zwei prominente Beispiele für Anwendungen, die den Verbraucherschutz in einer digitalen Welt auf den Plan rufen. Ihr wesentlicher Berührungspunkt liegt im häufig nicht ausreichenden Datenschutz.

Die Vorteile von RFID[1] und Kundenkarten aus Verbrauchersicht

Aus der Sicht von Verbrauchern bieten RFID-Etiketten im Einzelhandel zunächst verbesserte Informationen über Produkte. Das können Informationen über spezielle Anwendungen sein, die auf dem Chip gespeichert werden, die Überprüfung der Echtheit von Medikamenten oder die Kontrolle des wirklichen Mindesthaltbarkeitsdatums sein. Zudem versprechen Industrie und Handel Kostenersparnisse durch verbesserte und schnellere Organisationsabläufe, die sich in Produktpreisen niederschlagen könnten. Logistische Vorteile durch RFID-Kennzeichnung sind auch in ganz anderen Bereichen denkbar, so bei der Gepäckabfertigung oder in Bibliotheken. Vereinfachte Zugangskontrollen sind ein expandierendes Feld und schließlich kann die gezielte Verbindung von persönlichen Daten wie sie etwa in Krankenhäusern ausprobiert werden, eine genauere und schnellere Informationsübermittlung in sensiblen Bereichen sichern.

Bei Kundenkarten sorgen kleine Rabatte von zwei, drei Prozent dafür, dass Kunden persönliche Daten herausgeben, auf deren Basis individuelle oder allgemeine Kundenprofile erstellt werden. Sowohl Kunden als auch Unternehmen können im Einzelfall von individuellem Marketing und Werbeangeboten profitieren.

Risiken für die Privatsphäre

Bei RFID-Systemen wurden die Ursachen für mangelnden Schutz von persönlichen Daten vor allem auf der Anbieterebene gesehen, d. h. in der Gestaltung und dem Einsatz der RFID-Produkte. Viele Kritiker sehen das Hauptproblem im zentralen Merkmal der RFID-Technologie, d.h. der Möglichkeit, ein jedes Objekt, das mit einer RFID-Etikette bestückt ist, einzeln zu identifizieren. Denn damit kann auch einem Verbraucher oder einer Verbraucherin eine ganz bestimmte Ware, die sie erworben haben, direkt zugeordnet werden. Von Industrievertretern wird eingeräumt, dass es bei Einzelhandelskunden zur Verknüpfung von eigenen personenbezogenen Daten und Objektdaten kommen kann. Dies ist beispielsweise beim Kauf einer RFID-bestückten Ware möglich, wenn zugleich die Kundenkarte eingelesen wird. Auf diese Weise aber lassen sich individuelle Konsummuster erstellen. Auch weitere Möglichkeiten, Handlungs- und Bewegungsmuster von konkreten Personen zu verfolgen, sind denkbar. Die Ursprungsidee der genauen Registrierung und Lenkung von Waren erweitert sich also unverhofft, wenn solche einzeln identifizierbaren Teile die Daten des Besitzers mitliefern.

Verbraucherschützer machen daher auf die Sensibilität gegenüber personenbeziehbaren Daten aufmerksam, für deren Unversehrtheit genauso gesorgt werden müsse wie für personenbezogene Daten.

Erschwerend kommt hinzu, dass aufgrund der Datenübertragung per Funk die Datenaufnahme vom Betroffenen unbemerkt vorgenommen werden kann. Dies verschärft sich durch den Umstand, dass die Funketiketten wegen ihrer geringen Größe unbemerkt z. B. in Kleidung ange-

1 RFID ist die Abkürzung für Radio Frequency Identification.

bracht und belassen werden können. Schon heute denken Bekleidungsunternehmen über die RFID-Verwendung zur Sortierung von Kleidern für Distributionszwecke nach.

Einzelne Kritiker plädieren deshalb dafür, den breiten Einsatz von RFID im Alltag zu überdenken und in besonders sensiblen Feldern von vorne herein darauf zu verzichten.

Die Mehrheit der Podiumsteilnehmer war allerdings der Ansicht, dass die Technologie für Unternehmen so viele Vorteile bietet, dass sich ihre Einführung kaum vermeiden lassen werde. Nichtsdestotrotz war es unter Vertretern der Verbraucherseite Konsens, dass es bei allen geplanten RFID-Anwendungen eine Vielzahl von Schwierigkeiten gibt, für die Lösungen im technischen Bereich oder bei Bedingungen, unter welchen RFID-Tags angewendet werden, noch gefunden werden müssen.

Weitere Kommentatoren sahen schließlich auch die Behörden in der Pflicht, für angemessene Vorschriften zu sorgen, die Missbrauch rechtlich besser als bislang absichern würden.

Im Fall von Kundenkarten lassen sich Missbrauchsmöglichkeiten von Daten direkt nachvollziehen. Die hier erhobenen personenbezogenen Daten werden in große Kundendatenbanken eingespeist, die vielfach kommerziell ausgewertet werden können. So sind nicht nur Werbeunternehmen an Kundenprofilen interessiert, sondern insbesondere der steigende Umsatz von Auskunfteien aller Art macht aus dem Verkauf von Kundendateien ein lukratives Geschäft.

Beim Thema Kundenkarten stand im Mittelpunkt der Diskussion die Selbstverantwortung von Kunden ihren Daten gegenüber. Stellungnahmen von Kritikern und Politik machten deutlich, dass dieser Ansatz zuweilen als Ausrede gegenüber einem verbesserten Umgang von Kartenanbietern mit persönlichen Daten ihrer Kunden dient. Insbesondere die Art und Weise, wie Kunden in die Aufnahme ihrer Daten einwilligen können, bestimmt stark das Ergebnis der individuellen Entscheidung. Datensparsamkeit beim Erheben von Kundendaten allgemein – sei es als Selbstverpflichtung der Unternehmungen oder als gesetzliche Vorschrift – leistet eine Abhilfe gegen potenziellen Datenmissbrauch, so das übergreifende Credo.

Empfehlungen zum weiteren Verfahren

Zur Verhinderung von Datenmissbrauch zeichneten sich im Wesentlichen drei Hauptstrategien ab. Die erste hat die Datensicherheit im Blick, für die technische Lösungen gefunden werden müssen. Angesichts der unklaren Sicherheit der RFID-Tags im deutschen Reisepass werden Entwicklungen in diesem Bereich genau von der Öffentlichkeit verfolgt werden. Man kann davon ausgehen, dass sie Ausstrahlungskraft auf Vertrauen in die RFID-Technologie in zukünftigen privatwirtschaftlichen Anwendungen mit Kundennähe haben werden.

Die Politik ist jedoch nicht nur bei der Bewertung der Sicherheit von Anwendungen mit hoheitlichen Funktionen gefragt. Da eine Datenverschlüsselung, die hohen Sicherheitsstandards entspricht, sowohl in der Anschaffung als auch im Betrieb teuer ist, wird es im kommerziellen Bereich zu Abwägungen zwischen Sicherheitsanspruch und Finanzierbarkeit kommen. Wie die Veranstaltung zeigte, spielt die Kostenfrage auch bei Überlegungen, wie RFID-Tags nach Erfüllung ihrer Funktion abgeschaltet werden könnten, eine wichtige Rolle.

Gemäß einer zweiten Strategie, die auf die zivilgesellschaftliche Selbstorganisation von Interessen auf Verbraucher- und auf Unternehmerseite setzt, könnten in diesem Zusammenhang Gütesiegel und Selbstverpflichtungserklärungen von Unternehmen eine größere Rolle in der Debatte bekommen. Zwei Aspekte allerdings machen deutlich, dass es nötig werden kann, anwendungsspezifische gesetzliche Standards zu veranlassen. Zum einen ist es seit Beginn der Moderation von Unternehmer- und Verbraucherperspektiven zum Thema RFID durch das Bundesverbraucherschutzministerium vor zwei Jah-

ren zu keiner freiwilligen Selbstverpflichtung von Unternehmerverbänden gekommen. Die gemeinschaftliche Haftung im Schadensfall scheint hier eine zu große Hürde zu sein. Zum anderen setzt die Vielfalt von Aspekten, die bei RFID den Datenschutz tangieren, einen sehr hohen Anspruch an die Informationsaufnahme und Sachkompetenz des Verbrauchers/der Verbraucherin, die ihn oder sie in die Lage versetzen würden, über die gewünschte Sicherheit zu urteilen. So kann auch eine Kennzeichnungspflicht von Produkten, die RFID-Chips erhalten, nur bedingt weiterhelfen. Im Kern eines politisch verantwortlichen Umgangs mit der neuen Technologie liegt es also, schon im Vorfeld eines breiten Roll-Outs Rahmenbedingungen zu setzen, die gewährleisten, dass sowohl der Handel als auch Verbraucher von den Innovationen profitieren können.

Nichtsdestotrotz erweist es sich als sinnvoll, daneben den offenen Dialog mit den unterschiedlichen Interessenvertretern zu fördern und zu begleiten. So kann die Privatwirtschaft beispielsweise früh erkennen, welche Anwendungen mehr und welche weniger auf die Akzeptanz von Verbrauchern stoßen. Unternehmensvertreter bestätigten, dass sie bereits Lernprozesse durchlaufen hätten. Verbraucherverbände und Bürgerorganisationen erhalten mehr Zugang zu Informationen und der Gesetzgeber Signale, wo letztlich Handlungsbedarf von staatlicher Seite entsteht.

Im Rahmen der dritten Strategie, die sich an die gesetzliche Sicherung des Datenschutzes richtet, müssen noch zwei weitere Aspekte geklärt werden:

Es ist vielfach darauf hingewiesen worden, dass geltende Datenschutzbestimmungen, an welchen sich Unternehmen bei der Ausgestaltung der RFID-Anwendungen orientieren, das Problem haben, dass ein Verstoß dagegen kaum Folgen nach sich zieht. Spürbare gesetzlich fest geschriebene Sanktionen könnten den Datenschutz also mittelbar verstärken.

Schließlich sollte eine wirksame Technologiegestaltung ihren Schwerpunkt nicht bei der Begrenzung möglicher negativer Folgen ansetzen. Gerade die Ebene der Datenerhebung bietet dem Gesetzgeber einen großen Handlungsspielraum, der Probleme von Beginn an unterbinden kann. Dazu gehört im Bereich von Kundenkarten die verbindliche Einführung einer Opt-In-Option bei der Einwilligung zur Freigabe persönlicher Daten, die Verpflichtung zur anonymisierten Aufnahme von personenbezogenen Daten oder kundenfreundliche Abmeldeoptionen. Im öffentlichen Bereich und bei verbrauchernahen RFID-Anwendungen könnte man beispielsweise über eine frühzeitige Trennung zwischen Datenbanken mit persönlichen und personenbeziehbaren Daten nachdenken oder auch die regelmäßige Prüfung der Datenschutzkonformität von Anwendungen veranlassen.

1. Was ist ein RFID-Chip?

RFID ist die Abkürzung für *Radio Frequency Identification*. Radio Frequency ist der englische Ausdruck für Funk, über den Informationen aus dem Chip an ein Lesegerät kommuniziert werden. ID, also Identifikation, bezieht sich auf den Chip, der eine weltweit eindeutige Seriennummer, die sogenannte EPC-Nummer enthält (EPC – European Product Code).

RFID ist ein System, mit dem Objekte über das Auslesen von Daten identifiziert werden können. Häufig wird im Zusammenhang mit der Technologie von Transpondern, Tags, Smartlabeln oder Funketiketten gesprochen. Ein RFID-Transponder setzt sich aus einem Silizium-Chip und einer Kupfer- oder Aluminiumantenne zusammen. Die Bezeichnung „Transponder" bezieht sich auf die Stellung des einzelnen RFID-Speicherelements im gesamten RFID-System: Der Transponder ist Datenträger und Überträger zugleich, der seine im Chip gespeicherte Information über die Antenne an ein Lesegerät, das ebenfalls mit einer Antenne ausgestattet ist, weitergibt. Eine computergestützte Datenbank schließt das System am anderen Ende ab. Die Datenübertragung erfolgt verschlüsselt, zu der man also ein autorisiertes Lesegerät braucht. Da die Transponder in verbraucherrelevanten Anwendungen keine eigene Energiequelle haben, funken sie nicht selbständig, sondern übertragen ihre Daten in Antwort auf ein vom Lesegerät empfangenes Signal.

Der Hauptunterschied der RFID-Technologie zu einem Strichcode (auch Barcode genannt), wie er heutzutage bei Waren gängig ist, liegt im Aufbau des EPCodes. Auf einem Strichcode werden lediglich Warengruppen erfasst. Sinngemäß speichert er die Information: ‚Dies ist eine Dose von Firma XY' – ein RFID-Chip hingegen beinhaltet: ‚Dies ist 467561654..'. Die **Kennzeichnung und Identifizierung von Einzelteilen oder Einzelprodukten** ist eine der wichtigsten Eigenschaften, die sich Industrie und Handel zunutze machen. Mit Hilfe dieser Art der Kodierung ist jeder einzelne Gegenstand identifizierbar. Über eine Kombination mit persönlichen Daten wäre er im Zweifelsfall auch genau einem Besitzer zuzuordnen.

Auch das Lesen der kodierten Daten funktioniert anders als bei einem Strichcode. Das Einscannen eines Barcodes erfolgt über den direkten Sichtkontakt, weshalb der Vorgang für alle Beteiligten unmittelbar nachvollziehbar ist. Ein RFID-Chip wird hingegen mit Hilfe einer eingebauten Antenne über Funk gelesen, was einen gewissen **räumlichen Abstand** zwischen Quelle und Lesegerät erlaubt. Dies erleichtert die Handhabung erheblich. Es bedeutet aber auch, dass das Auslesen unbemerkt passieren kann. Gegenüber dem Barcode hat RFID auch den logistischen Vorteil, **mehrere Chips in einem Schritt zu lesen**. Bei der sogenannten Pulk-Erfassung kann so beispielsweise der Inhalt einer ganzen Palette auf einmal erfasst und im Warenwirtschaftssystem abgespeichert werden. Während bisher der Lagerist die Paletten einzeln per Hand einscannen muss, reicht bei RFID das Passieren einer Schranke, die mit der entsprechenden Auslesevorrichtung auf Funkbasis ausgestattet ist. Schließlich ist für die Industrie und den Handel eine dritte Eigenschaft interessant, wenn nämlich **wiederbeschreibbare Speicherchips** eine laufende Aktualisierung nützlicher Informationen ermöglichen, so z. B. für Reparaturprozesse.

Es werden Chips mit **drei verschiedenen Funkreichweiten** eingesetzt. Bei der Produktion und bei Transportabläufen werden in der Regel die günstigsten Niederfrequenzchips mit der geringsten Reichweite eingesetzt. Am weitesten verbreitet sind Hochfrequenzetiketten, die bis zu 2 Meter weit funken können. Chips im Ultrahochfrequenzbereich mit einer Reichweite von 4 bis 5 Metern werden vom Einzelhandel als be-

sonders attraktiv angesehen, der ihre noch geringe Verbreitung forciert. Wie *Cord Bartels, Business Development Manager des RFID-Entwicklers NXP Semiconductors in Hermansburg* darlegte, lässt sich die erreichte Reichweite zentimetergenau technisch spezifizieren. Wenn der erforderliche Abstand zum Lesegerät auf wenige Zentimeter begrenzt wird, lasse sich das Auslesen der Daten als eine bewusste Handlung herstellen.

Wichtig ist für die abschließende Klärung die **Unterscheidung von passiven und aktiven Transpondern**. Verbraucher kommen in der Regel nur mit passiven Transpondern, die nicht selbstständig funken können, in Berührung. Alle Aussagen in der Veranstaltung beziehen sich deshalb nur auf diesen Typus. Aktive Transponder, die mit eigener Energiequelle und einem Sender ausgestattet sind, haben eine weitaus höhere Funkreichweite und werden zum Beispiel vom Militär zum Aufspüren von Panzern verwendet. So geht auch die RFID-Technologie insgesamt auf Forschung für militärische Anwendungen zurück. Solche aufwendigen aktiven Transponder spielen aber bei der Verbreitung von RFID in der Warenproduktion, Handel und Konsum keine Rolle.

2. Wirtschaftliche Potenziale von RFID

Vielfältige Anwendungsfelder

Die als Zukunftstechnologie bezeichneten RFID sind zwar in aller Munde, für den individuellen Verbraucher zugänglich und damit anschaulich sind sie aber noch kaum. Bislang kommen RFID-Chips in ausgewählten Anwendungsfeldern für hochwertige Güter oder dort, wo sie eine langlebige Funktion erfüllen sollen, vor. Für den Einsatz als Massen- und Wegwerfware sind ihre Materialkosten bislang noch zu hoch.

Die Funketikette im Supermarkt, welche beim Kauf eines Joghurtbechers dem Lager meldet, dass bald Nachschub in den Regalen notwendig ist, ist deshalb noch nicht in Sicht. Doch wie *Andreas Füßler von GS1 Germany GmbH*[2]*, Köln* ausführte, gehört für den Einzelhandel die Verbesserung der Inventurvorgänge zu den wichtigsten Innovationen, die RFID mit sich bringt. Während man dies für andere Bereiche noch nicht abschließend beurteilen könne, sei klar, dass das größte Potenzial der RFID-Transponder in der **Warenlogistik** liege. Es wird daher auf Hochtouren an Ersatzmaterialien für den teuren Siliziumträger der Chips geforscht. Bis zur Produktreife sollen aber noch bis zu acht Jahre vergehen.

Im Verkaufsraum ließen sich die RFID-Tags auch zum **individuellen Marketing** nutzen, indem an Servicepunkten mit einer Art Funk-Hot-Spot, der Kunde die Möglichkeit erhielte, Produktinformationen und weitere Dienstleistungen zu dem Produkt abzurufen. Als bislang einziges Unternehmen hat die Metro Group ein Demonstrations-Store am Niederrhein eingerichtet, wo einige wenige ausgewählte Produkte mit RFID-Chips bestückt werden und den Kunden den Supermarkt der Zukunft vorstellen sollen.

Vorstellungen wie die Möglichkeit einer sekundenschnellen Berechnung der Gesamtkosten eines Einkaufswagensinhalts oder gar die Kasse, die ohne Kassiererin oder Kassierer auskommt, gehören vorerst zu reinen Zukunftsentwürfen des Einzelhandels. Ob eine Transponder-Kasse tatsächlich jemals realisiert werden kann, ist aus Sicht von *Andreas Füßler* fraglich, da dies stark von der wirtschaftlichen Weiterentwicklung der Technologie abhänge.

Laut Aussage von *Cord Bartels von NXP Semiconductors, Hermansburg,* sind am weitesten Chips verbreitet, bei welchen das *Konzept der bewussten Handlung,* d. h. eine genau auf die Erfordernisse begrenzte Reichweite des Chips umgesetzt wurde. Dies betreffe zum Beispiel den öffentlichen Personennahverkehr in einigen großen Städten weltweit, wo RFID die Zugangskontrollen zu Bahnsteigen etc. regelt.

Dem Konzept der bewussten Handlung steht die *automatische Erfassung* gegenüber. Hier kommen RFID-Chips in einigen Anwendungsfeldern zum Einsatz, die im Hinblick auf den Schutz von Persönlichkeitsrechten oder Datensicherheit als unbedenklich gelten können. Solche Einsatzbereiche von RFID sind z. B. sehr kleine Chips, die Geldscheine extrem fälschungssicher machen sollen, wie sie zurzeit in Japan entwickelt werden; der seit 1990 bei weltweiten Laufveranstaltungen eingesetzte *Championchip* zur genauen Unterscheidung der Laufzeiten einzelner Sportler und Sportlerinnen oder auch die in einzelnen Bibliotheken praktizierte Ausstattung von Büchern mit Funkchips, um den Ausleihvorgang und das Auffinden der Bücher zu erleichtern. Mit vergleichbaren Interessen rüstet der Frankfurter Flughafen zurzeit die Gepäckaufnahme auf Funk-

2 GS1 Germany GmbH kümmert sich um eine weltweit standardisierte Vergabe des European Product Code. Das Unternehmen vergibt die EPC-Nummern und verwaltet den Datenbestand mit den ihnen zugewiesenen Produkten.

chips um. Solche Innovationen vor allem im effizienterem **Management von komplexen Prozessen** und in der **Warenverfolgung** sind insbesondere für den Handel interessant und entfalten dort in der Logistik ihr wirtschaftliches Potenzial.

Im privatwirtschaftlichen Tätigkeitsfeld nehmen die Chips die größte Rolle bei der **Steuerung der Produktionsabläufe** in Werkhallen und bei der **Rückverfolgung von transportierten Gütern** ein. So werden in einigen Automobilwerken Fahrzeugteile mit Funketiketten versehen, die an Maschinen Befehle für die benötigte Art der Montierung oder den Farbauftrag abgeben können. VW transportiert zudem beispielsweise Karosserieteile in Behältern mit Funkchips. Nach eigenen Angaben des Unternehmens lässt sich der Verlust der Transportware um ein Drittel reduzieren.

Schließlich ist der Bereich von **Zugangskontrollen** ein boomendes Feld für RFID. Darunter kann man sich sowohl den Autoschlüssel, mit dessen Hilfe man die Wegfahrsperre löst, vorstellen, als auch beispielsweise Chips in Clubausweisen oder Skipässen, die an Schranken die Zutrittsberechtigung des Inhabers funken.

Die Funketiketten können in jeder Art von Gebrauchsgegenständen untergebracht werden, sogar in Papier. Anwendungen aus der Landwirtschaft zur Kennzeichnung von Rindvieh oder auch zum Aufspüren von entlaufenen Haustieren zeigen, dass sie auch zur Implantation unter die Haut geeignet sind.

Zur erhöhten öffentlichen Aufmerksamkeit für die Funktechnologie hat die Fußballweltmeisterschaft beigetragen, als die Eintrittskarten für die Spiele mit solchen Chips ausgestattet wurden, um jene fälschungssicher zu machen. Neben Bedenken zum Datenschutz, die von Verbraucherschützern und Nichtregierungsorganisationen vorgebracht wurden, hat sich bei diesem Ernstfall für die Technologie im großem Maßstab auch schnell die Grenze der Produktreife gezeigt. Die Etiketten haben bei der Kontrolle öfter versagt, so dass es ein Streitpunkt bleibt, ob RFID hier ihren Zweck, mehr Sicherheit für die Veranstalter und für die Zuschauer zu gewährleisten, erfüllt hat.

Im prominentesten Beispiel für RFID-Technologie, dem neuen Reisepass, dient sie der **Sicherung von hoheitlichen Aufgaben**. Der deutsche Reisepass enthält seit November 2005 einen RFID-Chip, auf dem die üblichen persönlichen Daten sowie das biometrisch genormte Photo digital gespeichert werden. Das Verfahren wurde noch unter dem vormaligen Innenminister Schily eingeführt, als das US-Außenministerium angekündigt hatte, zukünftig Einreisegenehmigungen eventuell nur auf der Basis von biometrischen Bestimmungsmerkmalen zu gewährleisten, die auf einem Chip im Pass gespeichert werden. Noch im Laufe des Jahres 2007 soll auf allen neu beantragten Pässen auch der Fingerabdruck gespeichert werden. Das Innenministerium versprach sich von der kostspieligen Innovation fälschungssichere Pässe, die insbesondere vor der Einreise von Terroristen schützen sollen und wegen treffsicherer Kontrollmerkmale die Abfertigung an Grenzkontrollen beschleunigen sollten.

Beispiel ÖPNV

Nils Zeino-Mahmalat vom Kompetenz Center Elektronisches Fahrgeld Management (KCESP), Verkehrsverbund Rhein-Ruhr, Gelsenkirchen stellte die Anwendungsmöglichkeit im Öffentlichen Personennahverkehr vor. Im Verkehrsverbund Rhein-Ruhr, Rhein-Sieg und Niederrhein werde eine RFID-Karte als Monatskarte verwendet. Bislang wird darauf nur die Zeitfahrkarte gespeichert, mit dem Ziel, Fälschungen zu vermeiden bzw. verloren gegangene Karten sperren zu lassen. Zukünftig sollen aber mehr Daten gesammelt und gespeichert werden, wobei es sich nicht um persönliche Verkehrsdaten handeln soll. Im Fokus stehe vielmehr die **Ermittlung der Linienbelastung**, d. h. die Ermittlung dessen, auf welchen Strecken zu welcher Uhrzeit wie viele Passagiere die Fahrzeuge nutzen. Bislang gebe es dazu nur ungenaue Schätzungen, die auf Stichprobenzählungen beruhen, welche anschließend auf den Gesamtverkehr hochgerechnet werden. Eine genauere Analyse von Fahrgastströmen würde hingegen die Planung des Angebots von Bussen und Bahnen und dabei insbesondere die Umsteigebeziehungen erheblich erleichtern.

Nach Angaben von *Zeino-Mahmalat* wird ein solches Verfahren zurzeit nur im öffentlichen Nahverkehr des Kreises Schwäbisch-Hall erprobt. Hier erhält man als häufiger Gelegenheitsfahrer eine Smartcard, mit der man sich beim Betreten eines Fahrzeugs anmeldet. Wenn man die Karte nah an ein Lesegerät hält, wird elektronisch der Beginn einer Fahrt aufgezeichnet. Die Datenübertragung erfolgt in jedem Fall verschlüsselt über ein Sicherheitsmodul, da der Verkehrsverbund daran interessiert ist, dass die registrierten Fahrscheine fälschungssicher bleiben. Beim Verlassen des Fahrzeugs meldet sich der Kunde/die Kundin wieder ab. Ähnlich wie bei der Telefonrechnung bekommt man bei diesem Verfahren am Monatsende eine Abrechnung über die verbrauchten „Fahrscheine". In Zukunft lässt sich nach Vorstellung des Verkehrsverbundes Rhein-Ruhr automatisch die für den Kunden beste Berechnungsart kalkulieren und je nach Art der Nutzung könnten Fahrgästen **Vielfahrerrabatte** oder auch optionsweise eine **Abrechnung nach gefahrenen Kilometern** statt nach Anzahl der Einzelfahrten angeboten werden. Außer den Vorteilen, die dabei für die Verbraucher entstehen, erhält das Verkehrsunternehmen parallel Daten über Fahrgastströme. Zeino-Mahmalat berichtete, dass es sich beim Pilotprojekt in Schwäbisch-Hall gezeigt habe, dass die Fahrgäste in vielen Bereichen andere Wege nehmen als von den Verkehrsplanern vorgesehen.

Für den Schutz gegen die Einsicht von persönlichen Daten durch das Unternehmen werden laut Zeino-Mahmalat technische Sperren eingebaut. In ähnlicher Weise werde dies heute auch bei Telefonunternehmen gehandhabt.

Vorteile von RFID für Verbraucher

Manfred Zöllmer, Sprecher des Gesprächskreises „Verbraucherpolitik", Mitglied der SPD-Bundestagsfraktion und Stellvertretender Vorsitzender des Bundestagsausschusses für Ernährung, Landwirtschaft und Verbraucherschutz sieht als Vorteile von RFID vor allem deutlich verbesserte Möglichkeiten der Verbraucherinformation. Diese sei das A und O einer jeden guten Verbraucherpolitik. Beim Einkauf ließen sich mittels der Technik gezielte Zusatzinformationen über Bildschirme an die Konsumenten weitergeben. So zum Beispiel spezielle Informationen für Diabetiker oder Allergiker. Gegenüber herkömmlichen Verfahren, solche Informationen vor allem auf dem Packungstext abzudrucken, ließe sich so ein Overkill an Informationen vermeiden. Denn jede Verbraucherin und jeder Verbraucher könnte sich die ihn interessierenden Angaben auswählen. Am weiteren Horizont stehe ein individualisiertes Marketing.

Verbraucherschützer weisen auf die Möglichkeit der Überprüfung der Frische von Produkten (Mindesthaltbarkeitsdatum) hin. Auch die Echtheit von z. B. Medikamenten würde sich mit Funketiketten eindeutig identifizieren lassen. Vertreter der Industrie verwiesen zudem auf Vorteile, die aus schnelleren und effizienteren Abläufen bei der Warenherstellung und beim Vertrieb resultieren würden. So würde den Verbrauchern zugute kommen, dass die Frische von Produkten verbessert und die Kosten für die Logistik günstiger würden.

Zukunftschancen aus Sicht der Unternehmen

Die Industrie sieht in der RFID-Technologie Verwertungschancen vor allem bei der Realisierung von Einsparpotenzialen in der Prozesssteuerung und Lagerhaltung und bei der Entwicklung neuartiger, intelligenter Produkte. *Manfred Zöllmer, MdB* verwies darauf, dass die größte Bedeutung von RFID in der Logistik läge: „Hier sind wir technisch gesehen auf dem Weg zum Internet der Dinge, zu einer Überall-Kommunikation durch Computer. Die Produkte können dann untereinander kommunizieren, was sehr viel Kosten sparen hilft".

Nach einer Zusammenstellung von Deutsche Bank Research zum Thema RFID[3] zeigen Anwendungen und Vorfeldanalysen aus unterschied-

3 Heng, Stefan: RFID-Funkchips. Zukunftstechnologie in aller Munde. Deutsche Bank Research, economics 55. 24. Januar 2006.

lichen Branchen, dass sich Kosten im Einzelhandel vor allem durch vermiedenes Fehlen von nachgefragten Waren im Lager oder im Supermarktregal einsparen lassen. Das kann fast die halbe Ersparnis ausmachen. Die andere Hälfte geht auf effizienter organisierte Abläufe sowie verminderten Diebstahl zurück.

Für den Absatzmarkt der RFID-Technologie prognostiziert das kommerzielle deutsche Marktforschungsinstitut Soreon Research Investitionen im Handel in der EU-15 in Höhe von 2,5 Mrd. Euro im Jahre 2008. In Deutschland könne dieser Absatz bei ca. einer halben Milliarde Euro liegen. Dabei geht man davon aus, dass nicht die RFID-Hardware, also der Funkchip, sondern die Software zur Datenverarbeitung sowie die im Umfeld angesiedelten Dienstleistungen der wichtigste Stützpfeiler des Wachstums sein werden.

3. Technische und ökologische Herausforderungen

Nach einer Einschätzung von acatech, dem Konvent der Technikwissenschaften in der Union der Akademien, stellt der **Datenschutz** das größte Hemmnis für den massenhaften Einsatz von RFID dar. Daneben gibt es aber für eine breite Anwendung von RFID noch vielfältige **technische Hürden**:

- Sie beginnen bei der Beanspruchung oder **Lebensdauer der Chips**, eine Frage, wie sie sich z. B. bereits beim neuen Biometriepass stellt.
- Für die Anwendung in der Logistik besteht das Problem, dass sich zu viele Transponder im Lesebereich befinden können. Außerdem kommt es zu **Störeinflüssen der Funkübertragung** durch Reflexionen an Metall oder Wasser, was sich negativ auf das Leseverhalten der Etiketten mit einer Fehlerquote von 25 Prozent auswirkt.
- Erst vor wenigen Monaten hat der niederländische Wissenschaftler Andrew Tanenbaum bewusst gemacht, dass die Tatsache, dass man es hier mit Chips zu tun hat, auch die Nachteile von digitaler Datenübertragung mit sich bringt. Er zeigte, dass eine versehentliche oder gezielte **Übertragung von speziellen Viren** möglich ist[4]. Auch für die anwendenden Unternehmen ist ein immenser Schaden vorstellbar, wenn beispielsweise über Lesegeräte an Kassen der Supermarktrechner infiziert werden könnte.
- Auch *Andreas Füßler von GS1 Germany* räumte ein, dass ein Angriff durch Computerviren theoretisch auch in diesem Bereich denkbar sei. Allerdings bewirke die im Vergleich zum sonst üblichen Datenvolumen die kurze, überschneidungsfreie Nummer des EPC, dass sich Virenszenarien fast ausschließen ließen. Demgegenüber betonte die Computerexpertin *Rena Tangens von FoeBuD, Verein zur Förderung des öffentlich bewegten und unbewegten Datenverkehrs*[5]*, Bielefeld,* dass die RFID-Technologie gerade, da sie sich noch in Entwicklung befinde, viele Angriffsfelder biete. So seien Verschlüsselungsmöglichkeiten nicht vollständig sicher, und es sei theoretisch vorstellbar, dass der Lagerbestand einer Firma über Chipviren komplett gelöscht werden könne.
- Völlig ungeklärt ist bislang die Frage, wie man ausreichend Frequenzbereiche gewähren kann, in welchen RFID-Etiketten funken sollen. Bislang beschränkt sich die Erlaubnis – wenngleich zunächst aufgrund der noch geringen Nachfrage – auf einige wenige Frequenzen, die bei mehreren, sich nebeneinander befindenden Lesegeräten schnell ausgelastet sind. Hinzu kommen Störungen bei der Signalübertragung in der Nähe von anderen elektronischen Geräten oder Funkgeräten. Die **Standardisierung des Frequenzbereichs** für eine weitgehend störungsfreie Übertragung der RFID-Funksignale im Abstand zu anderen üblichen Frequenzen gehört zu den grundlegenden Herausforderungen für die massenhafte Verbreitung der Funktechnologie. Hierbei handelt es sich um übergreifende hoheitliche Aufgaben, deren funktionierende Regelung Unternehmen überhaupt erst in die Position versetzt, das Geschäftsfeld der RFID-Technologie erfolgreich zu besetzen.
- Letztlich muss die mittlerweile zum Standard gehörende Anforderung der Einhaltung von bestimmten **ökologischen Kriterien** in die Reihe der technischen Herausforderungen mit aufgenommen werden. Wie für alle Chips gilt

4 Vgl. Wodka mit Computervirus, Süddeutsche Zeitung 1./2. April 2006.

5 Der 1987 gegründete Verein beschäftigt sich nach Darstellung von Rena Tangens mit Gefahren, die bestimmte Technologien für die Gesellschaft darstellen, und bietet Alternativen dazu an. Viele der Mitglieder arbeiten selbst bei der Entwicklung von Technologien, weshalb sich der Verein explizit als technikoffen versteht.

auch für RFID-Chips, dass zur ihrer Herstellung kein Blei mehr verwendet werden darf. Insbesondere das bislang in den Antennen der Transponder verwendete Kupfer macht aber die Entsorgung der Etiketten nach wie vor schwierig und teuer.

- Ähnlich wie beim Mobilfunk wird man auch auf die Umweltbelastung durch **Strahlung** aufmerksam. Dadurch, dass bei den im Rahmen der Veranstaltung diskutierten Anwendungen nicht die Etiketten, sondern die Lesegeräte funken, muss nicht mit Problemen in Privathaushalten gerechnet werden. Doch wie man mit erhöhter Dichte an Funksignalen in beispielsweise Lagerhallen umgehen können soll, gehört zu den noch kaum bearbeiteten Fragen. Auch die Untersuchung der Auswirkungen der Funkfrequenzen von RFID gestaltet sich ähnlich schwierig wie beim Mobilfunk, doch gibt es in Europa als Reaktion auf Verbraucherängste vor Elektrosmog zumindest eine Leistungsbeschränkung von RFID-Systemen im Hochfrequenzbereich auf 0,5 Watt. In den USA beträgt sie zum Vergleich 2 Watt. Da die Funkleistung direkt mit der Reichweite der Strahlen zusammenhängt, schränkt die regulatorische Intervention gleichzeitig die technische Ausbeutung und die Gewinnspanne, die mit RFID erzielt werden kann, ein.
- Am anderen Ende der finanziellen Anforderungen stehen schließlich die **Herstellungskosten** für die Chips, die bislang regulär aus Silizium bestehen. Das teure Metall soll in ferner Zukunft – die RFID-Branche geht von ca. 15 Jahren aus – durch hauchdünne Polymerschichten (Kunststoff) ersetzt werden. Die diesbezügliche Forschung hält dann auch ein Recycling der Etiketten für möglich.

Eine Beschleunigung für die Weiterentwicklung der Technologie, die auf die genannten technischen Probleme reagieren würde, versprechen sich Fachleute von branchenbezogenen Anwendungs- und international einheitlichen Technologiestandards. Dazu braucht es allerdings Anreize in Form von erwartbarer potenzieller Ausweitung ihres Einsatzes und damit eine weit gehende **Akzeptanz der Technologie**.

4. Datenbanken wecken Begehrlichkeiten – die Risiken von RFID

Kriterien für Verbraucherfreundlichkeit

Cord Bartels von NXP Semiconductors in Hamburg betonte, dass praktisch jede komplexe technische Lösung Chancen wie Risiken in sich berge. Den Referenten aus Politik, Wirtschaft und Zivilgesellschaft dienten als Maßstab für die jeweilige Verbraucherfreundlichkeit oder Verbrauchergefährdung durch RFID-Anwendungen unterschiedliche Ansätze, die grob in zwei Argumentationslinien unterschieden werden können:

Wahlfreiheit mit Hilfe informationeller Chancengleichheit

Zentrales Thema der Verbraucherpolitik ist nach Ansicht von *Manfred Zöllmer, MdB* die Forderung nach einem gleichberechtigten Verhältnis zwischen der Nachfrage- und der Angebotsseite. Zöllmer sieht beim Umgang mit Daten ähnliche Grundsätze wirken wie sie auf dem Gütermarkt vorherrschen. Danach sollten Hersteller und Anwender von RFID-Lösungen zunächst über die gleichen Informationen zu Produkten und Dienstleistungen verfügen. Aus Kundensicht würden **Transparenz über die Datenaufnahme und Datenverarbeitung** bei einzelnen Anwendungen entscheidend sein, ob sie ihre Daten gegen versprochene Vorteile eintauschen wollen. Kunden könnten im Einzelhandel also beispielsweise abwägen, ob individuell abrufbare Produktinformationen und eine schnellere Abwicklung an der Kasse es ihnen wert sind, die Einführung von Funketiketten auf Lebensmittelverpackungen zu unterstützen und Gefahr zu laufen, dass ihre Einkaufsmuster rückverfolgt werden können. Sie könnten auch bewusst einfordern oder eben darauf verzichten, dass die Chips beim Verlassen des Ladens verlässlich abgeschaltet werden. Zugleich könnten Unternehmen im Rückbezug erfahren, von welchen Wünschen und Interessen sich (potenzielle) Kunden leiten lassen und die RFID-Anwendungen entsprechend nachbessern. Die Hauptforderung Zöllmers war vor diesem Hintergrund, dafür zu sorgen, dass Verbrauchern **möglichst viele Informationen** zur Verfügung gestellt werden.

Selbstbestimmung durch Einhaltung rechtsstaatlicher Prinzipien

Dem Ansatz, der den Verbraucher als Kunden mit Wahlmöglichkeiten begreift, steht eine Perspektive gegenüber, die den Verbraucher als Bürger mit Rechtsansprüchen definiert. Nach dem Standpunkt einiger Vertreter der Verbraucherseite steht nicht der Austausch von Daten zu fairen oder unfairen Bedingungen im Fokus, sondern der Raum bürgerlicher Freiheitsrechte, der durch unterschiedliche gesellschaftliche Gruppen und ihre jeweiligen Interessen begrenzt wird und daher umkämpft ist. Letztlich kommt es darauf an, wie sich die Gesellschaft als Ganze darüber verständigt – d. h. unter Einbezug von Wirtschaft, Verbrauchern und Politik – wem sie welche Freiheitsrechte auf Kosten anderer Gruppen zubilligen will. Dies schließt auch das Verhältnis von Freiheit und staatlicher Kontrolle gegenüber Bürgern und Bürgerinnen sowie Unternehmen ein. In letzter Instanz werden Freiheitsrechte in Gesetzesform, d.h. staatlich abgesichert.

So stellt nach einer Einschätzung von acatech, dem Konvent der Technikwissenschaften in der Union der Akademien, die Einhaltung des **Datenschutzes** das größte Hemmnis für den massenhaften Einsatz von RFID dar. Unter Datenschutz ist der Schutz von Persönlichkeitsrechten zu verstehen, der verhindern soll, dass Menschen, Institutionen oder Firmen durch das Wissen und die Informationen, die sie ansammeln, Zugriff auf andere haben. Die Datenhoheit der Einzelnen als **Grundrecht auf informationelle**

Selbstbestimmung soll ihnen erlauben, selbst zu bestimmen, mit wem sie persönliche Daten teilen.

Grundzüge des Datenschutzes

Rena Tangens von FoeBud verdeutlichte, dass Datenschutz insbesondere für Handlungsmöglichkeiten in der Zukunft relevant sei. Denn je nachdem, ob man maßgeblich nach der Gegenwärtigkeit seiner Handlungen oder in erster Linie nach der Vergangenheit beurteilt werde, könnten Freiräume geöffnet oder geschlossen werden. Ein Beispiel aus dem Alltag ist die Zeitspanne, die für die Ermittlung der persönlichen Bonität durch Banken und Versicherungen herangezogen wird.

Für den *Vertreter der Verbraucherzentrale Bundesverband, Christian Thorun* ist das Grundrecht der informationellen Selbstbestimmung wichtig, weil selbstbestimmtes Handeln der Einzelnen nur möglich sei, wenn diese sich nicht permanent öffentlich zur Schau stellen müssten. Jede öffentliche Preisgabe von Daten einer Person erhöht aber die Möglichkeit, dass Dritte Handlungsschritte dieser Person ohne deren Wissen nachvollziehen können. Der **Rückzug in die eigene Privatsphäre** sei deshalb ein Wesensmerkmal einer freiheitlichen Gesellschaft.

Dafür müssten folgende wichtigste Prinzipien des Datenschutzes verfolgt werden:

1. Das Prinzip der **Datensparsamkeit** geht von dem Grundsatz aus, dass der beste Schutz vor Datenmissbrauch die Prävention darstellt. Werden nur minimal Daten herausgegeben, gespeichert und verarbeitet, wird das Missbrauchspotential deutlich verringert. Befinden sich personenbezogene Daten erst einmal im öffentlichen Raum, ist es oftmals schwer zu kontrollieren, ob mit ihnen auch korrekt umgegangen wird. Daher sollten nur so wenige Daten wie nötig erhoben, gespeichert und verarbeitet werden.
2. Das **Transparenzgebot** soll gewährleisten, dass der Bürger über den Umfang, die Art und den Zweck der Datenerfassung informiert ist: Er soll wissen, wer welche seiner Daten zu welchem Zweck erhebt und verarbeitet.
3. Die **freiwillige Einwilligung** soll gewährleisten, dass der Bürger die Souveränität über seine Daten behält. Personenbezogene Daten über ihn sollen nur dann verarbeitet werden, wenn dies durch eine Rechtsvorschrift ausdrücklich erlaubt oder angeordnet wird, oder wenn der Bürger selbst hierzu im Wissen der Konsequenzen und ohne Zwang einwilligt.

Risiken der Technologie: Konsummuster rückverfolgen

Das Besondere an der RFID-Technologie besteht darin, dass die Kommunikation zwischen RFID-Chips und RFID-Lesegerät kontaktlos und prinzipiell unsichtbar und damit für den Verbraucher nicht transparent erfolgt. Das bedeutet, dass die RFID-Chips unbemerkt von Unbefugten ausgelesen werden könnten.

Konkret liegt das verbraucherschutzrechtliche Problem bei Funketiketten nach Darstellung von *Manfred Zöllmer, MdB* hauptsächlich in einer möglichen **Vernetzung** zwischen Produktcodes auf der einen Seite und großen Datenbanken auf der anderen Seite. Dies treffe insbesondere zu, wenn die **Produktcodes zusammen mit personenbezogenen Daten** wie sie beispielsweise beim bargeldlosen Zahlungsverkehr in den Computer eingespeist werden, erhoben werden. So sei das Zusammenbringen von Personendaten und Konsumverhalten zumindest theoretisch herstellbar, womit Verhaltensweisen von Verbrauchern erfasst und als komplexe Konsummuster ausgewertet werden könnten. Hier könne sich unversehens ein neues und lukratives Geschäftsfeld für Dienstleistungen öffnen, an welchen von Seiten der Werbeindustrie großes Interesse vorstellbar sei.

Nach Ansicht des *Verbraucherschützers Christian Thorun* wird zudem der massenhafte Einsatz der RFID-Technologie dazu führen, dass es für Verbraucher unüberschaubar wird, wer auf ihre Daten zugreift. Dadurch liefen Verbraucher Gefahr, die Hoheit über die eigenen Daten zu verlieren. Zwar würden Einzelprodukte heute aus Kostengründen noch nicht mit RFID-Chips ausgestattet, dies sei aber nur eine Frage der Zeit. Wohin die Entwicklung gehen kann, zeige ein Projekt aus Dubai. Dort soll ein großes Shopping-Center

mit einem Kundenmanagement-System ausgestattet werden, das auf RFID-Technologie beruht. Wenn Kunden das Center betreten, sollen sie anhand ihrer Kundenkarte, die mit einem RFID-Chip versehen sein wird, erkannt werden. Daraufhin werden ihnen aktuelle auf sie zugeschnittene Sonderangebote präsentiert und Werbung angeboten werden.

Thorun sieht eine enorme Gefahr, wenn diese Praxis auch in Deutschland Einzug halten sollte. Denn die eindeutige Identifizierung eines Kunden in Verbindung mit umfangreichen Datenbanken zum Einkaufsverhalten könnten nicht nur dazu genutzt werden, Verbrauchern gezielt Werbung und Angebote zukommen zu lassen, sondern auch dazu, die Preise dynamisch an die Verbraucher anzupassen. Ein **dynamisiertes Preissystem** führe aber dazu, dass Menschen aufgrund von oft nicht nachvollziehbaren Kriterien diskriminiert werden.

Rena Tangens von FoeBuD wie auch einige Teilnehmer aus dem Publikum finden die Vorstellung vom gläsernen Kunden an sich sehr bedenklich. Dies aber würde Realität, wenn ein Händler, sobald ein Kunde wiederholt sein Geschäft erneut betritt, dem Kunden ansehen können wird, welche Kleidungsstücke er gerade trägt und wann er diese gekauft hat.

Der Verband FoeBuD sieht auch im Geschäftsgebaren von Unternehmen in Deutschland Anzeichen dafür, dass diese Technologie mit sehr großer öffentlicher Aufmerksamkeit betrachtet werden muss. Auf eine Initiative des Vereins geht die Verleihung des Big Brother Awards zurück. 2003 erhielt die Einzelhandelskette *Metro* den Preis für ihren Future Store in Rheinberg bei Duisburg, zunächst präventiv zur Anregung einer Diskussion über eine Technologie, die die Gefahr der Beschneidung individueller Freiheitsrechte in sich birgt. Erst nach der Nominierung habe sich herausgestellt, so *Regina Tangens,* dass Missbrauch tatsächlich schon stattgefunden haben soll, indem neben den vier als RFID-Träger ausgewiesenen Produkten im Sortiment, auch die Metro-Kundenkarte einen nicht deklarierten Chip enthielt, mit dem die Kunden ahnungslos herumliefen. Metro habe dabei auch im Nachgang den Dialog mit Verbraucherschützern verweigert.

Bewegungsprofile erstellen

Über den Bereich des Konsumentenschutzes hinaus gehen Szenarien, die die Möglichkeit von RFID betrachten, Bewegungsprofile von Menschen nachzuvollziehen. Solche Bewegungsmuster ließen sich sowohl für private wie für hoheitliche Zwecke nutzen.

Ein reales Beispiel ist in diesem Zusammenhang die auf der Veranstaltung mehrfach angesprochene Praxis der Supermarktkette *Tesco* in Großbritannien gegenüber ihren Angestellten. *Tesco* lässt ihre Angestellten RFID-Chips in ihrer Arbeitskleidung tragen, mit welchen ihr Aufenthaltsort überprüft werden kann. Ursprünglich ist dies mit der Begründung nach besserer Koordination des Einsatzes der Mitarbeiter auf großen Verkaufsflächen eingeführt worden. Bekannt geworden ist dieser Fall aber dadurch, dass auch der Verbleib in den Pausenräumen und auf Toiletten auf diese Weise überwacht wurde und in Form von Abmahnungen Folgen für das Arbeitsverhältnis einzelner Mitarbeiter nach sich gezogen hat.

Rena Tangens von FoeBuD führte ein negatives Zukunftsszenario an, das hoheitliche Interessen am Gebrauch der von RFID zur Verfügung gestellten Daten aufzeigen sollte. Mit solchen Szenarien arbeitet nach Angabe von *Jürgen Karwelat* auch das Verbraucherschutzministerium des Bundes:

> „Marion Z. erhält einen Bußgeldbescheid in Höhe von 10 Euro über eine ordnungswidrige Müllentsorgung im Teich des Stadtparks. Marion Z. ist sich sicher, dass ihr ein solches Verhalten nie in den Sinn kommen würde. Es stellt sich heraus, dass der Zusammenhang mit Marion Z. sich dadurch ergeben hat, dass sie das Riegelpapier an einer Supermarktkasse unter Nutzen einer Karte mit persönlichen Daten gekauft hat. Zwar ist sie sich sicher, dass sie Schokoriegel an ein Kind verschenkt hat, aber der Chip an der Verpackung hat sie als Käuferin dieses einen besagten Exemplars identifiziert. So muss sie zähneknirschend das Bußgeld zahlen.“

Für heutige Verhältnisse erscheint der dem Beispiel zugrunde liegende Zugang zu privatwirtschaftlichen Datenbanken durch Behörden in diesem Ausmaß eher unrealistisch und rechtlich nicht möglich. Den Charakter von reinem Science-Fiction verliert dieses Beispiel aber, wenn man sich die in den letzten Jahren zunehmend geschaffenen Ausnahmetatbestände vergegenwärtigt – so insbesondere im Bereich der Vorratsdatenspeicherung und der Auskunftspflicht über persönliche Verbindungsdaten, die Telefongesellschaften gegenüber der Polizei haben. Ein aktuelles Beispiel für eine der ursprünglichen Verwendung gegenüber zweckfremde Nutzung von Daten ist die vom ehemaligen Innenminister Otto Schily veranlasste Kontrolle von LKW-Mautdaten zur Verbrechensaufklärung. Dieser Vorgang ist vom Bundesdatenschutzbeauftragten Schaar scharf kritisiert worden[6].

Rena Tangens machte schließlich auf eine Gefahr für Grundrechte wie freie Meinungsäußerung oder Versammlungsfreiheit, die mit wachsenden Kontrollmöglichkeiten der Alltagspraktiken von Menschen einhergingen, aufmerksam: „Wenn Menschen gemerkt haben, dass Informationen über sie analysiert werden, werden sie dazu neigen, sich zukünftig so zu verhalten, dass es für sie vorteilhaft ausgewertet wird. Das wird unser Verhalten beeinflussen. Man geht nicht mehr zu Bürgerversammlungen, weil klar ist, dass die Teilnehmerdaten gespeichert werden und mir das dann vielleicht in fünf Jahren Probleme im Beruf bereiten wird".

Zwischenfazit: auch personenbeziehbare Daten diskutieren

RFID kann, wie andere Technologien auch, als eine Möglichkeit für die Nutzung von Dateninformationen gegen Individuen betrachtet werden. *Rena Tangens* und *Christian Thorun* führten aus, dass wenn Daten erst einmal generiert worden sind, sie für vieles verwendet werden könnten. Ihr Tenor lautete: Datenbanken wecken Begehrlichkeiten. Digital vorliegende Daten verführten dazu, sie zu speichern und zu verarbeiten. Wenn die Daten einmal generiert sind, sei ihre anderweitige Nutzung nur mit großem Aufwand und permanenter Aufmerksamkeit des Einzelnen und der Öffentlichkeit abzuwenden. So bestehe die Gefahr, dass ein kurzfristiger ökonomischer Vorteil und die Steigerung der Qualität von Konsumverhalten mittelfristig demokratie- und grundrechtsgefährdende Nebeneffekte entwickeln können. Deshalb plädierten beide dafür, möglichst wenige Daten zu erheben. Auf diese Weise lasse sich der beste Datenschutz herstellen. *Thorun* legte zudem Wert darauf, vor diesem Hintergrund nicht nur personenbezogene Daten im Fokus zu haben, sondern auch über Verfahren zum Umgang mit „nur" **personen*beziehbaren* Daten** nachzudenken.

Bei aller notwendigen Sensibilisierung gegenüber potenzieller Gefährdung der persönlichen Sphäre bedarf es der Klarstellung, dass nicht alle RFID-Anwendungen diese tangieren können. Bei den sogenannten *unverbundenen geschlossenen Systemen* wie im genannten Beispiel der Produktionssteuerung in Automobilwerken ist eine Zuordnung einer Produktkennzeichnung zu einem einzelnen Käufer nicht realistisch.

Datensicherheit technisch unterlaufen

Aus Sicht von Verbrauchern und Datenschützern sind im Hinblick auf mit technischer Datensicherheit verbundene Fragestellungen zunächst solche Anwendungen als kritisch anzusehen, die **personenbezogene Daten** speichern, wie z. B. in Mitgliedsausweisen aller Art. Ohne spezielle Absicherungen besteht die Gefahr, dass der Chip unbemerkt abgefragt werden kann, zumal auch die Lesegeräte in unverdächtige Gebrauchsgegenstände als Schranke eingebaut werden können.

6 Vgl. Mit Mautdaten auf Gangsterjagd, Süddeutsche Zeitung, 5./6. August 2006; Fehlende Transparenz. Interview mit Peter Schaar. In: Move. September 2006

Auch mit Blick auf die u. U. problematische Ermittlung von Konsum- und Bewegungsprofilen ist denkbar, dass es interessierte Personen gibt, die auf **nicht legalem Wege** an gespeicherte Daten gelangen wollen. Bei der Veranstaltung wurde zum Beispiel darüber berichtet, dass die Funk-Kommunikation zwischen RFID-Scanner und Chip aus einer gewissen Entfernung mit handelsüblichem Amateurfunk-Equipment abgehört werden kann.

Von Vertretern der Wirtschaft wurde gegenüber dieser Art von Befürchtungen angeführt, dass die Daten verschlüsselt übertragen werden und nur eine autorisierte Datenbank im Hintergrund es erlauben würde, empfangene Daten lesen zu können. Wie auch beispielsweise bei der vom Bundesgesundheitsministerium lancierten elektronischen Gesundheitskarte seien die Verschlüsselungsverfahren mittlerweile auf einem hohen Niveau, so *Andreas Füßler von GS1 Germany GmbH, Köln.*

Hierauf führten *Rena Tangens, FoeBuD* und weitere Diskussionsteilnehmer aus dem Publikum an, dass **Verschlüsselung** eine Frage des Geldes sei, und gerade die Anwendungen im Einzelhandel extrem preissensibel seien. Es stünde also zu befürchten, dass es zwar für unternehmensinterne Prozesse gute Sicherungstechniken geben wird, dort aber, wo es um Verbraucherinteressen geht, die Kosten gescheut werden könnten.

Datensicherheit meint im Unterschied zum Datenschutz die Integrität von Daten. Sie soll verhindern, dass Daten verloren gehen oder zerstört werden und sie soll sicher stellen, dass Daten abgreif- und abhörsicher übertragen werden. Hier sind also Fragen von IT-Sicherheit betroffen.

Das Vertrauen in die Sicherheit von Verschlüsselungstechniken ist in der Öffentlichkeit mit der Einführung des elektronischen Reisepasses, der auch mit einem RFID-Chip ausgestattet ist, in Zweifel geraten. Hier hat sich die Dimension der Datensicherheit als ein hochproblematisches Feld erwiesen. So soll es nur zwei Wochen nach der Einführung des Passes Chipspezialisten gelungen sein, die Zugangssperre eines Passchips zu knacken und die Daten zu kopieren[7]. Nach Angaben der Computerexperten gelang ihnen die Überwindung der Sicherung gerade mit Hilfe des Verschlüsselungscodes. Dieser bestehe aus der Passnummer, Geburtsdatum und dem Ablaufdatum. Solche Daten ließen sich in Datenbanken vieler Unternehmen aus dem Dienstleistungsbereich finden, die diese Angaben bei ihren Kunden bei ihnen abfragen, so z. B. von Fluggesellschaften, Autovermietungen, Hotels[8].

Daten zentral zugänglich machen

Bei den genannten Beispielen handelt es sich um die Anlage neuer Datenbanken und die Gewinnung von Informationen, die man zuvor nicht sammeln konnte. Ein wichtiger Teil der Datenschutzproblematik, die im Zusammenhang mit RFID diskutiert wird, betrifft auch Bereiche, in welchen Daten bereits längst gesammelt werden, durch RFID-Technik aber die Einrichtung von **zentraler Speicherung der Daten** als logische Effizienzkonsequenz erscheint.

Ein sensibles Feld ist zum Beispiel die Erfassung von Patientendaten im Krankenhaus. Im Klinikum Saarbrücken wird seit April 2005 der Ernstfall für einen flächendeckenden Einsatz von RFID-Tags für die Kontrolle verschiedener Abläufe, in deren Mittelpunkt der Patient steht, geprobt[9]. Hierzu tragen alle Patienten ein RFID-Armband mit individueller Nummer, unter der in

7 Vgl. Bericht in Buisinessnews vom 8. August 2006.
8 Vgl. Steffen Kraft: Der Fehlpass. In: Tagesspiegel vom 10. Februar 2007.
9 Vgl. Franke, Janet: Datenfunk am Krankenbett. In: move. Mai 2006.

einer Datenbank Angaben über Name, Alter, Gewicht und Laborwerte der Patienten gespeichert sind. Mit Hilfe mobiler PCs erhalten Ärzte so während der Visite die Möglichkeit, auf benötigte Daten direkt zuzugreifen. Ursprünglich wurde dieses Verfahren eingeführt, um eine korrekte Medikamentenverabreichung sicher zu stellen. Auch soll es doppelte Schreibarbeit verhindern, wenn das Pflegepersonal bereits während einer Behandlung die Patientendaten aktualisieren kann. Die effiziente und bequeme zentrale Speicherung von Patientendaten birgt aus Sicht von Datenschützern aber zugleich eine größere Gefahr für unbefugten Zugriff auf sensible Daten als dies bei einer dezentralen Art des Speicherns der Fall ist. Auch könne es wünschenswert sein, für ÄrztInnen und Pflegepersonal unterschiedliche Zugriffsberechtigungen auf Datensätze zu vergeben, was allerdings komplexe logistische Lösungen erforderlich mache.

Zusammenfassend ergab die Diskussion, dass die RFID-Technologie zwar eine Reihe von Vorteilen für den Verbraucher mit sich bringt, dass die Anwendung aus Datenschutzgesichtspunkten jedoch eine Reihe gravierender Probleme aufwirft. Daher müssen die Rahmenbedingungen so gestaltet werden, dass die eingangs genannten Grundprinzipien des Datenschutzes auch bei RFID-Anwendungen eingehalten werden. Wenn Verbraucher zudem eine echte Wahl haben sollen, sich für oder gegen die Freigabe ihrer Daten zu entscheiden, muss eine Lösung gefunden werden, wie ausreichende Informationen über mögliche Folgen der Datenverarbeitung zur Verfügung gestellt werden (können). Unter dem nun folgenden speziellen Fokus auf den Umgang mit persönlichen Daten bei Kundenkarten, wird ausführlich auf eine weitere Schwierigkeit – die Einwilligung zur Freigabe persönlicher Daten – eingegangen.

5. Verbraucherfallsstricke bei Kundenkartensystemen

Wie *Manfred Zöllmer, MdB* ausführte, gibt es in Deutschland über einhundert verschiedene Payback-Karten „von der ADAC-Karte bis zur ZOO-Freundschaftskarte". Marktführer bei den Karten ist die Firma *Payback,* gefolgt von *Happy Digits*. Eine weite Verbreitung haben Rabattkartenprogramme mit dem Fall des Rabattgesetzes und der Zugabeverordnung gefunden. Mittlerweile geht man nach Untersuchungen davon aus, dass ca. 90 Prozent der Bundesbürger Kundenkarten besitzen, ein Drittel soll sogar vier Karten haben. Dem stünden Kundenrabatte von 0,25 und drei Prozent gegenüber, manchmal auch, wie bei der IKEA-Shopping Card, seien auf der Haben-Seite gar keine finanziellen Anreize für den Kunden zu verbuchen. Bei dem System von Kundenkarten handele es sich insgesamt um einen Austausch von persönlichen Daten und kleinen Rabatten, da laut Stiftung Warentest nur bei zwei von 36 untersuchten Kundenbindungssystemen die Kunden anonym blieben. Gleichzeitig hätten Untersuchungen ergeben, dass Kunden die Höhe der ihnen gewährten Rabatte deutlich überschätzen. Die Unternehmen nutzten die Kundenprofile, um die Kunden gezielt zu bewerben und an sich zu binden. Die Erstellung der Kundenprofile helfe, Kosten im Bereich der Werbung zu sparen.

Dem negativ belegten Tauschgeschäft von „mageren Rabatten für Daten" setzte *Peter H. Drunkenmölle, Leiter der Rechtsabteilung Loyalty Partner, der Betreiberfirma von Payback,* die Notwendigkeit, das Kundeninteresse stärker hervorzuheben, gegenüber. Denn der Umstand, dass *Payback* seit über sechs Jahren erfolgreich am Markt agiere, beweise, dass Kunden aus dem Prinzip Kundenkarte Positives herausziehen würden. Kundenorientierung genauso wie Kundenvertrauen sei gerade die Grundlage des Geschäftsmodells von Kundenkarten, bei Erfolg sei man deshalb augenscheinlich in der Lage, Kunden etwas anzubieten, was sie bräuchten. So liege der Reiz im heutigen Kundenkartensystem nicht mehr alleine im Grundrabatt, den man beim Kauf erhält, sondern darin, dass es darüber hinaus weitere Möglichkeiten zum Punktesammeln, Aktionen für weitere Rabatte usw. gibt.

Probleme mit Datenschutzaspekten

Anders als bei RFID-Anwendungen, sprachen die Podiumsteilnehmer Kundenkarten kaum eine Rolle beim unerlaubten Herauslesen von Daten zu. Eine Gefährdung gehe vielmehr von der unkontrollierten Verwendung legal erhaltener Daten aus, sei es von der sammelnden Stelle, sei es von Dritten.

Übermäßige Datenerhebung

Christian Thorun von der Verbraucherzentrale Bundesverband sah den zentralen Kritikpunkt an Rabattkartenprogrammen darin, dass die meisten Rabattkartenprogramme das Prinzip der Datensparsamkeit massiv verletzen. Viele Unternehmen würden sehr viel mehr Daten erheben, als für den eigentlichen Zweck notwendig wäre.

Hintergrund sei, dass Daten über das Einkaufsverhalten nicht nur zur Abrechnung von Rabattpunkten, sondern auch für Werbezwecke erhoben würden. Auch nehme der Handel mit personenbezogenen Daten an Dritte stark zu. Der Umsatz mit individuellem Marketing habe beispielsweise innerhalb eines Jahres um knapp 30 Prozent von 25 Mrd. Euro auf 32 Mrd. Euro im Jahr 2005 zugelegt. Die Wirtschaftszeitschrift *Capital* habe errechnet, dass allein die vier größten Auskunfteien jährlich mehr als 140 Millionen Datensätze über Verbraucher an die Wirtschaft liefern; der niedersächsische Datenschutzbeauf-

tragte ging nach Angaben von Thorun bereits 2002 davon aus, dass jeder Bundesbürger über 18 Jahre durchschnittlich in 52 kommerziellen Datenbanken erfasst ist.

Durch die systematische Erfassung des Einkaufsverhaltens könnten so ganz detaillierte personenbezogene Einkaufsprofile erstellt werden. Diese Gefahr würde bei elektronischen Kundenbindungssystemen, an denen sich unterschiedliche Händler beteiligen, sogar noch potenziert, mit den bereits für RFID-Tags problematisierten Folgen für individuelle Freiheitsrechte. Was bei einem staatlichen Eingriff zu einem Aufschrei bei den Bürgern führen würde, sei heute in leicht abgeschwächter Weise im nicht-staatlichen Bereich bereits Realität geworden. Fragwürdig sei z. B. die Abfrage des vollständigen Geburtsdatums, des Berufs, des Einkommens oder von Hobbys. Wenn man nicht den gläsernen Verbraucher wolle, müsse das Sammeln von Daten auf ein Minimum beschränkt bleiben, so das Fazit von *Thorun*.

Zur Verwendung der gesammelten Daten stellte *Peter Drunkenmölle von Payback* klar, dass Daten zu Marketingzwecken darauf geprüft würden, wie Angebote zielgruppenspezifisch gemacht werden könnten. Ausgeschlossen sei hingegen die Erstellung von Persönlichkeitsprofilen, für die Daten aus unterschiedlichen Kaufvorgängen zu einer komplexen individuellen Datenbank zusammengeführt würden. *Drunkenmölle* verwies auf die fehlende praktische Verwendung solcher Profile für Werbezwecke, die daraus hervorgehe, dass die herkömmliche Marketingstrategie aus wenigen aussagekräftigen Merkmalen Kundengruppen zu definieren versuche. Demgegenüber seien die Informationen aus der Kundenkarte zu individuell. Nicht befürchten müsse man schließlich, dass persönliche Daten und Kaufverhalten an andere, ebenfalls die Dienste von *Payback* nutzende Unternehmen, weitergegeben würden. Das gleiche gelte auch für Scoring-Daten an Banken und Versicherungen, wenngleich *Drunkenmölle* in diesem Punkt nicht für alle Kundenkartenanbieter gerade stehen wollte.

Unerlaubte Weitergabe von Kaufprofilen

Den Schilderungen des *Payback*-Vertreters setzte *Thorun* Beispiele aus der Praxis entgegen, die die Redlichkeit von Branchenkollegen in puncto Einhaltung des Datenschutzes in Frage stellen sollten. *Thorun* sagte: „Ich möchte keinem seriösen Anbieter von Rabattkartenprogrammen eine kriminelle Intention unterstellen. Fakt ist jedoch, dass die Datenerfassung und -verarbeitung schon heute zu negativen Effekten für die Verbraucher führen.

1. Die Verbraucherzentralen werden mit Beschwerden über ungewollte Werbeanrufe überhäuft. Hierbei geht es den aufgebrachten Verbrauchern nicht nur darum, dass die Anrufe als störend empfunden werden, sondern viele Verbraucher sind auch erstaunt darüber, über wie viele Informationen der Anrufer bereits verfügt.
2. Banken nutzen personenbezogene Daten zunehmend, um die Kreditwürdigkeit von Verbrauchern einzuschätzen. Dies bezeichnet man mit Scoring. Versicherungen haben starkes Interesse an Informationen über Konsumgewohnheiten (Gesundheitsartikel, Alkohol, etc.).
3. Technische Pannen können nie ausgeschlossen werden. So hat ein Missgeschick des Internet-Dienstanbieter AOL dazu geführt, dass 20 Millionen von im Internet veröffentlichten Suchanfragen dazu genutzt werden können, Rückschlüsse auf die Nutzer über deren finanzielle Situation, Krankheiten, Lebensschicksale und das Sexualleben zu ziehen.“

Der feine Unterschied bei der Einwilligung

Viel Raum bei der Diskussion über Praxis von Kundenkartensysteme nahm im Verlauf der Veranstaltung die Gestaltung der Einwilligung zur Freigabe von persönlichen Daten ein. Verbrauchervertreter, Vertreter der Politik als auch Teilnehmer aus dem Publikum sprachen vor allem

die mangelnde Transparenz von Einwilligungserklärungen an. Sie prangerten an, dass auf diese Weise von einer freiwilligen Zustimmung und bewusster Entscheidung der Kunden für die Nutzung ihrer persönlichen und ihrer konsumbezogenen Daten keine Rede sein könne.

Manfred Zöllmer, MdB betonte insbesondere das Anliegen, die Datenerhebung in der Gestalt einer **Opt-In-Lösung** allgemein verbindlich zu machen.

Im Rahmen einer Opt-In-Einwilligung muss der Verbraucher ausdrücklich der Nutzung seiner Daten, beispielsweise zu Werbezwecken, zustimmen und nicht erst aktiv diese Verwendung verbieten müssen (Opt-Out). Eine solche Opt-In-Lösung ist im Gesetz gegen unlauteren Wettbewerb bereits zur Anwendung in anderen Bereichen verankert.

Den Unterschied führte *Christian Thorun von der Verbraucherzentrale Bundesverband* plastisch vor:

„Fragt man Verbraucher beispielsweise: Wollen Sie, dass Ihre Daten zu Werbezwecken verwendet werden?, so antworten zwanzig Prozent mit „Ja“, achtzig Prozent entscheiden sich also dagegen. Fragt man aber anders herum: Ziehen Sie Ihre Einwilligung zurück?, so sagen auch wieder zwanzig Prozent „Ja“. Hier müssen deshalb transparente Bedingungen geschaffen werden, dass Verbraucher nicht aus Unverständnis oder weil sie fürchten, nicht in den Genuss des angestrebten Vorteils zu kommen, auf Ihr Recht verzichten.“

Bemängelt wurde auch die Praxis vieler Betreiber von Rabattkarten, die die **Einwilligung** zur Verwertung von personenbezogenen Daten zu Werbezwecken für die Teilnahme an Rabattprogrammen voraussetzen. Die Verbraucherzentrale Bundesverband sieht hier den Grundsatz der Freiwilligkeit nicht erfüllt und hat daher Klage u. a. gegen den Branchenführer *Payback* eingereicht.

Aus dem Publikum wurde die Frage nach einer kundenfreundlichen Abmeldeoption gestellt. Es wurde angeregt, eine solche Möglichkeit an den Touchscreens von Payback, die sich in Einkaufsläden befinden einzurichten. Sie könnte ähnlich wie bei Newslettern funktionieren, von welchen man sich per Mausklick loslösen kann. *Peter Drunkenmölle* räumte ein, dass dieser Weg zur Abmeldung nicht existiert, sondern über einen Anruf beim Callcenter verläuft. Die gespeicherten Daten würden danach allerdings noch weitere zehn Jahre aufbewahrt, was nach Aussage von *Drunkenmölle* auf die Aufbewahrungspflicht nach dem Handelsgesetzbuch von den dahinter stehenden buchhalterischen Vorgängen, die zum Punktesammeln nötig sind, zurückgeht.

Das Fazit lautete, dass viele Kundenbindungssysteme nicht unbedingt gegen Gesetze verstoßen, dass diese aber dazu verleiten, dass Verbraucher umfassende Daten über sich selbst preisgeben. Der Umfang dieser Daten in privaten Händen habe mittlerweile Dimensionen angenommen, die Regulierungen notwendig machen.

6. Schutzregelungen gegen Datenmissbrauch

Die Positionen im Dreieck Staat-Wirtschaft-Verbraucher

Die Referenten bezogen unterschiedliche Positionen zu notwendigen Maßnahmen, die gegen die Bedenken bei RFID-Anwendungen und Kundenkarten ergriffen werden müssten. Die Pole der Debatte werden einerseits markiert durch neue gesetzliche Vorschriften beim Datenschutz sowie die Sanktionierung von Unternehmen, die gegen die Bestimmungen verstoßen. Dahinter steht die Vorstellung, dass marktgetriebene Prozesse ihrem Wesen nach hierarchisch ablaufen. Gerade der Vorsprung eines Akteurs in Wissen und Information wird als ein wichtiger Antriebsmotor der wirtschaftlichen Dynamik angesehen. Deshalb können Marktprozesse als unvollkommen im Sinne von Transparenzgeboten, der Weitergabe von Informationen sowie der Einhaltung von für alle gleichen Regelungen angesehen werden. Um *gläserne Kunden* zu verhindern, gelten, nach dieser Auffassung staatlich vorgegebene Rahmenbedingungen in Form von rechtlich verbindlichen Regelungen sowie die Sanktionierung von Verstößen als ein notwendiges Korrektiv zum Marktversagen.

Dem stehen andererseits Selbstverpflichtungserklärungen der Unternehmen und zum Teil auch die Idee von Gütesiegeln gegenüber, welche die Eigeninteressen der Wirtschaft als ausreichenden Wirkmechanismus für verbraucherfreundliche Selbstregulierungen innerhalb einer Branche in den Vordergrund stellen. Gegen das Szenario vom gläsernen Kunden werden das Prinzip der Freiwilligkeit und der zivilgesellschaftlichen Selbstorganisation von Interessen sowohl auf der Unternehmer- wie auf der Verbraucherseite angeführt. Staatliche Regulierung wird als vergleichsweise hemmend für die unternehmerische Tätigkeit und als einschränkend für die Wirtschaftlichkeit von Dienstleistungen und Produkten betrachtet.

Schließlich gibt es auch das Szenario vom *gläsernen Bürger*. Damit wird vor einem natürlichen Kontrollbestreben des Staates gewarnt, mit dem Regierungen um die Erhaltung ihrer Machtposition im staatlichen Apparat ringen. Zur ausreichenden demokratischen Kontrolle genügt es nach Ansicht von Kritikern nicht, auf die Einhaltung von gesetzlichen Bestimmungen wie der des Datenschutzes zu pochen. Vielmehr sei es eine wichtige Korrektivfunktion, wenn aus der Mitte der Zivilgesellschaft heraus Handlungstrends und Zukunftsszenarien, die dem widersprechen, frühzeitig öffentlich thematisiert werden können und in die Gestaltung der politischen Agenda mit eingebunden werden.

Offener Dialog im Vorfeld

Teile der Unternehmerlandschaft gehen davon aus, dass neue technologische Anwendungen dann zum Erfolgsfaktor ihrer wirtschaftlichen Tätigkeit werden, wenn bereits der Prozess der Einführung dieser Technologie vom Austausch mit Anwendern und Kritikern begleitet wird. Damit signalisieren Unternehmen einer aufmerksamen kritischen Öffentlichkeit gegenüber, dass sie bereit sind, schon im Vorfeld verbraucherschutzkonforme technische oder auch institutionelle Regelungen anzuwenden und nicht gegen Verbraucherinteressen agieren wollen.

Primat auf technischer Lösbarkeit von Verbraucherschutz

Bei allen Podiumsteilnehmern aus der Wirtschaft herrschte Einigkeit darüber, dass ein System dann sicher würde, wenn die Diskussion offen und anwenderspezifisch geführt werde. Zu einer solchen

Offenheit gehört nach den Worten von *Cord Bartels von NXP Semiconductors* auch die Abwägung, ob aufgezeigte Gefahrenpotenziale tatsächlich technisch gelöst werden können oder man im Zweifelsfall auch endgültig Abstand von einer Technologie nehmen müsse. Als Entwickler müsse man zunächst die Grenzen einer Technologie bestimmen und Risiken definieren, um sie im Prozess der Implementierung, wo dies möglich ist, auf technischem Wege zu beheben. In den vergangenen Jahren habe es in Deutschland bei den Auseinandersetzungen zu RFID an Wissen und konkreten Handlungsoptionen zu einzelnen Anwendungsfällen gefehlt. Die Diskussion sei nur sehr global und von „Glauben und Fürchten" geprägt abgelaufen.

Interessenbestimmung im Konsens?

Andreas Füßler von GS1 beschrieb, wie sein Unternehmen, dessen Tochtergesellschaft EPCglobal als Verwalterin der EPC-Standards gewissermaßen das Herz der RFID-Technologie bedient, eine Diskussionsplattform für alle interessierten Kreise zur Verfügung stellt. Hier sollen Lösungsvorschläge zu Fragen des Daten- und des Warenverkehrs in der Konsumgüterwirtschaft, aber auch in angrenzenden Bereichen, ausgearbeitet werden. Die Durchsetzung der Technologie beruhe auf der Annahme gleicher technischer Standards durch Hersteller und Dienstleister der RFID-Technologie. Daher verlaufen die Arbeiten nach Aussage von *Füßler* zwingend auf dem Konsensprinzip. Hierdurch verspreche man sich eine hohe Effizienz für eine erfolgreiche Erstellung von Lösungspfaden. Von daher sei auch der Konsens mit Verbrauchern und der Politik sehr wichtig.

Rena Tangens von FoeBuD e.V., korrigierte, dass ein Konsensprinzip nur bedingt zur gewünschten Verbesserung des Datenschutzes führe. Man dürfe nicht vergessen, dass Unternehmen erst dadurch zu datenbewussten Unternehmen würden, indem Druck auf sie ausgeübt werde. So habe die Verleihung des Big Brother Awards an die *Payback*-Kundenkarte im Jahre 2000 die Beachtung des Datenschutzes bei den Unternehmens-Verantwortlichen stark vorangetrieben. Bei allen Fortschritten in der Unternehmenskultur könne nicht davon ausgegangen werden, dass Unternehmen sich freiwillig Regeln unterzögen. Hierfür brauche es die entsprechend informierte und aufgeklärte Öffentlichkeit und den Einsatz von Gruppen wie FoeBuD.

Verbraucherakzeptanz als zentraler Regulierungsfaktor

Der Unternehmensvertreter Cord Bartels von NXP Semiconductors vertrat eine ähnliche Auffassung wie *Rena Tangens* **im Sinne** eines konsensorientierten Dialogs zwischen Wirtschaft und Verbrauchern ein. Szenarien von gläsernen Kunden, Mitarbeitern oder Bürgern stellte er den Einwand entgegen, dass man es mit landestypischen Kulturen des Verbraucherschutzes zu tun habe: „Die treibenden Kräfte [für einen bedenklichen Einsatz von Technologien] sitzen meist anderswo. Deutschland wird die Geschwindigkeit nicht vorgeben. Es wird uns schwer fallen, den Aufbau von gewissen Technologien zu verhindern oder auch nur zu hemmen." Demgegenüber betonte *Bartels* Chancen, die in der Mitgestaltung der Technologien lägen. Er führte die Praxis des von Tangens erwähnten Metro-Konzerns, welcher von NXP mit RFID-Chips beliefert wird, als Beispiel an. Das negative öffentliche Echo, das der Pilotversuch im Future-Store nach sich gezogen habe, habe den Konzern veranlasst, von den Chip-Produzenten zu verlangen, dass die Transponder dauerhaft deaktiviert werden können. Wo also die Verbraucherakzeptanz bedroht sei, zeige sich eine klare Rückkopplungsschleife von der Öffentlichkeit in die Wirtschaft hinein. Im Dialog mit den Kritikern der Technologie liegt seiner Meinung nach deshalb gerade eine große Chance für die Industrie. Voraussetzung sei aber eine Offenheit auf beiden Seiten, gemeinsam nach Problemlösungen zu suchen. Wenn frühzeitig in diesen Prozess eingetreten wird, könne das den engagierten Unternehmen sogar weltweit einen Wettbewerbsvorteil bescheren.

Alle Podiumsteilnehmer, die privatwirtschaftliche Unternehmungen repräsentierten, sprachen von einem Lernprozess, in welchen sich ihr Haus im Laufe der jeweiligen unternehmerischen Tä-

tigkeit habe begeben müssen. Unabhängig davon, wie man das Zustandekommen von verbraucherorientierten Ergebnissen im Einzelfall bewertet, zeigt die zunehmend Verbreitung findende Unternehmensstrategie zum Dialog mit unterschiedlichen Interessengruppen wie wichtig eine aufmerksame Öffentlichkeit und das Einstehen für Bedenken von Verbraucherseite ist. Von vorne herein von deckungsgleichen Perspektiven von Unternehmen, Datenschützern und Verbrauchern auszugehen, würde die Wirklichkeit allerdings unzulässig verzerren.

Der Staat als Moderator

Jürgen Karwelat vom Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (BMELV), Referat Verbraucherschutz in der Informations- und Dienstleistungsgesellschaft, berichtete, dass das Bundeswirtschaftsministerium bereits vor zwei Jahren begonnen habe, die Einführung von RFID politisch zu begleiten und über Rahmenbedingungen nachzudenken. Auch *Karwelat* stellte in den Mittelpunkt des Konzeptes des Bundes die Verbraucherakzeptanz. Hierzu sei vor zwei Jahren ein Runder Tisch mit der Wirtschaft sowie den Verbraucherzentralen, Datenschützern und beispielsweise auch der Vereinigung FoeBuD gegründet worden. „Gutes Zureden" zu Beginn solle schärfere Rahmenbedingen und schließlich gesetzliche Lösungen abwenden helfen.

Im Falle von RFID sieht *Karwelat* bislang noch keinen Handlungsbedarf für die Ausweitung der Regulierungsfunktion des Staates, wie bspw. ein spezielles RFID-Gesetz zu schaffen oder das Bundesdatenschutzgesetz zu verändern. Zu seinen Aufgaben als Vertreter der Politik zählte Karwelat das aufmerksame Beobachten, Aufklären von Problemen und Vordenken von Szenarien: „Denn eines ist klar, bei dieser rasanten Entwicklung von digitaler Technik sind bestimmte Entwicklungen gegangen worden, die nicht mehr zurückzuholen sind. Dann ist möglicherweise der Weg in eine Sackgasse, in einen Überwachungsstaat gegangen, den wir verhindern müssen."

Instrumente für selbstbestimmte Kundenentscheidungen

Manfred Zöllmer, MdB definierte die Selbstbestimmung des Kunden als die zentrale verbraucherpolitische Forderung. Dazu gehöre Transparenz über die Verwendung der Technologie, wie sie die **Kennzeichnung von Produkten, die RFID-Chips enthalten**, bietet.

Ein weiteres denkbares Instrument sind **Gütesiegel**, mit deren Hilfe Unternehmen die Selbstverpflichtung zur Einhaltung von Datenschutzkonformität signalisieren können. Gütesiegel wurden in der Veranstaltung nur kurz angesprochen, was möglicherweise mit dem bekannten Problem zusammenhängt, dass sie für die beteiligten Unternehmen komplexe Probleme mit Haftungsregelungen bei Nichteinhaltung mit sich bringen.

Auf Selbstverpflichtungen sollte aus Sicht von *Andreas Füßler von GS1* das Hauptaugenmerk der Industrie liegen. Aus der erwähnten Diskussionsplattform in seinem Unternehmen ist ein Positionspapier der deutschen Wirtschaft mit Leitlinien zum Einsatz der RFID-Technologie entstanden. Danach zählen zu den wichtigsten **Leitlinien der deutschen Wirtschaft**:

Transparenz darüber, wo RFID eingesetzt wird. Dies geschieht üblicherweise mit Hilfe von Produktkennzeichnungen, wie sie auch für andere sensiblen Technologien, z. B. gentechnische Veränderung von Saatgut, eingefordert werden. Heute findet man eine *Kennzeichnung* von RFID in Form des EPC-Logos auf Transportetiketten in der Logistik, wo die Technologie im Rahmen von Pilotprojekten getestet wird. Ein ähnliches Logo sei in Zukunft auch auf Konsumprodukten vorstellbar.

Freiheit des Kunden, selbst entscheiden zu können, wie er diese Technologie eingesetzt sehen möchte. Dazu gehört in erster Linie die Möglichkeit, den Transponder, so er denn Verbreitung im täglichen Leben, beispielsweise im Supermarkt, findet, *deaktivieren* zu können. Oder sich zu entscheiden, ihn auch nach dem Kauf zu nutzen.

Dissens bei Deaktivierungskonzepten

Auch von *Manfred Zöllmer, MdB* wurde die Forderung eingebracht, Kunden zu ermöglichen, dass die RFID-Chips auf eigenen Wunsch **deaktiviert** werden können. Der Verbrauchervertreter *Christian Thorun* unterstrich, dass Verbraucher bei der Anwendung von RFID Angst vor einem Kontrollverlust hätten und die Gefahr sähen, zunehmend überwacht zu werden. Daher würden auch 73 Prozent der Teilnehmer einer Umfrage zu diesem Thema fordern, dass RFID-Chips, die beispielsweise im Einzelhandel verwendet werden, an der Kasse nicht nur deaktiviert, sondern technisch zerstört werden.

Manfred Zöllmer, MdB sprach sich demgegenüber gegen eine generelle Deaktivierung von Etiketten von gekauften Waren aus. Er betonte, dass sich sonst nicht mehr die Zusatzinformationen und Anwendungen in Verbindung mit Lesestationen im Haushalt nutzen ließen.

So sieht *Andreas Füßler von GS1* zwar derzeit in der Deaktivierung von RFID-Chips den Minimalkonsens einer verbraucherfreundlichen Einführung von RFID. Aus seiner Sicht liegt aber in der Umsetzung dieser Anforderung der größte Dissens zwischen Herstellern und Nutzern. Bislang gäbe es auch noch keine zufriedenstellende technische Lösung, da eine automatische Deaktivierung über ein elektronisches Abschaltsystem am Kassenausgang für Kunden nicht überprüfbar ist. Die bislang einzige sichtbare Form über das Abknicken der Antenne sei wiederum für die Unternehmen zu umständlich und zu kostspielig.

Die Deaktivierung ist noch auf andere Weise mit einem schwerwiegenden Problem verbunden. Laut einer Analyse der Deutsche Bank Research[10] können nur wiederbeschreibbare Chips elektronisch abgeschaltet werden. Würden die Chips dieses Typs nun bevorzugt verwendet werden, so böten sie die Möglichkeit für eine gezielte Veränderung der auf ihnen gespeicherten Produktdaten. Dabei ist eine Spannweite von Störungen von Behinderungen der Logistik bis zur Geschäftsschädigung durch z. B. veränderte Mindesthaltbarkeitswerte von Lebensmitteln denkbar.

Vor diesem Hintergrund wurde auf dem Podium der Vorschlag aufgegriffen, genau wie bei Kundenkarten auch bei RFID-Chips eine Opt-In-Option einzuführen. Damit würde die Deaktivierung von Chips beim Verlassen des Ladens der Regelfall. Kunden böte sich umgekehrt auf dem Wege einer Einwilligung die Möglichkeit, eventuelle Vorteile von eingeschalteten Chips gegen mögliche Risiken selbst abzuwägen. Die praktische Umsetzung dieses Vorgangs schien bei den Industrievertretern aber noch schwer vorstellbar.

Gestaltung von Technologien beginnt auf der Ebene der Datenerhebung

Da aus Sicht von Verbraucherschützern der Ansatz zur Verhinderung von Technologien nicht effektiv durchsetzbar ist, plädierte auch *Christian Thorun* für die Mitgestaltung von Technologien durch Verbraucherverbände. Eine wirksame Mitgestaltung beginne aber nicht bei der Folgenbegrenzung, sondern bei der vorsorgenden Konditionierung der Technologie auf die maximale Begrenzung ihres negativen Wirkungsradius.

Im vorliegenden Fall beginne die Gestaltung also bei der Gestaltung der Datenerhebung selbst. Denn beispielsweise sei es manchmal der beste Datenschutz, Dienstleistungen, die mit der Preisgabe persönlicher Daten verbunden sind, nicht in Anspruch zunehmen. Die Einschätzung der Sensibilität von Daten durch Verbraucher sei ein umstrittener Punkt, dem man am besten mit Vorschriften zur möglichst **sparsamen Datenerhebung** begegnen könne.

Peter H. Drunkenmölle, Leiter der Rechtsabteilung Loyalty Partner, Payback, wandte ein, dass es aus juristischer Sicht zwar durchaus Diskussionen über die Mündigkeit des durchschnittlich informierten Verbrauchers gäbe. In Bereichen mit unmittelbarer Gefährdung des Verbrauchers würde diesem deshalb zuweilen die Entscheidung durch

10 Heng, Stefan: RFID-Funkchips. Zukunftstechnologie in aller Munde. Deutsche Bank Research, economics 55. 24. Januar 2006.

gesetzliche Bestimmungen abgenommen – wie beispielsweise beim Gammelfleisch. Bei den hier diskutierten Anwendungen sah *Drunkenmölle* aber keine Gefahr einer unmittelbaren Gefährdung, die beispielsweise ein Verbot von Kundenkarten rechtfertigen würde.

Zur Minimierung von Risiken bereits bei der Datenerhebung wurden folgende Maßnahmen benannt:

- Konkretisierung des Bundesdatenschutzgesetzes zur Verpflichtung zum Opt-In, um das Prinzip der Datensparsamkeit zu verteidigen;
- Verpflichtung der Rabattprogrammbetreiber, personenbezogene Daten nur anonym zu erfassen;
- Umfassende Information der Verbraucher über den Inhalt, Einsatz und Verwendungszweck gespeicherter persönlicher Daten und der auf RFID-Chips gespeicherter Objektdaten
- Deaktivierung als Standardoption an der Kasse im Einzelhandel;
- Evaluierung der Kosten und Nutzen von alternativen Verfahren, wie dem Barcode, im Vergleich.

Brauchen wir einen neuen Datenschutz?

In Überlegungen zu Regelungsbereichen, auf die das Prinzip der Vorsorge angewendet werden sollte, wurden schließlich als Ausblick auch die Datenschutzbestimmungen einbezogen. *Christian Thorun* führte aus, dass der vorliegende Datenschutz geschaffen worden sei, um den Verbraucher vor dem Staat zu schützen. Technologische Entwicklungen habe man dabei nicht im Blick gehabt. Vor diesen veränderten Anforderungen stelle sich heute die Frage, wie neben persönlichen Daten auch **personenbeziehbare** Daten und Verfahren dort verantwortungsvoll verankert werden können.

Nach einer Analyse des Datenschutzexperten Alexander Roßnagel folgen solche Überlegungen auf die Einsicht, dass in einer Zeit allgegenwärtiger Datenverarbeitung das Abheben auf Verarbeitungsregeln von personenbezogenen Daten alleine nicht mehr ausreiche:

„Vielmehr sind im Sinne vorgreifender Folgebegrenzungen auch Situationen zu regeln, in denen noch gar keine personenbezogenen Daten entstanden sind. So bedürfen zum Beispiel die Sammlungen von Sensorinformationen, Umgebungsdaten oder von pseudonymen Präferenzen einer vorsorgenden Regelung, wenn die Möglichkeit oder gar die Absicht besteht, sie irgendwann einmal mit einem Personenbezug zu versehen. […] Ebenso entspricht es dem Vorsorgegedanken, die einzusetzenden Techniksysteme präventiven (freiwilligen) Prüfungen ihrer Datenschutzkonformität zu unterziehen und diese Prüfung zu dokumentieren."[11]

Als weiteren Aspekt im Rahmen von Datenschutzbestimmungen regten die Podiumsteilnehmer die Debatte über **Sanktionen** für Unternehmen, die gegen Datenschutzbestimmungen verstoßen, an. Während *Christian Thorun* und *Rena Tangens* hier von einem klaren gesetzlichen Handlungsbedarf sprachen, appellierte *Manfred Zöllmer, MdB* abschließend an Anstrengungen auf Unternehmensseite. Er forderte die Wirtschaft dazu auf, Verstöße gegen Selbstverpflichtungsauflagen der Wirtschaft zu ahnden, damit gesetzliche Reglementierungen außen vor bleiben können.

11 Alexander Roßnagel (2006): Datenschutz im 21. Jahrhundert. In: Aus Politik und Zeitgeschichte, 30. Januar 2006.

Moderator, ReferentInnen, Tagungsplanung und -organisation, Verfasserin der Broschüre

Moderation:

Rainer Wolf
Freier Journalist, WDR, Wuppertal

Referenten und Referentin:

Cord Bartels
Business Development Manager
NXP Semiconductors, Hermannsburg

RA Peter H. Drunkenmölle
Leiter der Rechtsabteilung
Loyalty Partner, Betreiberfirma Payback, München

Dr. Andreas Füßler
Leiter der Abteilung Forschung und Entwicklung, GS1 Germany GmbH, Köln

Jürgen Karwelat
Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz
Referat Verbraucherschutz in der Informations- und Dienstleistungsgesellschaft, Berlin

Rena Tangens
FoeBuD e.V. , Verein zur Förderung des öffentlich bewegten und unbewegten Datenverkehrs, Bielefeld

Dr. Christian Thorun
Verbraucherzentrale Bundesverband e.V.
Referent Wirtschaftsrecht, Handel und Wettbewerb, Berlin

Nils Zeino-Mahmalat
KompetenzCenter Elektronisches-Fahrgeld-Management (KCESM), Verkehrsverbund Rhein-Ruhr, Gelsenkirchen

Begrüßung und Schlusswort:

Hannelore Hausmann
Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung, Bonn

Manfred Zöllmer, MdB
Sprecher des Gesprächskreises „Verbraucherpolitik“ der Friedrich-Ebert-Stiftung
SPD-Bundestagsfraktion, Stellv. Vorsitzender des Bundestagsausschusses für Ernährung, Landwirtschaft und Verbraucherschutz, Berlin

Tagungsplanung und -organisation:

Hannelore Hausmann
Margit Durch
Abteilung Wirtschafts- und Sozialpolitik der Friedrich-Ebert-Stiftung, Bonn

Verfasserin der Broschüre:

Johanna Maiwald
Politikwissenschaftlerin, M.A., Berlin

ISBN 978–3–89892–748–2

Neuere Veröffentlichungen der Abteilung Wirtschafts- und Sozialpolitik

Wirtschaftspolitik
Was wir Deutschland schulden
WISO direkt

Arbeitskreis Mittelstand
Eine neue Kultur der Selbständigkeit:
Voraussetzung für ökonomischen und sozialen Fortschritt

Gesprächskreis Verbraucherpolitik
Was bringt die Reform des Versicherungsrechts für die Verbraucher?

Gesprächskreis Sozialpolitik
Sozialstaatsstrategien und Beschäftigung im europäischen Vergleich
WISO Diskurs

Gesprächskreis Arbeit und Qualifizierung
Mitarbeiterbeteiligung in Europa, Japan und den USA
Staatliche Rahmenbedingungen für finanzielle Beteiligungsmodelle
WISO Diskurs

Arbeitskreis Arbeit-Betrieb-Politik
Wettbewerb, Prekarität und Sozialschutz:
die sozialen Lizenzanforderungen nach § 6 Abs.3 S.1 Nr.3 PostG
WISO Diskurs

Arbeitskreis Dienstleistungen
Dienstleistungen in Deutschland:
besser als ihr Ruf, dennoch stark verbesserungsbedürftig!

Europäische Wirtschafts- und Sozialpolitik
Polen auf dem Weg zum Euro: Was kommt auf Polen und Deutschland zu?
WISO Diskurs

Gesprächskreis Migration und Integration
Berufliche Ausbildung und Lehrstellenmarkt: Chancengerechtigkeit für Jugendliche mit Migrationshintergrund
WISO direkt

Frauen- und Geschlechterpolitik
Kapital und Kinderkrippen:
Betreuungskonzepte für Kleinkinder aus der Geschlechterperspektive
WISO direkt

Volltexte dieser Veröffentlichungen finden Sie bei uns im Internet unter

www.fes.de/wiso