



Papers on International Political Economy

Arbeitspapiere der Arbeitsstelle Internationale Politische Ökonomie
Working Papers by the Center for International Political Economy

Hrsg. von Prof. Dr. Susanne Lütz



Lukas Jeuck

Datenschutz in der EU –
Der Einfluss transnationaler Akteure auf die RFID-
Empfehlung der Europäischen Kommission



No. 2
2009

Freie Universität  Berlin

Arbeitsstelle Internationale Politische Ökonomie
Center for International Political Economy

Lukas Jeuck

Datenschutz in der EU - Der Einfluss transnationaler Akteure auf die RFID-Empfehlung der Europäischen Kommission

PIPE Working Paper No. 2/2009
Arbeitsstelle Internationale Politische Ökonomie, Berlin
Center for International Political Economy, Berlin
Hrsg. von Prof. Dr. Susanne Lütz

12 December 2009
Papers on International Political Economy
ISSN 1869-4985 (Print)
ISSN 1869-8468 (Internet)

© 2009 by the author(s)

Papers on International Political Economy are working papers from the current research of the Center for International Political Economy at the Free University of Berlin. They appear in irregular intervals and are available for download free of charge from the homepage of the Center.

Lukas Jeuck schloss im Dezember 2009 den Master Internationale Beziehungen der Freien Universität Berlin, der Humboldt-Universität zu Berlin und der Universität Potsdam ab. Diesem ging ein Bachelor der Politikwissenschaften an der Universität Bremen und der Universidad Pública de Navarra voraus, den er 2007 erwarb.

Inhaltlich beschäftigte sich der Autor dabei u.a. mit den politischen Interaktionen von Staaten, internationalen Organisationen und nichtstaatlichen Akteuren. Von besonderem Interesse ist für ihn dabei die Frage, unter welchen Bedingungen nichtstaatliche Akteure Einfluss auf internationale Governance haben.

Darüber hinaus interessiert ihn die Ausgestaltung der Regulierung von Märkten, vor allem in der Europäischen Union, aber auch in Entwicklungs- und Schwellenländern.

Lukas.Jeuck@gmail.com

Downloads
<http://www.polsoz.fu-berlin.de/polwiss/forschung/oekonomie/ipoe/index.html>
PIPE Working Papers

Arbeitsstelle Internationale Politische Ökonomie
Center for International Political Economy
Freie Universität Berlin
Ihnestraße 22
14195 Berlin
Germany

Tel. (+49-30) 838-56470
Fax. (+49-30) 838-56474
<http://www.polsoz.fu-berlin.de/polwiss/forschung/oekonomie/ipoe/index.html>

Abstract

Mit RFID steht seit wenigen Jahren eine Technologie zur Verfügung, die einerseits ein großes wirtschaftliches Potential besitzt, mit deren verbreitetem Einsatz andererseits jedoch auch datenschutzrechtliche Risiken einhergehen. Seit Mai 2009 existiert eine Kommissionsempfehlung zu diesem Thema. Dieser Artikel untersucht diese Policy darauf hin, welche Akteure die Ergebnisse des Politikformulierungsprozesses maßgeblich beeinflussten. Das zentrale Anliegen der Arbeit ist die Analyse des Gewichtes verschiedener von Theorien der europäischen Integration als besonders einflussreich erachteter Akteure. Da weder die Betrachtung der Mitgliedstaaten (Liberaler Intergouvernementalismus) noch die der Kommission (Neo-Funktionalismus) eine erschöpfende Erklärung bieten, wendet sich die Arbeit sowohl transgouvernementalen als auch transnationalen Akteuren zu und zeigt, dass beide Akteure wesentlichen Einfluss nehmen konnten. Abschließend wird ein erster Versuch unternommen, zu erklären, warum diese Akteure im vorliegenden Fall einflussreich waren, obwohl gemeinhin angenommen wird, dass ihr Gewicht für politische Entscheidungen in der EU minimal ist. Hierbei wird auf das Bedürfnis nach Expertise einerseits aber auch die geänderte Rolle transnationaler und transgouvernementaler Akteure in der Umsetzung nicht verbindlicher Governanceformen hingewiesen.

Inhaltsverzeichnis

1. Einleitung	1
2. RFID - Chancen und datenschutzrechtliche Risiken	3
2.1. RFID Technologie und ihre (potentielle) Nutzung	3
2.2. Erwartete und realisierte Vorteile des Einsatzes der RFID Technologie	4
2.3. Potentielle Gefahren der RFID Technologie	5
3. Die Regulation von RFID durch die Empfehlung der Europäischen Kommission	7
3.1. Die Empfehlung der Europäischen Kommission als Steuerungsinstrument	8
3.2. Institutionalisierte Stakeholderdialog während der Regelsetzung	9
3.3. Transnationale und transgouvernementale Akteure als zentrale Handlungsträger	11
4. Zur Erklärungskraft gängiger Theorieansätze	14
4.1. Liberaler Intergouvernementalismus	15
4.2. Neofunktionalismus	16
4.3. Transnationale und transgouvernementale Akteure als wirkmächtige Teilnehmer	20
4.3.1. Zugang transnationaler und transgouvernementaler Akteure	20
4.3.2. Bedürfnis nach Expertise	21
4.3.3. Anerkennung durch nichtstaatliche und transgouvernementale Akteure	22
5. Schluss	24
Bibliographie	25
Annex	30
Interviews	31

1. Einleitung

Die Europäische Gemeinschaft wandte sich dem Thema des Datenschutzes und dem damit eng verknüpften Schutz der Privatsphäre erst vergleichsweise spät zu. So hatte das Europäische Parlament schon seit 1976¹ (Newman 2008: 109) wiederkehrend eine entsprechende Initiative durch die Europäische Kommission gefordert. Doch erst mit dem Entwurf einer Datenschutzrichtlinie von 1990 begann die Kommission selbst aktiv zu werden (Europäische Kommission 1990). Dieser politische Gestaltungsprozess führte schließlich zur Datenschutzrichtlinie von 1995 (Europäischer Rat 1995), einem Dokument, das zwar von verschiedenen Seiten kritisiert², aber dennoch als zentrales Dokument für einen EU-weiten Schutz der Privatsphäre und als globales Vorbild angesehen wird (s. Simitis 1995:469, Newman 2008: 128, Farrell 2003: 285).

Obwohl die Identifizierung mit elektromagnetischen Wellen, im Englischen *radio frequency identification* (RFID), schon seit dem 2. Weltkrieg bekannt ist und eingesetzt wurde (OECD 2008: 6), kommt dieser Technologie erst im Zeitalter der fortschreitenden Informatisierung der Wirtschaft und Gesellschaft (OECD 2008: 10) eine gewichtige Rolle zu³. Gleichzeitig fielen durch technische Fortschritte die Kosten für die Herstellung der Chips, so dass vor allem der wirtschaftliche Nutzen von RFID in den letzten Jahren enorm gestiegen ist und die Technologie damit für einen immer größeren Kundenkreis attraktiv wird. Mit der zunehmenden Verbreitung und Nutzbarkeit der Technologie rückte RFID als datenschutzrelevantes Problem, das nach Ansicht vieler nur unzureichend durch die bestehende Gesetzgebung der EU und der EU Mitgliedstaaten abgedeckt ist, in den Fokus der politischen Diskussion.

2006 gab die Kommission schließlich bekannt, dass sie sich dem Thema RFID inhaltlich annehmen würde. In einem Prozess, der eine zweifache öffentliche Konsultation, eine Reihe von Workshops und die monatliche Konsultation einer mit Stakeholdern besetzten Interessengruppe beinhaltete, wurde eine Empfehlung an die Mitgliedstaaten verfasst, auf welche Art und Weise mit der RFID Technologie vor dem Hintergrund von Gefahren für die Privatsphäre und den Datenschutz zu verfahren sei. In der am 13.05.2009 veröffentlichten Empfehlung (Europäische Kommission 2009) kommt dabei nicht mehr, wie in vorangegangenen ähnlich gelagerten Fällen, eine gesetzliche Regulierung, und im weitesten Sinne staatliche Umsetzung und Kontrolle zum Tragen, sondern eine deutlich ausgeweitete Selbstregulierung durch alle Stakeholder.

Die folgende Projektarbeit geht der Frage nach, wie sich eine RFID-Empfehlung der Kommission herausbilden konnte, die, in Abkehr von der üblichen Praxis im Bereich des Datenschutzes, auf eine selbstregulierende und Stakeholder gestützte Umsetzung abzielt. In anderen Worten: Wie kam es zu einer spezifischen Policy in Form einer Empfehlung der EU Kommission mit einem stark ausgeprägten Element der Selbstregulation durch die Stakeholder auf nationalstaatlicher Ebene?

Dabei sollen die Partizipationsformen und der Einfluss nichtstaatlicher Akteure im politischen Prozess der Entstehung der Kommissionsempfehlung durch eine umfassende empirische Bestandsaufnahme, die sich insbesondere auf eine Dokumentenanalyse und semi-strukturierte Experteninterviews stützt, systematisch

¹ „The European Parliament passed a series of resolutions calling for supranational action, including those of 3 May 1976 O.J. (C 100) 27; 8 May 1979 O.J. (C 140) 147; and 9 March 1982 O.J. (C 87) 39.”

² So beispielsweise vom Juristen und ehemaligen hessischen Datenschutzbeauftragten Spiros Simitis (Simitis 1995)

³ Einen äußerst gelungenen Überblick über den Begriff und Inhalt der Informatisierung bietet Boes 2005.

erkundet werden. Ausgehend von diesen Erkenntnissen soll zugleich das Erklärungspotential gängiger Theorien der EU-Integrationsforschung untersucht werden. Daran anknüpfend sollen Implikationen um den Einfluss nichtstaatlicher Akteure formuliert werden, die darauf zielen, die Debatte um neue Formen der Steuerung und die Abgabe staatlicher Kompetenzen an nichtstaatliche Akteure weiterzuentwickeln.

Die Abkehr von staatlichen zu einer selbstregulierenden Steuerungsform im Bereich des EU-weiten Datenschutzes lässt sich dabei nicht allein auf die verschiedenen behandelten Technologien und Probleme zurückführen, sondern liegt auch an einer verschobenen Teilhabe nichtstaatlicher Kräfte am vorausgegangenen Diskurs sowie an einer veränderten Rolle derselbigen in der anschließenden inhaltlichen (oder substanziellen) Ausgestaltung der Kommissionsempfehlung. Denn - so argumentiert diese Arbeit zusammenfassend - die Stakeholder sind in dem institutionellen Setting eines Stakeholderverfahrens nicht mehr bloße auf Expertise gestützte Ideengeber, sondern darüber hinaus Handlungsträger der Regelumsetzung, deren Anerkennung für das Wirken der Regulation durch die Europäische Union notwendig ist. Dass ohne die Akzeptanz der Inhalte des Steuerungsinstrumentes durch die nichtstaatlichen Akteure eine Umsetzung der Empfehlung undenkbar wäre, erklärt den primären Einfluss auf die Regulierung.

Diese Einsicht hat weitere Implikationen für die Diskussion um politischen Einfluss in der Europäischen Union und darüber hinaus. Neben Staaten und den gemeinschaftlichen Akteuren können in bestimmten Konstellationen auch transgouvernementale und transnationale Akteure spürbaren Einfluss auf den politischen Output nehmen.

Dazu wendet sich die Arbeit in einem ersten Schritt (II) der RFID Technologie zu und zeigt auf, welche gesellschaftlichen Probleme und welcher Nutzen durch eine weitreichende Einführung entsteht. Dabei werden die mit dem Einsatz der Technologie verknüpften datenschutzrechtlichen Probleme im Speziellen in Augenschein genommen, da sie von vielen Experten als die gravierendsten angesehen werden (Europäische Kommission 2007a). Vor diesem Hintergrund, in dem wirtschaftliche Möglichkeiten und datenschutzrechtliche Bedenken in einem Spannungsfeld stehen, wird die Arbeit anschließend die Besonderheiten der Empfehlung der Europäischen Kommission von Mitte Mai 2009 herausarbeiten, ausgehend von der Wahl des Steuerungsinstrumentes über die Prozesse der Regelsetzung und der Konzeption der Regelumsetzung (III). Hieran schließt sich die Analyse des politischen Prozesses und der Ergebnisse aus Sicht der gängigen Theorien der europäischen Integrationsforschung, dem liberalen Intergouvernementalismus und neuerer Varianten des Neofunktionalismus, an. Aufgrund der Beobachtung, dass beide Ansätze keine ausreichende Erklärungskraft bieten, soll ein Versuch unternommen werden, die wesentlichen wirkmächtigen Eigenschaften nichtstaatlicher Akteure für die Regulation der RFID Technologie zu beschreiben. Dabei gelang es den nichtstaatlichen Akteuren, die Empfehlung der EU nicht nur dadurch zu beeinflussen, dass sie Expertise bereitstellten und *access* besaßen, sondern auch durch die Notwendigkeit der Akzeptanz der getroffenen Regelung durch die nichtstaatlichen Akteure (IV). Die so gewonnen Einsichten werden noch einmal auf ihre Implikationen für das Zusammenspiels der Europäischen Union und nichtstaatlicher Akteure hin untersucht und zusammengefasst (V).

2. RFID - Chancen und datenschutzrechtliche Risiken

2.1 RFID Technologie und ihre (potentielle) Nutzung

Kern der RFID Technologie sind oftmals sehr kleine Transponder/ Tags, auf denen bis zu einer gewissen Speichermenge jede beliebige Information gespeichert werden kann. Diese Informationen können dann mit einem entsprechend ausgestatteten Lesegerät auf eine gewisse Distanz via Funkwellen abgefragt werden.

Dabei variiert die Abfragereichweite allerdings beträchtlich: So genannte passive Transponder verfügen über keine eigene Energiequelle und müssen die für die Sendung der Daten erforderliche Energie aus dem elektromagnetischen Impuls der vom Lesegerät ausgesandten Radiowelle bestreiten. Entsprechend gering ist die Abfragereichweite, aber umso kleiner bzw. einfacher kann auch der verwandte Transponder sein. Besonders bei Close-Coupling-Systemen mit Reichweiten von bis zu einem Zentimeter und Remote-Coupling-Systemen, welche eine Reichweite von einem Meter selten überschreiten, kommen daher passive Systeme zum Einsatz (BSI 2005: 34f).

Bei Long-Range-Systemen, die bei derzeitigem Entwicklungsstand über eine Distanz von zehn Metern abgefragt werden können⁴, werden hingegen Transponder mit eigener Energieversorgung, also aktive Systeme, verwendet (BSI 2005: 34f). Diese Systeme sind allerdings im Vergleich zu den passiven kostenintensiver.

Mit Hilfe der RFID Technologie ist es damit möglich, Informationen, die auf einem Chip gespeichert sind, ohne direkten erkennbaren Kontakt eines Lesegeräts zum Transponder auszulesen. Das Auslesen selbst erfolgt dabei leichter und schneller als bei den bereits gängigen optischen Systemen, weil eine größere Zahl an Identifikationen gleichzeitig, bzw. kurz hintereinander erfolgen kann und kein direkter optischer Kontakt bestehen muss.

Auch ist es eine Frage der verwandten Komponenten, ob eine Verschlüsselung der auf den Transpondern gespeicherten Daten vorliegt oder nicht und ob eine aufwendige Authentifizierung von Transponder und Lesegerät vollzogen wird (BSI 2005: 42-45). Um eine Verschlüsselung des Datentransfers zwischen den Komponenten zu ermöglichen, sind bereits eine Reihe von Verfahren u.a. vom Bundesamt für Sicherheit in der Informationstechnik (BSI) oder dem unabhängigen Standardisierer GS1 mit dem Standard für RFID Technologie, dem EPCglobal (BSI: 39f) entwickelt worden.

Um allerdings eine höhere Reichweite, Speicherkapazität oder Sicherheit der Systeme zu ermöglichen, bedarf es aufwändigerer Designs, was zu einer Erhöhung der Kosten für die Produktion und Verwendung der Chips selbst führt.

Es kommt bereits zu einer weitläufigen Verwendung der Technologie in vielen Lebensbereichen, obwohl technische Probleme fortbestehen und der rechtliche Rahmen innerhalb der EU bis vor kurzem ungeklärt war. Die Einsatzorte von RFID sind dabei weitläufig und sollen an dieser Stelle nur beispielhaft ausgeführt werden:

Mit der Einführung biometrischer Reisepässe zum 1. November 2005 enthalten alle nach diesem Stichtag ausgegebenen deutschen Pässe einen RFID Tag in der Vorderseite des Deckels. Die Regierung versprach sich hiervon einerseits eine verbesserte Fälschungssicherheit, andererseits aber auch eine Beschleunigung der Grenzkontrollen.

⁴ Möglich sind mit solchen Systemen Reichweiten bis 100 Meter. In der Entwicklung befinden sich RFID-Transponder und Lesegeräte, die eine Verwendung bis 1 Kilometer ermöglichen.

In der Herstellung kommt RFID bereits an vielen Stellen zum Einsatz. Unter anderem nutzen Audi und Volkswagen Transponder auf den Chassis, die bei der Steuerung von Robotern im Produktionsprozess helfen sollen (Batcheldor 2007).

Im Einzelhandel waren es in der Vergangenheit vor allem die Metro Group und Walmart, die auf eine Einführung der Technologie drängten. Metro eröffnete 2004 einen „Future Store“, in dem RFID sowohl bei der Kennzeichnung der angelieferten Ware, als auch bei der anschließenden Auszeichnung im Supermarkt selbst verwendet wurde und wird.

Eine große Zahl öffentlicher Verkehrsunternehmen wie z.B. die Verkehrsbetriebe der Stadt London, TfL, bieten ihren Kunden zu vergünstigten Konditionen die so genannte Oyster Card an. Auf dieser befindet sich ein Transponder für Close-Coupling Systeme. Dabei hat sich die Bezahlkarte in London als Zahlungsmittel inzwischen weit verbreitet. Auch Städte in Deutschland, wie Hanau, führten 2002 ein auf einem RFID System basiertes Bezahlssystem ein.

Auch im Bereich Militär und Sicherheit wird die RFID immer stärker integriert. So setzt die US Armee in der Versorgung der Truppen in Afghanistan und Irak verstärkt auf RFID gestützte Systeme. Mit Hilfe einer Kombination von RFID und Satellitentechnologie gelingt es den amerikanischen Streitkräften dabei, Informationen über den Transport und die Versorgungslage in Echtzeit zu erhalten (Swedberg 2009).

2.2 Erwartete und realisierte Vorteile des Einsatzes der RFID Technologie

Die Technologie macht es möglich, Objekten eindeutige Identitäten zuzuweisen. Diese können, da kein direkter optischer Kontakt von Nöten ist, schnell und in großer Zahl erfasst und über eine Weiterverarbeitung in Echtzeit genutzt werden.

Daraus ergeben sich zum einen große Einsparmöglichkeiten bei Personal- und Lagerkosten, denn vor allem in der Verarbeitung von Informationen über Warenbewegungen vom Bestellvorgang, Wareneinkauf, über die Annahme, Bewegung im Unternehmen, dem Verkauf und Vertrieb fallen notwendige Datenerhebungen und –verarbeitungen an, die durch RFID, so zumindest die Hoffnung, stark vereinfacht und beschleunigt werden könnten (Interview mit einem Vertreter eines Mittelstandsverbandes).

Weiterhin erhöht sich durch die größere Transparenz die Möglichkeit, noch komplexere Produktionsformen zu ermöglichen, die vor allem in Zeiten einer fortschreitenden Globalisierung, mit der auch eine erhöhte Koordination verschiedener Akteure einhergeht, attraktiv wird.

Neben dem produzierenden Gewerbe hat auch der Einzelhandel ein großes Interesse an einer baldigen und weitreichenden Nutzung der Technologie. Denn durch eine fortgeschrittene Informatisierung und Automatisierung von Wareneingang, -verwaltung und -verkauf an den Konsumenten lassen sich Personalkosten einsparen, ein schnellerer Verkauf und eine geringere Menge an Ausschuss als auch Diebstahl erzielen.

Vor allem von pharmazeutischen Unternehmen wird erwartet, dass sie RFID Transponder dafür nutzen, ihre Produkte gegen Produktpiraterie zu schützen. Hierfür wird allerdings eine weitgehende Verbreitung von RFID-Lesegeräten entlang der Lieferkette, also vom Transport bis zur Apotheke vorausgesetzt, was bislang noch relativ kostspielig zu sein scheint.

Der Dänische Technologierat, ein unabhängiges Gremium des nationalen dänischen Parlaments, wies auch auf potentielle neue Produkte und Dienstleistungen hin, die durch RFID entstehen könnten, darunter Möglichkeiten der erweiterten Produktbeschreibung und –authentifizierung, des Preisvergleichs, der Rückverfolgbarkeit der Herkunft, der zielgenauen Werbung, und der besseren Information über

Inhaltsstoffe und Ablaufdaten (Teknologi-Rådet 2006: 11). Somit lassen sich auch für Konsumenten Vorteile erzielen.

Weiterhin entsteht mit der RFID Technologie auch ein neuer Markt für eine Vielzahl innovativer Produkte. Für die Entwicklung des Marktes für RFID Anwendungen reichen die Schätzungen von einem Volumen von 1,5 Milliarden US\$ für das Jahr 2010 bis hin zu 3 Milliarden für dasselbe Jahr. 2015 wird bereits ein Umfang von 26,9 Milliarden angenommen (OECD 2008: Tabelle 3, S.12).

Aus Sicht einiger Experten und der Europäischen Kommission ist die RFID Technologie darüber hinaus eine der wesentlichen Komponenten eines sich in der Entstehung befindlichen Internets der Dinge (Europäische Kommission 2008: 3, Europäische Kommission 2009b). Vorgebracht wird in der EU die Vision eines Internets, in das auch über RFID Transponder, Wireless-LAN und Sensortechnik Gegenstände eingebunden sind und miteinander kommunizieren können.

Die potentiellen Vorteile und Gewinne, die durch den Einsatz der RFID Technologie entstehen, nehmen dabei umso mehr zu, desto weitläufiger sie verwendet wird. Dabei entstehen sowohl in der Produktion als auch in der Logistik und dem Handel Netzwerkeffekte (Interview mit einem Kommissionsmitglied): Je mehr Unternehmen ihre Produkte mit interoperablen Transpondern ausstatten, desto größer sind die gewonnenen Effizienz- und Informationsgewinne in der Produktions- und Lieferkette und desto günstiger wird auch der Einsatz für Unternehmen, da zu erwarten ist, dass die Kosten für RFID Systeme bei gesteigerter Herstellung aufgrund von Größenvorteilen fallen werden.

Mit einem weitläufigen Einsatz gehen auch veränderte Handlungsgewohnheiten einher. Die Vision eines Internets der Dinge kann hier beispielhaft herangezogen werden: Sollte eine große Zahl an Autos mit Hilfe von RFID in der Lage sein zu kommunizieren, wo sie sich gerade befinden, so ließe sich ein sehr viel sichereres Verkehrsleitsystem installieren als dies bislang möglich ist.

Somit hat die Einführung einer derartigen Technologie nicht allein wirtschaftliche Folgen, sondern eröffnet auch neue Handlungsmöglichkeiten bezüglich der Kontrolle, der Koordinierung und der Lebensgestaltung.

2.3 Potentielle Gefahren der RFID Technologie

Verschiedene Interessengruppen und staatliche Stellen haben auf eine Reihe von Problemen hingewiesen, die bei einer Einführung der RFID Technologie entstehen könnten bzw. bereits bestehen.

So kritisieren sie, dass, sollte die Technologie umfassend umgesetzt werden, eine gesteigerte Anfälligkeit bei technischem Versagen bestünde, was eine erhöhte Technologieabhängigkeit zur Folge hätte (Interview mit einem Industrievertreter). Weiterhin können die Effizienzgewinne aus Sicht der Arbeitnehmerschaft kritisch gesehen werden. Vor allem die Gruppe der Geringqualifizierten, die bislang den Hauptteil der Erfassung von Güterbewegungen übernimmt, wird weiter aus dem Arbeitsmarkt gedrängt. Schließlich gibt es auch Bedenken, ob die genutzten Funkwellen gesundheitsschädlich sein könnten und ob Probleme bei der Abfallentsorgung von mit Transpondern versehenen Produkten bestehen. (vergl.: Schweizerische Bundesamt für Gesundheit 2005).

Die schwerwiegendste Kritik an der Technologie ist jedoch, dass mit ihr datenschutzrechtliche Probleme verknüpft sind. Datenschutz versucht grundsätzlich, den Missbrauch bei der Erhebung und Verwendung personenbezogener Daten zu verhindern. In Deutschland, das im Bereich des Datenschutzes neben den USA eine Vorreiterrolle einnahm, gilt nach Rechtssprechung des Bundesverfassungsgerichts im

Volkzählungsurteil von 1983, dass es sich bei der „informationellen Selbstbestimmung“ um ein Grundrecht handelt, das dem Einzelnen zuspricht, selbst zu bestimmen, mit wem er seine personenbezogenen als auch personenbeziehbaren Daten teilen will und zu welchem Zweck. Das schließt auch die Kontrolle des Umfangs der erhobenen Daten mit ein⁵. International und regional speist sich die Verankerung des Datenschutzes im Recht aus einer Reihe von Dokumenten: Dazu zählen die Empfehlung der OECD vom 23. September 1980 (OECD 1980) und ein fast zeitgleich veröffentlichtes Übereinkommen des Europarats vom 21. Januar 1981 (Europarat 1981), sowie eine Richtlinie der Vereinten Nationen von 1990 (Vereinte Nationen 1990).

Zum Problem mit europäischer Dimension wird RFID allerdings dadurch, dass auch die EU seit 1995 über eine Richtlinie verfügt in der Datenschutz zum wichtigen Element der gemeinsamen Politik erhoben wird (Rat der Europäische Union 1995)⁶. Eine weitere Bestätigung erhielt der Datenschutz in der EU durch die Aufnahme in die Grundrechtecharta im Jahr 2000⁷. Aus der Überlegung heraus, dass bei einer Nichtbeachtung der informationellen Selbstbestimmung die Persönlichkeitsrechte der Bürger belangt wären, leitet sich die Schwere der Gefährdung ab, die sich bei einer unregulierten Verwendung datenschutzrechtlich relevanter Technologien wie der automatisierten Datenverarbeitung, der Telekommunikation oder dem Internet ergeben.

Dass es sich bei RFID um eine datenschutzrechtlich relevante Technologie handelt bzw. handeln kann, wird dabei von allen Stakeholdern anerkannt:

Es ist möglich, persönliche Informationen über Kunden oder Mitarbeiter auf den entsprechend programmierten Transpondern zu speichern. Somit wäre eine eindeutige Zuordnung einer Person mit einem Transponder hergestellt und der Träger ist solange mit Hilfe von Lesegeräten in seinem Verhalten verfolgt, solange er den Transponder bei sich trägt und in Reichweite eines Lesegeräts ist.

Weiterhin wurde für den Einzelhandel angemerkt, dass, sollten Kunden an der Kasse einen mit RFID versehenen Gegenstand zusammen mit einer Kunden- oder Kreditkarte erwerben, die Möglichkeit besteht über die Zuordnung und das unbemerkte Auslesen des individuellen Produktcodes (IPC) den Bewegungen und Präferenzen eines Kunden zu folgen (VZBV 2007). Allgemeiner ist somit auch eine indirektere Zuordnung denkbar, bei der alle, die auf die entsprechende Datenbank zugreifen können, über den einmaligen IPC Rückschlüsse über das Verhalten von Personen ziehen können.

Auch könnten an Gegenständen angebrachte RFID-Tags dazu führen, dass andere über das eigene Konsumverhalten genaueres erfahren. Sollte es sich dabei um Gegenstände⁸ handeln, von denen nicht erwünscht ist, dass andere erfahren, dass sie mitgeführt werden, so kann das einen Eingriff in die

⁵ „Unter der Bedingung der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzten Erhebung, Speicherung, Verwendung, und Weitergabe seiner persönlichen Daten von dem allgemeinen Persönlichkeitsrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“ (Bundesverfassungsgericht 1983, zitiert in: Garstka 2003: 48).

⁶ Näheres zu diesem für die Diskussion um Datenschutz in der Europäischen Union zentralen Dokument findet sich im Abschnitt 3.

⁷ Artikel 8 der Europäischen Grundrechtecharta zum Schutz personenbezogener Daten besagt dass „(1) [j]ede Person [...] das Recht auf den Schutz der sie betreffenden personenbezogenen Daten [hat]. (2) Diese Daten dürfen nur das Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken. (3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.“

⁸ Ein Interviewteilnehmer führte als Beispiel ein Salman Rushdie Buch an.

Persönlichkeitsrechte darstellen, da die Überwachung zu einer erzwungen Verhaltensänderung führen könnte.

Weit weniger wahrscheinlich, aber in seinen Konsequenzen schwerwiegend, wäre ein Szenario, in dem die Technologie eine weitgehende Einführung erfahren hat und somit an vielen Orten Lesegeräte vorzufinden sind. Dann könnte über einen versteckt angebrachten Transponder ein vollständiges Bewegungsprofil erstellt werden (s. u.a. Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) 2009)).

Auch für die Produktion wurden bereits Bedenken geäußert. Durch die Verwendung von RFID Systemen wird es möglich, Mitarbeiter zu überwachen, um Bewegungs- und Leistungsprofile zu erstellen (Verdi 2007: 65ff).

Die Diskussion um Datenschutz und RFID weist zusammenfassend wesentliche Merkmale einer allgemeineren Debatte um neue Technologien mit großen wirtschaftlichen und gesellschaftlichen Potentialen einerseits und einer Reihe von Bedenken daten- und verbraucherschutzrechtlicher Natur andererseits auf. Mit der fortschreitenden Informatisierung der Gesellschaft entstehen dabei immer neue technologische Möglichkeiten, die sowohl große Potentiale als auch Risiken nicht zuletzt datenschutzrechtlicher Natur aufweisen. Die Frage der Entscheidung zwischen verschiedenen Schutzniveaus und der Nutzbarkeit von Technologie ist dabei nicht ausschließlich, aber doch notwendigerweise eine gesellschaftliche Abwägungssache und somit letztlich ein politische Fragestellung.

Für die Regulierung im Bereich RFID Technologie gilt es daher, unter Annahme einer generellen Wunsches nach Datenschutz und größtmöglichem wirtschaftlichen Nutzens, folgende drei Fragenkomplexe zu beantworten:

1. In wieweit beeinflusst die Umsetzung der Technologie das Datenschutzniveau der Bürger negativ und wie groß ist der zu erwartende Nutzen der dem gegenüber steht?
2. Weiterhin gilt es dann zu klären: Welches Schutzniveau ist angemessen und sollte angestrebt werden?
3. Wie kann eine Regulierung aussehen? Soll die Umsetzung von den Anwendern durch eine freiwillige Selbstkontrolle selbst übernommen werden? Ist eine hierarchische Steuerung über Ge- und Verbote und Gesetze angebracht? Sind Mischformen am sinnvollsten?

Die letzte Frage wird diese Arbeit gemäß der aufgeworfenen Fragestellung im Folgenden weiter behandeln.

3. Die Regulation von RFID durch die Empfehlung der Europäischen Kommission

Mit der am 12. Mai 2009 veröffentlichten „Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID- gestützten Anwendungen“ (RFID-Empfehlung) kam die politische Diskussion auf Ebene der EU zu einem vorläufigen Abschluss.

Wie der folgenden Teil aufzeigt, bestimmten zwei Faktoren maßgeblich das Ausmaß der Partizipationsmöglichkeiten staatlicher und nichtstaatlicher Akteure bei der Entstehung der RFID-Empfehlung: Zum einen die Wahl einer Empfehlung als Regulierungsinstrument durch die Europäische Kommission und zum anderen die starke Fokussierung auf transnationale und transgouvernementale Akteure bei der Regelsetzung und –umsetzung.

3.1 Die Empfehlung der Europäischen Kommission als Steuerungsinstrument

Indem die Kommission als politisches Instrument eine Empfehlung wählte, legte sie sich auf ein spezifisches Steuerungsinstrument fest, um sich der RFID-Technologie als datenschutzrelevantem Problem anzunehmen. In diesem Fall geschah dies gerade nicht über die Initiierung einer Richtlinie, also einem vergleichsweise hartem, sondern eines weichen Steuerungsinstrumentes. Im Gegensatz zu EU-Richtlinien oder EU-Verordnungen ist bei einer Empfehlung die Zustimmung der anderen EU-Institutionen nicht notwendig und sie ist nicht zwingend in nationales Recht umzusetzen. Die Verwendung des Konjunktivs im Zusammenhang mit Handlungsempfehlungen à la „Mitgliedstaaten sollten ihren Beitrag zu diesem Prozess leisten“ (Europäische Kommission 2009a: 48) bringt zum Ausdruck, dass die RFID-Empfehlung nur bei Akzeptanz durch die Regelungsadressaten Wirkmächtigkeit erhalten kann: „Diese Empfehlung gibt den Mitgliedstaaten *Orientierungshilfen* [Hervorhebung durch L.J.] für die Gestaltung und den Betrieb von RFID-Anwendungen“ [Europäische Kommission 2009a: 48].

Aus einer ebensolchen Empfehlung erwächst insgesamt zwar kein hierarchisch organisierter Handlungs- bzw. Unterlassungszwang über Gesetze. Denkbar wäre sogar, dass sowohl Nationalstaaten und/ oder Betreiber die Kommissionsempfehlung ignorieren und sich nach Gutdünken, allerdings im Rahmen der geltenden datenschutzrechtlichen Bestimmungen verhalten. Ein gewisser Druck auf die Mitgliedstaaten und die anderen angesprochene Akteure entsteht jedoch durch die Aufforderung, bis 24 Monate nach der Veröffentlichung (also im Mai 2011) einen Bericht über die eingeleiteten Maßnahmen bei der Kommission vorzulegen. Außerdem behält sich die Kommission das Recht vor, innerhalb von drei Jahren selbst einen Bericht über den Grad der Umsetzung der Empfehlung im Amtsblatt zu veröffentlichen, wobei sie hier im Besonderen analysieren will, wie wirksam sich die Empfehlung gegenüber Wirtschaftsteilnehmern und Verbrauchern erwiesen hat (Europäische Kommission 2009a.: 51; Folgemaßnahmen). Daraus entsteht ein Potential für sogenanntes ‚*naming und shaming*‘ auch jenseits der Mitgliedstaaten.

Das Instrument der Empfehlung setzt auf die Selbstverpflichtungen der Akteure, den Einsatz von RFID datenschutzfreundlicher zu gestalten. Die Wahl einer Empfehlung, die neben Regierungen jedoch auch nichtstaatlichen und mit den Datenschutzbeauftragten auch transgouvernementale⁹ Akteuren gegenüber ausführliche und direkte Handlungsvorgaben macht, ist im Bereich des Datenschutzes eine neue Entwicklung. Sowohl die Grundsteinlegung datenschutzrechtlicher Bestimmungen in der Europäische Union in Form der Datenschutzrichtlinie (EU 1995) als auch die stärker auf spezifische Technologien und Märkte wie das Internet und Telekommunikation abzielende Datenschutzrichtlinie für elektronische Kommunikation von 2002¹⁰ (EU 2002) wurden in Form einer Richtlinie verabschiedet. Dabei folgten diese Entscheidungen den Verhandlungen zur Datenschutzdirektive erst nach 1993¹¹ (Heisenberg 2005: 54), nach Art 251 (ex-189b) EG-Vertrag dem Mitentscheidungsverfahren, was dem Europäischen

⁹ Unter transgouvernementalen Akteuren versteht diese Arbeit quasi-autonome mit bestimmten Aufgaben und Machtressourcen versehene Netzwerke von Staatsdienern (vergl. Newman 2008).

¹⁰ Der volle Name des Instruments lautet Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

¹¹ Da die ersten Verhandlungen zur Datenschutzrichtlinie 1990 begannen wurde nach der alten Regelung mit dem Verfahren der Zusammenarbeit (Art. 252 EG-Vertrag) gearbeitet. Nach der Unterzeichnung des Vertrags von Maastricht trat das Mitentscheidungsverfahren (Art. 251 EG-Vertrag) an dessen Stelle.

Parlament neben dem Europäischen Rat die Notwendigkeit der Zustimmung zuspricht. Da es sich um Verhandlungen in der ersten Säule handelte, war für eine Annahme eine qualifizierte Mehrheit notwendig.

Als potentiell mögliche, ebenfalls ‚weiche‘ Regulierungsalternative wäre auch die Offene Methode der Koordinierung (OMK) in Betracht gekommen, bei der sich die Mitgliedstaaten auf häufig sehr offene politische Ziele einigen, die dann mit Hilfe von Benchmarks und Indikatoren die Befolgung der Ziele durch die Mitgliedstaaten messen. Die Ergebnisse werden von der Europäischen Kommission veröffentlicht und es kann bei Nichterfüllung Druck aufgebaut werden. Weiterhin erhofft man sich über den Performanzvergleich der Länder Best-Practice¹² Modelle zu finden, von denen andere lernen können, um somit insgesamt zu besseren Regulationsmodellen zu gelangen (Eberlein/ Kerwer 2004: 123f). Damit eignet sich die OMK besser für eine effektive Regulierung über weiche Faktoren wie ‚*naming and shaming*‘ oder politisches Lernen als eine Empfehlung. Aber auch für die Nutzung der OMK bedarf es der Zustimmung durch die im Rat vertretenen Mitgliedstaaten.

Um sich den datenschutzrechtlichen Bedenken im Zusammenhang mit RFID anzunehmen, wählten die Europäischen Institutionen eine Kommissionsempfehlung trotz einer schwachen rechtlichen Durchsetzbarkeit von weichen Steuerungstypen, einer historisch anderen Regulierungspraxis im Bereich Datenschutz und unter Anbetracht anderer alternativer weicher Steuerungsformen mit größerer Erfolgsaussicht.

3.2 Institutionalisiertes Stakeholderdialog während der Gesetzgebung

Die am 12. Mai 2009 veröffentlichte „Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID- gestützten Anwendungen“ (RFID-Empfehlung) stellt das Endergebnis eines ca. dreijährigen politischen Prozesses dar, sich zu der RFID Technologie vor dem Hintergrund bestehender und perzipierter datenschutzrechtlicher Bedenken zu positionieren.

1999 war es Forschern am MIT gelungen, durch die Integrierung mehrere technischer Verbesserungen RFID Systeme zu entwickeln, um diese kostengünstig und somit für die breite Anwendung nutzbar zu machen (Heisenberg 2005: 150). Die in diesem Zusammenhang entstandene Firma Auto-ID, welche später mit anderen Unternehmen zu EPC global fusionierte, warnte dabei früh über datenschutzrechtliche Probleme und Bedenken der Bürger (Heisenberg 2005: 111).

Seit 2003 erfolgten erste auf Ebene der Mitgliedstaaten angesiedelte Stellungnahmen zum Thema Datenschutz und RFID. Eine erste Entschließung erfolgte im selben Jahr auf der Internationalen Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre in Sidney¹³. Dieser folgten andere Entschließungen auf nationaler¹⁴ und internationaler¹⁵ Ebene, die die datenschutzrechtlich Problematik der RFID Technologie anführten und bereits erste Empfehlungen entwarfen.

¹² Vielleicht können sich auch ‚worst-practice‘ Fälle finden, von denen andere Mitgliedstaaten tunlichst Abstand nehmen sollten.

¹³ International Conference of Data Protection & Privacy Commissioners: Resolution of Radio-Frequency Identification . 20. November 2003.

¹⁴ In Deutschland sind dies: Die Konferenzen der Datenschutzbeauftragten Nr. 67 (2004), 72 (2006) und der 21. Tätigkeitsbericht des Bundesdatenschutzbeauftragten (2006).

¹⁵ International Conference of Data Protection & Privacy Commissioners: Resolution of Radio-Frequency Identification . 20. November 2003.

Es entspann sich in verschiedenen Staaten eine hitzige Debatte um die datenschutzrechtlichen Probleme, die mit einer weiträumigen Einführung von RFID einhergehen könnten¹⁶.

Politische Aktivität ging zuerst von der Europäischen Kommission aus: Viviane Reding, Kommissarin für Informationsgesellschaft und Medien, vertrat auf einer Veranstaltung auf der Cebit im März 2006 die Ansicht, dass den berechtigten Bedenken in Zusammenhang mit Datenschutz und Datensicherheit durch die Europäische Kommission Rechnung zu tragen sei. So fürchtete sie einen fragmentierten Ansatz, der den Schutz der Privatsphäre nicht ausreichend würdigen könnte (Reding 2006: 5). Auch stellte sie in Aussicht, dass sich alle Stakeholder an den Diskussionen um einen möglicherweise notwendigen Regelungsbedarf beteiligen sollten. Zu diesem Zweck kündigte sie einen offenen Konsultationsprozess und eine Serie von Workshops mit allen Stakeholdern an (Reding 2006).

In insgesamt fünf Workshops, die zwischen dem 6. März und 16. Oktober 2006 von der Generaldirektion (DG) Informationsgesellschaft und Medien organisiert wurden, sprachen alle relevanten Stakeholder von Unternehmen, Mitgliedstaaten, Forschungsinstituten, zivilgesellschaftlichen Gruppen, Standardisierern und Kommissionsmitgliedern zu einer Vielzahl von Themengebieten. Neben Workshops zu RFID und dem Internet der Dinge, Interoperabilität und Standardisierung und dem RFID Frequenzspektrum wurde auch eine Veranstaltung zu Datenschutz, Gesundheits- und Sicherheitsthemen angeboten. Auf dieser in mehreren Sitzungen organisierten und über zwei Tage stattfindenden Sitzung ging es der Kommission in erster Linie darum, ein solides Verständnis für die bedeutendsten Sicherheits- und Vertrauensbedenken, die Gesundheitsrisiken und datenschutzrechtlichen Probleme der Technologie zu generieren (Europäische Kommission 2006).

Gleichzeitig fanden seit dem 3. Juli 2006 Onlinekonsultationen auf der ‚Your voice in Europe‘ Website der EU statt. Mehrere thematische Blöcke lassen sich identifizieren, von denen einer der zentralsten thematischen Einheiten „Security, Privacy and Data Protection, and Safety“ (Europäische Kommission 2007b: 17f) ist. Insgesamt 2190 Antworten gingen im Konsultationszeitraum zwischen Juli und September 2006 bei der Kommission ein, was einen Rekord in der öffentlichen Anteilnahme an Onlinekonsultationen der Kommission darstellte (Interview mit Mitglied der Europäischen Kommission). Am 15. März 2007 kam es schließlich zur Veröffentlichung einer Kommissionsmitteilung, in der das weitere Vorgehen der Kommission beschrieben wurde. Dabei sah die Kommission vor allem zu den Themen Datenschutz und Datensicherheit erhöhten Diskussionsbedarf (Europäische Kommission 2007a: 10). Vor allem um die Bedenken gegenüber der Gefährdung des Datenschutz und Datensicherheit auszuräumen und eine verstärkte Verständigung zwischen den beteiligten Interessen herbeizuführen, war eine der zentralsten Maßnahmen, die angekündigt wurde, die Einrichtung einer RFID Interessengruppe, in der alle Gruppierungen ausgewogen vertreten sein sollten. Auch werde die Kommission bis Ende 2007 „eine Empfehlung zu Grundprinzipien veröffentlichen, die von den Behörden und anderen Beteiligten im Zusammenhang mit der RFID-Nutzung anzuwenden sind“. Schlussendlich versprach die Kommission auch unter Beteiligung der Interessengruppe und der Artikel-29-Gruppe die zukünftigen gesetzgeberischen Maßnahmen zu identifizieren, die für den Erhalt der Privatsphäre nötig sind (Europäische Kommission 2007a: 10f).

¹⁶ So kam es in der Bundesrepublik 2004 zu Auseinandersetzungen zwischen dem FoeBud, einer Datenschützer-NGO und der Metro Group um im Metro Future Store verwandte RFID Technologie. Metro hatte für die Konsumenten unbemerkt, RFID-Tags in den Kundenkarten untergebracht. Diese Entdeckung wurde von den Datenschützern genutzt um die Diskussion zu verschärfen und auf die Gefahren hinzuweisen (FoeBud 2004). Ähnliche Diskussionen entflammten auch in Großbritannien und den USA (Hunt et al. 2007: 98ff).

Ab Juni 2007 trafen sich die Mitglieder der RFID Interessengruppe, also Vertreter der Industrie, der Verbraucherschützer, der Gewerkschaften, der Standardisierer und des DG Informationsgesellschaft und Medien mit nationalen und europäischen Datenschützern, Experten und Staatenvertretern, wobei letztere allerdings nur zu bestimmten Sitzungen eingeladen wurden. Die Sitzungen fanden in etwa monatlich (Interview mit einer Vertreterin der Industrie) und bis März 2009 statt.

Obwohl die Empfehlung in der Mitteilung für Ende 2007 angekündigt war, dauerte es bis Mitte Mai 2009, bis das Dokument schließlich veröffentlicht wurde.

Im Februar 2008 hatte die Kommission eine erste Entwurfsfassung des Vorschlags konzipiert und veröffentlicht. Dieser Entwurf wurde in einer zweiten Onlinekonsultation bis April 2008 Abschnitt für Abschnitt zur Kommentierung freigegeben. Die Bearbeitung von über 1000 Seiten unstrukturierter Texte durch 600 Antworten, mit denen sich die Kommission daraufhin konfrontiert sah, führte zu einer Bearbeitungszeit derselbigen von vier bis fünf Monaten (Interview mit Kommissionsmitarbeiter des DG Informationsgesellschaft und Medien).

Konzeptionell beendete die Kommission ihre Arbeit im Zeitraum zwischen August und September 2008 (Interview mit Kommissionsmitarbeiter des DG Informationsgesellschaft und Medien). Allerdings benötigte das DG Informationsgesellschaft und Medien noch einmal insgesamt sechs Monate, um einerseits die juristischen Fragen zu klären (etwa vier Monate) und die Zustimmung der anderen DGs einzuholen und deren Vorschläge mit einzuarbeiten (Interview mit Kommissionsmitarbeiter des DG Informationsgesellschaft und Medien).

Somit lässt sich festhalten, dass die politische Konzeption in großem Maß begleitet wurde von nichtstaatlichen und transgouvernementalen Akteuren. Diesen wurde sowohl in den beiden Onlinekonsultationen und der Interessengruppe die Möglichkeit gegeben, ihre Positionen zu den verschiedenen Regulierungselementen gegenüber der Kommission mitzuteilen. Obwohl die Kommission sich spätestens seit 2001 darauf festlegte, die Interessen nichtstaatlicher Akteure anzuhören, geht das vorgefundene Maß an Teilhabe sehr weit (Europäische Kommission 2001).

3.3 Transnationale und transgouvernementale Akteure als zentrale Handlungsträger

Obwohl die Empfehlung formell an die Mitgliedstaaten gerichtet ist (Europäische Kommission 2009a: 51), werden auch andere Handlungsträger angesprochen die ihre Aktionen entsprechend den Vorstellungen der Kommission anpassen sollen. Zu allererst sind dies RFID-Anwendungsbetreiber, also all jene die „über Zweck und Mittel des Betriebs einer [RFID-] Anwendung entscheide[n]“. Darunter fallen neben Behörden und Einrichtungen auch natürliche und juristische Personen wie Unternehmen (Europäische Kommission 2009a: 49, Begriffsbestimmungen).

Weiterhin werden auch den nationalen Datenschutzbeauftragten, von Newman als transgouvernementale Akteure („*transgovernmental actors*“) bezeichnet (Newman 2008), für die Durchsetzung und nähere nationale Ausformulierung der Empfehlung herangezogen (Europäische Kommission 2009a: 50; Datenschutzfolgenabschätzung). Dies geschieht durch eine Handlungsaufforderung an alle nationalen Datenschutzbeauftragten und den Zusammenschluß aller nationalen und des europäischen Datenschutzbeauftragten in der Artikel-29-Gruppe. Schließlich werden auch zivilgesellschaftliche Akteure und Standardisierungsorganisationen als Regelungsadressaten einbezogen.

Die folgende Tabelle gibt einen detaillierten Überblick über die in den Regelungsinhalten neben den Mitgliedstaaten angesprochenen Akteure und das von ihnen erwünschte Verhalten.

Tabelle 1: Ergebnisse des Regulierungsprozesses

Datenschutzfolgenabschätzung (S.50)	
Betreiber („Branche“)	<ul style="list-style-type: none"> - Zusammen mit Zivilgesellschaft: Ausarbeitung eines allg. Rahmens für Datenschutzfolgenabschätzung innerhalb von 12 Monaten - Datenschutzfolgenabschätzung im Einklang mit allg. Rahmen und den zuständigen Behörden - Einsatz organisatorischer und technischer Maßnahmen um Schutz personenbezogener Daten sicherzustellen, Benennung eines für Datenschutz Verantwortlichen
Zivilgesellschaft	<ul style="list-style-type: none"> - Zusammen mit Betreibern: Ausarbeitung eines allg. Rahmens für Datenschutzfolgenabschätzung innerhalb von 12 Monaten
Datenschutzbeauftragte („Art.-29-Gruppe“; „zuständige Behörden“)	<ul style="list-style-type: none"> - Art.-29-Gruppe: Prüfung des allg. Rahmens für die Datenschutzfolgenabschätzung - nationale Datenschutzler: Überprüfung der Datenschutzfolgenabschätzungen

Informationssicherheit (S. 50)	
Betreiber	<ul style="list-style-type: none"> - Entwicklung neuer Programme bzw. Anwendung bestehender Programme um angemessenes Sicherheitsniveau zu garantieren (Zertifizierung, Selbstbewertung)
Europäische Kommission	<ul style="list-style-type: none"> - Ermittlung von die Informationssicherheit bedrohenden Anwendungen
Nat. Datenschutzbeauftragte („zuständige nationale Behörden“)	<ul style="list-style-type: none"> - Entwicklung neuer Programme bzw. Anwendung bestehender Programme um angemessenes Sicherheitsniveau zu garantieren (Zertifizierung, Selbstbewertung)
Zivilgesellschaft	<ul style="list-style-type: none"> - Entwicklung neuer Programme bzw. Anwendung bestehender Programme um angemessenes Sicherheitsniveau zu garantieren (Zertifizierung, Selbstbewertung)

Informationen und Transparenz	
Betreiber	<ul style="list-style-type: none"> - Kurze, informative und verständliche Information über RFID-Anwendung im Rahmen von in der Empfehlung formulierten Mindeststandards
Europäische Normungsgremien	<ul style="list-style-type: none"> - Entwicklung eines europaweit einheitlichen RFID-Kennzeichens (inkl. Namen des Betreibers, Anlaufstelle für Information)

RFID-Anwendungen im Einzelhandel (S. 50f)	
Betreiber (als Einzelhändler bzw. Hersteller)	<ul style="list-style-type: none"> - Hinweis auf Verwendung von RFID durch Anbringung von RFID-Kennzeichen - Deaktivierung oder Entfernung der Tags am Verkaufsort, außer Kunde stimmt weiterem Betrieb zu, oder ... es werden keine personenbezogenen Daten erhoben (Datenschutzfolgenabschätzung) - Einzelhändler/ Produzent bleibt nach Deaktivierung rechtspflichtig

Sensibilisierungsmaßnahmen (S.51)	
Europäische Kommission	<ul style="list-style-type: none"> - Gemeinsam mit anderen Akteuren Aufklärung über Chancen und Risiken - Gemeinsam mit anderen Akteuren Ausarbeitung von Best-Practice-Fällen
Betreiber	
Datenschutzbeauftragte	
Zivilgesellschaft	

Forschung und Entwicklung (S. 51)	
Europäische Kommission	<ul style="list-style-type: none"> - Zusammenarbeit mit den anderen genannten Akteuren um Forschung und Entwicklung in Richtung eingebauter Sicherheit und Privatsphäre zu unterstützen
Betreiber (Branche)	
Zivilgesellschaft	

Folgemaßnahmen (S. 51)	
Mitgliedstaaten	<ul style="list-style-type: none"> - Treffen notwendiger Maßnahmen - 24 Monate nach Veröffentlichung der Empfehlung Mitteilung über getroffene Maßnahmen
Europäische Kommission	<ul style="list-style-type: none"> - Bericht über Umsetzung, Wirksamkeit und Auswirkungen auf Wirtschaftsteilnehmer und Verbraucher

Dabei ist auffällig, dass die Mehrzahl der in der Empfehlung vorgebrachten Handlungsorientierungen nur dann sinnvoll umgesetzt wird, wenn transnationale und transgouvernementale Akteure sich ihnen entsprechend verhalten: Es sind Unternehmen, die eine Datenschutzfolgenabschätzung unternehmen sollen, die Informationen bereit stellen und sensibilisieren und Best-Practice-Modelle entwickeln sollen. Dabei tun sie dies im Idealfall unter Mitarbeit und Aufsicht von zivilgesellschaftlichen Gruppen und den Datenschutzbeauftragten.

Dadurch soll nicht in Abrede gestellt werden, dass ein Eingreifen und unterstützendes Verhalten seitens der Mitgliedstaaten nicht auch zum Erfolg der Empfehlung beitragen würde. Allerdings wäre auch der Fall denkbar, dass die überwiegende Zahl der Handlungs- und Unterlassforderungen der Kommission ohne ein Zutun der nationalen Regierungen erreicht werden könnte, indem sich die Stakeholder selbst regulieren.

Spezifischer lässt sich sagen, dass allein die Erstellung eines Follow-Up-Berichts über im Sinne der Empfehlung getroffene Maßnahmen, den die Mitgliedstaaten bei der Kommission innerhalb von 2 Jahren einzureichen haben, vom Wirken der Regierungen abhängt. Alle anderen spezifizierten

Handlungsorientierungen richten sich immer auch an andere Akteure und könnten von diesen auch ohne das Zutun der nationalen Regierungen erbracht werden. Die bei weitem häufigste gebrauchte Formulierung ist die, dass Mitgliedstaaten dafür sorgen sollen, dass Betreiber, zivilgesellschaftliche Akteure und Behörden bestimmte Dinge tun bzw. unterlassen sollen.¹⁷ Demgegenüber beinhalten andere Abschnitte der Kommissionsempfehlung einen direkten Bezug auf die RFID-Betreiber. So heißt es hinsichtlich von RFID-Empfehlungen im Einzelhandel: „Die Betreiber sollten Einzelpersonen anhand eines europaweit einheitlichen Zeichens, das von den europäischen Normungsgremien mit Unterstützung der beteiligten Akteure entwickelt wird, über die Präsenz von RFID-Tags informieren, die an Produkten angebracht oder darin eingebettet sind.“ (Europäische Kommission 2009a: RFID-Anwendungen im Einzelhandel).

Aufgrund der Vielzahl an Handlungsaufforderungen, die sich direkt oder indirekt an Unternehmen, Datenschutzbeauftragte, die Zivilgesellschaft richten, kann von einer Empfehlung gesprochen werden, die über die Nationalstaaten als angesprochene Handlungsträger allein deutlich hinausgeht. Somit wird mit der RFID-Empfehlung eine breite Steuerung aller wesentlichen Akteure angestrebt. Denkbar wäre dabei, wie ausgeführt, auch eine Steuerung der transnationalen und transgouvernementalen Akteure an den Mitgliedstaaten vorbei, sollten diese kein Interesse daran haben, sich den Handlungsempfehlungen der Kommissionsempfehlung anzupassen. Dies entspräche einer aus Brüssel angeregten und mit der Empfehlung genauer spezifizierten Selbstregulierung der Stakeholder. Dabei handelt es sich allerdings nicht allein um eine Selbstverpflichtung der Industrie, sondern um Regelungen, die sowohl in der nationalen Präzisierung der Vorgaben (Erarbeitung einer Datenschutzfolgenabschätzung durch Betreiber und die Zivilgesellschaft, gemeinsame Erstellung eines Hinweiszeichens für RFID) als auch in der Umsetzung (Datenschutzfolgenabschätzung durch Datenschutzbeauftragte) alle wesentlichen Akteure einbeziehen und deren Mitarbeit benötigen.

Obwohl der Datenschutz und der darin verankerte Schutz der Privatsphäre zentrale Güter aller europäischen Staaten sind, werden neben den Mitgliedstaaten vor allem die Betreiber, zivilgesellschaftliche Akteure und Datenschutzbeauftragte zentral in die Durchführung der Umsetzung der Empfehlung eingebunden.

4. Zur Erklärungskraft gängiger Theorieansätze

Aufgrund der Vielzahl potentiell erklärender Variablen erscheint es sinnvoll eine Vorauswahl zu treffen, indem besonders einflussreiche und als erklärungskräftig betrachtete Theorien auf ihre Anwendbarkeit und Erklärungskraft hin überprüft werden. Diese Ansätze isolieren bestimmte als besonders wirkmächtig geltenden Variablen, deren Einfluss als zentral angenommen wird.

Neben dem liberalen Intergouvernementalismus in der Tradition Moravcsiks (Moravcsik 1991, 1997, 1998) machen auch moderne Varianten des Neofunktionalismus, die die Rolle der Kommission bei der Erweiterung ihrer Kompetenzen und der Einführung supranationaler Entscheidungsformen betonen,

¹⁷ Unter anderem sollen die Mitgliedstaaten sicherstellen, dass vor der Einführung von RFID-Anwendungen eine Technikfolgenabschätzung bezogen auf den Schutz der Privatsphäre erstellen sollen, geeignete Maßnahmen für den Schutz der personenbezogenen Daten und der Privatsphäre gewährleisten oder einen für den Datenschutz Verantwortlichen vor Ort benennen sollen (Europäische Kommission 2009a: 50; Datenschutzfolgenabschätzung).

Aussagen über das Zustandekommen politischer Entscheidungen in der Europäischen Union (Jabko 2006, Stone Sweet et al. 2001).

4.1 Liberaler Intergouvernementalismus

Nach Auffassung des liberalen Intergouvernementalismus sind es in erster Linie die im Europäischen Rat vertretenen Mitgliedstaaten, die in Verhandlungen miteinander über die Policies der Europäischen Union entscheiden. Da der liberale Intergouvernementalismus weiterhin davon ausgeht, dass Mitgliedstaaten ihre relative Macht einsetzen, um ihre Ziele zu erreichen, sind es vor allem die relativ gesehen mächtigen Mitgliedstaaten, die über den Ausgang von Verhandlungen entscheiden (Moravcsik 1991: 27, 48f). Als weiteres wesentliches Element dieser Theorie wird die Herkunft der nationalen Präferenzen hergeleitet aus der nationalen Interessenkonstellation. Dabei nehmen Staatsdiener die Rolle von Transmissionsriemen ein (Moravcsik 1997: 518) und übertragen bestimmte partikulare Interessen. Dabei gehen liberale Intergouvernementalisten gerade nicht davon aus, dass ein homogenes, alle Interessen gleichermaßen vertretendes Präferenzpaket verfolgt wird, sondern vielmehr, dass durchaus die Interessen einiger weniger entscheidend sein können (Moravcsik 1997: 518).

Für die im vorherigen Teil aufgeworfenen Fragen bedeutet dies: Sowohl die Entscheidung eine Kommissionsempfehlung als regulativen Rahmen, als auch das im Dokument stark ausgeprägte Element der Selbstregulierung unter Einbeziehung aller Stakeholder sollte den Präferenzen der mächtigsten Mitgliedstaaten entsprechen. Daher sollte sich der Wunsch nach einer Form von koordinierter Selbstregulation sowohl in den Äußerungen der wichtigsten Mitgliedstaaten, also Deutschland, Frankreich und Großbritannien finden. Außerdem müsste gezeigt werden, dass die Mitgliedstaaten zu diesem Zweck auf die Kommission als formellem Träger der Empfehlung eingewirkt haben, um eine Regulierung in ihrem Sinne zu erreichen.

Im Hinblick auf die RFID-Empfehlung ist hervorzuheben, dass die Initiative der Kommission, zumindest nicht mit Hilfe offizieller Kommunikationskanäle, auf die Forderung der Regierungen der Mitgliedstaaten zurückging. Zwar informierten sich Länder wie Deutschland frühzeitig bei entsprechenden nationalen Stellen über die datenschutzrechtlichen und anderen Probleme mit RFID (z.B. Bundesamt für Sicherheit in der Informationstechnik 2004), doch kam es weder national noch auf Ebene der EU im Rat zu Versuchen, eine Regulation der RFID Technologie anzustoßen. Erst die deutsche EU Ratspräsidentschaft 2007 organisierte eine Konferenz zu diesem Thema namens „RFID: Towards the Internet of Things“. Dieser ging jedoch zeitlich der Mitteilung der Kommission zur „Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem ordnungspolitischen Rahmen“ (Europäische Kommission 2007) voraus.

Somit lässt sich das Aufgreifen des Themas RFID und die Art der Konsultation unter weiter Einbeziehung der Stakeholder nicht aus den nationalstaatlichen Präferenzen oder der Initiative derselben ableiten. Vielmehr vertrat die deutsche Bundesregierung den Standpunkt, dass für einen Umgang mit den Datenschutzproblemen das bestehende Recht samt einer freiwilligen Selbstkontrolle durch die Industrie ausreichend wäre und daher zunächst keine regulativen Schritte seitens ihrer selbst benötigt würden¹⁸ (Deutscher Bundestag 2008: 14f). Damit erschließt sich auch die anfängliche Inaktivität der Bundesregierung: Sie hatte kein Interesse an einer Regulierung durch den Gesetzgeber, weder national noch auf Ebene der EU. Diese Position wurde von der Regierung noch einmal in einem Reflection Paper

¹⁸ „Es erscheint vorzuzugewürdig, zumindest zum gegenwärtigen Zeitpunkt auf eine gesetzliche Regelung zu verzichten und dem Markt zunächst die Chance zur Selbstregulierung zu lassen.“

zur von Frankreich organisierten Folgekonferenz „Internet of Things – Internet of the Future“ bestätigt¹⁹ (BMWi 2008: 4).

Auch dies steht in einem Kontrast zu den Ergebnissen des Regulierungsprozesses. Denn obwohl es zu keiner verbindlichen Regulierung in Form von hierarchischer Steuerung durch Gesetze kam, beinhaltet die Kommissionsempfehlung gewichtige Elemente der Regelsetzung und Umsetzung durch die Industrie, aber auch Datenschützer, Vertreter der Zivilgesellschaft, sowie der Kommission selbst²⁰. Damit geht sie eindeutig über eine freiwillige Selbstverpflichtung hinaus. Dieses Ergebnis stellt somit den Einfluss der Mitgliedstaaten auf das Ergebnis in Frage, denn auch die Regierung Großbritanniens forderte von der Kommission zumindest offiziell keine Regulation ein, sondern sprach sich für Selbstregulierung in Form von der Industrie selbst entwickelten Codes of Conduct aus (Parliamentary Office of Science and Technology: 4). Weiterhin kam es auch zu keiner Antwort des Europäischen Rats auf die Mitteilung der Kommission vom März 2007 (Europäische Kommission 2007). Allein der europäische Datenschutzbeauftragte veröffentlichte eine Stellungnahme zur selbigen (Europäischer Datenschutzbeauftragter 2008).

Anders erscheint der Einfluss der Mitgliedstaaten auf das gewählte Regulierungsinstrument zu bewerten zu sein. Denn der augenscheinliche Unwille vor allen Dingen Deutschlands und Großbritanniens eine verbindliche Steuerung über Gesetze zu wählen um den Einsatz von RFID zu regulieren bedeutete für die Kommission auch, dass ihr der Weg einer Regelsetzung mit Hilfe einer durch den Rat und das Parlament abzusegnenden Richtlinie erschwert wurde. Denn ein härteres Steuerungsinstrument wäre nicht und wenn überhaupt äußerst langwierig gegen die gemeinsame Ablehnung durch die großen Mitgliedstaaten erreichbar gewesen.

Aus diesen Überlegungen und empirischen Befunden ergibt sich, dass die vom liberalen Intergouvernementalismus als besonders zentral identifizierten großen Mitgliedstaaten wenig Einfluss auf die Inhalte der Empfehlung genommen haben. Weder entsprechen die Ergebnisse, vor allem die koordinierte Selbstregulierung der Stakeholder, der geäußerten Präferenz wichtiger Mitgliedstaaten wie Deutschland und Großbritannien, noch reagierten sie, zumindest für Außenstehende nachvollziehbar, durch politischen Druck auf die Kommission als diese das Thema RFID Regulierung aufbrachte und in der Mitteilung von 2007 ihre Überlegungen und Pläne für das weitere Verfahren mitteilte.

Zusammenfassend lässt sich somit sagen, dass die Wahl einer Empfehlung durchaus von den Präferenzen der Mitgliedstaaten beeinflusst wurde. Die Inhalte der Empfehlung dagegen decken sich weder mit den von Deutschland und Großbritannien bevorzugten freiwilligen Selbstregulierung, noch lassen sich Indizien einer Einflussnahme durch die Mitgliedstaaten auf den politischen Prozess der Regelsetzung finden.

4.2 Neofunktionalismus

Auch wenn der Funktionalismus mehrfach totgesagt wurde²¹, werden Elemente der Theorie bis heute in verschiedenen Bereichen der Europaforschung mit Erkenntnisgewinn angewandt (Stone Sweet/Sandholtz 1997, Jabko 1999). Kern der Theorie sind einerseits Interessengruppen, in den Mitgliedstaaten

¹⁹ „To the greatest extent possible, the necessary data protection measures should be taken in the form of voluntary commitments by industry.“

²⁰ S.o.

²¹ Unter anderem von seinem Begründer selbst (Haas 1975), aber auch von anderen wichtigen Integrationsansätzen (Moravcsik 1993: 475f)

sowie transnational organisiert, die regionale Integration bzw. europaweite Regulierungen bestimmter Politikbereiche fordern. Dem liegt die Überzeugung zu Grunde, dass bestimmte Probleme regional besser bewerkstelligt werden können als national, weswegen verschiedene Interessengruppen eine Übertragung der Entscheidungskapazitäten auf die EU Ebene fordern. Die Identifikation einer Nachfrageseite durch die Theorie von nichtstaatlichen Akteuren geht einher mit supranationalen Akteuren (Kommission, Europäischer Gerichtshof oder Parlament), die über ein gewisses Maß an Unabhängigkeit verfügen und ihre Kompetenzen erfolgreich für die Erfüllung ihrer eigenen Ziele und Überzeugungen einsetzen, die nicht immer im Sinne der Mitgliedstaaten sein müssen (Choi / Caporaso 2002: 485f; Jabko 1999:476ff). So kann es der Kommission gelingen, immer weitere Politikfelder zu vergemeinschaften, auch wenn dies von den Mitgliedstaaten nicht vorgesehen war. Dies gelingt ihr vor allem dann, wenn sie mit transnationalen Akteuren eine Koalition eingeht (Heritier 2001) und bereits ähnliche Politikbereiche supranationalisiert wurden. Die fortschreitende Supranationalisierung wird außerdem durch spill-overs herbeigeführt: Sind erst einmal einige Politikfelder europaweit geregelt und vereinheitlicht, so wird es ökonomisch und politisch sinnvoll, auch andere Bereiche zu supranationalisieren.

Damit ein neofunktionalistischer Erklärungsansatz die beiden im vorherigen Teil identifizierten Befunde der weichen Steuerung durch eine Regulation einerseits und der Steuerung über die freiwillige Teilhabe und Umsetzung durch die Stakeholder andererseits erklären kann, müssten folgende Befunde erbracht werden: Sollte die Kommission maßgeblichen Einfluss gehabt haben, so müssten sich die Ergebnisse erstens weitestgehend mit dem decken, was die Kommission präferierte und wofür sie sich eingesetzt hat. Zweitens müsste die Kommission das Thema RFID und Datenschutz selbst aufgebracht haben und im Sinne ihrer Präferenzen vorangetrieben haben²². Diese sollte im Sinne des Neofunktionalismus auf eine Ausweitung der supranationalen Ebene hinauslaufen, was bedeuten könnte, dass entweder ihr oder anderen supranationalen Akteuren, so z.B. dem Europäischen Parlament oder dem Europäischen Datenschutzbeauftragten wichtige Aufgaben bei der Bearbeitung der RFID Technologie übertragen werden (vergl. Jabko 1999:476ff).

Die Europäische Kommission thematisierte das Thema RFID, wie bereits erwähnt, erstmals auf der CeBIT 2006. Von Beginn an beanspruchte die Kommissarin für Informationsgesellschaft und Medien Viviane Reding eine Rolle für ihre Organisation bei der politischen Bearbeitung der datenschutzrechtlichen Bedenken²³. Auch hielt sie es für eine gesteigerte Erwartungssicherheit aller Wirtschaftsteilnehmer für notwendig, dass ein Prozess der politischen Festlegung angestoßen werden sollte²⁴ und dass dieser Prozess nicht fragmentarisch, sondern europaweit und unter Beteiligung auch außer-europäischer Stakeholder stattfinden sollte²⁵. Folglich lässt sich im Sinne des Neofunktionalismus festhalten, dass die Kommission auf ihr eigenes Bestreben hin aktiv wurde, um sich dem Thema RFID

²² Hiermit folge ich Newmans Überlegung bezüglich des Verhaltens der Kommission im Sinne des Neofunktionalismus (Newman 2008:107f)

²³ “We do listen to those people who say they are concerned about the capability of RFID technology for the thorough, automatic, and widespread surveillance of our daily lives. And it is our duty to respond to these concerns” (Reding 2006: 4).

²⁴ “These are fundamental issues on which we have to give citizens, consumers and organisations the legal certainty that their rights are protected, so that they can take up RFIDs with confidence. If it requires legal measures to build this confidence I will be willing to take them. The business opportunities of RFID can only be built on a basis of mutual trust.”

²⁵ “We are at risk of a fragmented approach to RFID. Now is the right time to think about these issues. This is why I am encouraging a wide ranging discussion involving all European stakeholders – and also beyond Europe.”

anzunehmen. Hierbei handelte sie, wie in 4.2.1 ausgeführt, nicht als Handlanger der Mitgliedstaaten. Auch einige Industrieverbände waren überrascht, dass die Kommission eine teilweise recht weitreichende Regulierung, wie in der Kommissionsmitteilung angedeutet, in Erwägung zog (Interview mit einem Vertreter eines Mittelstandverbandes).

Allerdings war die Position der Europäischen Kommission seit der ersten Benennung der RFID Technologie als datenschutzrelevant einem starken Wandel unterzogen: Während Kommissarin Reding noch auf der CeBIT im März 2006 meinte, dass sie eine Gefährdung der fundamentalen Rechte der Bürger unter keinen Umständen zulassen würde²⁶ und falls notwendig auch legislative Maßnahmen ergreifen würde²⁷ und diese Position sieben Monate später noch einmal wiederholte²⁸, hatten die Formulierungen auf der CeBIT des folgenden Jahres einen deutlich anderen Charakter. Nun betonte sie, dass die Kommission keine verbindlichen Regelungen mehr plane, sondern vorerst eine Selbstregulierung durch die Industrie ausreichend sei (RFID im Blick 2007). Selbes kommt auch in der Mitteilung der Kommission zur RFID Technologie zum Ausdruck. Hier heißt es, dass die Kommission prüfen werde, „welche Alternativen es für die Ausräumung der Bedenken und die Lösung der Probleme gibt“, dazu werde sie das „Gespräch mit allen Beteiligten suchen“ (Europäischen Kommission 2007a: 10). Dies deutet stark darauf hin, dass sich die Kommission zum Zeitpunkt der Mitteilung, also im März 2007, noch nicht festgelegt hatte, was die Art der Regulierung und den Inhalt derselben betrifft.

Die Einsicht, dass sich die Kommission im Spannungsfeld zwischen wirtschaftlichen Potentialen und dem Schutz der Privatsphäre der Unionsbürger nicht eindeutig positionierte, wurde auch von einem Interviewten angesprochen. Dieser sagte: „[D]aher schwankt die Kommission zwischen wie wichtig solche Innovationen für Europa sind und sie sich frei entfalten sollen, um dann im nächsten Satz zu sagen, aber trotzdem müssen wir den Bürger schützen“ (Interview mit Vertreter der Industrie).

Dass sie sich dennoch darauf festgelegt hatte, eine „Empfehlung zu Grundprinzipien [zu] veröffentlichen, die von den Behörden und anderen Beteiligten im Zusammenhang mit der RFID-Nutzung anzuwenden sind“ (Europäischen Kommission 2007a: 10) geht aus der Mitteilung hervor. Ob darüber hinaus jedoch eine Reform der Datenschutzrichtlinie für elektronische Kommunikation notwendig werden würde, gälte es dabei zu prüfen (Europäischen Kommission 2007a: 10f). An der Zielvorgabe der Kommission, sich der RFID Technologie regulatorisch anzunehmen und dies zunächst in Form einer Kommissionsempfehlung, hielt diese auch nach der Mitteilung im Frühjahr 2007 und dem Ende der inhaltlichen Arbeit im Oktober 2008 fest. So sprach ein Vertreter der Zivilgesellschaft in einem der Interviews davon, dass von Beginn an feststand, dass die Kommission plante, eine Empfehlung zu veröffentlichen²⁹.

Auch stand fest, dass die Kommission in der Empfehlung auf staatliche, aber auch nichtstaatliche Akteure abzielen würde. Dies kommt in der Mitteilung der Kommission vom März 2007 zum Ausdruck, in der es

²⁶ “Let me be clear: I will not see the liberty of citizens and their fundamental rights being compromised” (Reding 2006a: 5).

²⁷ “This additional feedback will be analysed and the Commission will report on it in a Communication to be issued by the end of 2006. In the Communication I will outline concrete any follow-up steps that are needed, including legislative measures where necessary” (Reding 2006a: 5).

²⁸ “We have to act now because the RFID technology is about to become very widely used. And there are tremendous potential benefits both for economy and society, in particular in Europe where we have a strong RFID potential if we manage to create the playing field and clear rules of the game. If this requires an updating of the legal framework then I am prepared to act” (Reding 2006b: 3).

²⁹ “Nein, dass die Struktur einer Empfehlung und einer Mitteilung geben wird das war von Haus aus klar, also das war der Plan der Kommission. Auch dass sich das eine mit RFID und das andere mit dem Internet der Dinge beschäftigen wird.“ (Interview mit einem Vertreter der Verbraucherschutz-NGOs).

heißt: „Ende 2007 wird die Kommission eine Empfehlung zu Grundprinzipien veröffentlichen, die von den Behörden und anderen Beteiligten im Zusammenhang mit der RFID-Nutzung anzuwenden sind“ (Europäische Kommission 2007: 10).

Weniger eindeutig war allerdings die inhaltliche Ausgestaltung der Empfehlung selbst. Neben der bereits diskutierten Unentschlossenheit, sich auf einen Standpunkt festzulegen, brachte die Kommission auch im Laufe der inhaltlichen Ausgestaltung gegenüber der einberufenen Interessengruppe immer wieder neue Überlegungen vor, von denen manche wieder verworfen wurden während andere ihren Weg in das Abschlussdokument fanden. So stellte die Kommission beispielsweise in der Interessengruppe andere Branchen vor, die neben dem Einzelhandel eine gesonderte Sektion erhalten sollten. Auf Grund des Widerstandes von Teilen der Interessengruppe blieb es dann bei spezifischen Vorgaben für den Einzelhandel³⁰.

Das Experimentieren mit verschiedenen Inhalten und Regulierungsverfahren legt nahe, dass die Kommission inhaltlich wenig gefestigt war und erst im Laufe der Gespräche zu den Inhalten kam, die in die Empfehlung aufgenommen werden sollten.

Zusammenfassend betrachtet lässt sich nicht abstreiten, dass die Kommission einen wesentlichen Akteur bei der Entstehung der Regulierung der RFID Technologie in Form einer Empfehlung darstellte. Denn obwohl die untersuchten Mitgliedstaaten Deutschland und Großbritannien eher eine freiwillige Selbstregulierung forderten, begann die Europäische Kommission und hier spezifischer das DG Informationsgesellschaft und Medien das Thema aufzugreifen und eine Regulierung, notfalls auch über hierarchische Steuerung in Aussicht zu stellen. Gleichzeitig zeigen die verschiedenen vorgebrachten Äußerungen von Kommissionsmitgliedern und die RFID-Mitteilung aber, dass sich die Kommission sowohl was die Ziele der Regulierung betraf (Wirtschaft vs. Datenschutz) als auch was die Wahl der Mittel anging (Empfehlung vs. Empfehlung + Reform der E-Privacy Richtlinie) noch nicht festgelegt war. Auch die Inhalte der Empfehlung standen, wie das Beispiel der spezifischen Vorgaben für Sektoren zeigte, noch nicht fest, sondern entwickelten sich erst im Laufe der Zeit. Allein dass eine Empfehlung erscheinen sollte und dass sie Handlungsvorgaben neben staatlichen Stellen auch für „andere“ Akteure umfassen sollte, schien von Kommissionsseite zu Beginn der Verhandlungen fest zu stehen. Daher lässt sich auch festhalten, dass neofunktionalistische Erklärungsansätze, die mit dem Aktivismus der Kommission argumentieren, die vorliegenden Ergebnisse nur bedingt erklären können. Denn es fehlt in der Kommissionsempfehlung erstens an einer starken Betonung supranationaler Regulierungsmechanismen und zweitens verfügte die Kommission zu Beginn der Verhandlungen im wesentlichen noch nicht über klar definierte Ziele, Vorstellungen davon wie sie diese erreichen wollte und wie genau die Inhalte der Empfehlung aussehen sollten.

Es lässt sich somit eine politische Unentschlossenheit feststellen, die von anderen Akteuren hätte genutzt werden können, um gewichtigen Einfluss auf die Regulierung zu nehmen.

³⁰ „The recommendation is generic and has a subsection on retail environments. We discussed with the expert group whether other subsections would make sense or not and if they are indeed a special case and if there is something else the generic case to say about it. And well, as you can obviously deduce the answer was no” (Interview mit einem Mitarbeiter der Kommission).

4.3. Transnationale und transgouvernementale Akteure als wirkmächtige Teilnehmer

Damit erscheint es sinnvoll zu überprüfen ob und wenn ja wie andere Akteure Einfluss auf die Empfehlung nehmen konnten. Hierfür bietet die Forschung um den Einfluss transnationaler und transgouvernementaler Akteure einige als wesentlich angenommene erklärende Variablen.

4.3.1 Zugang transnationaler und transgouvernementaler Akteure

Autoren wie Newman betonen, dass für eine erfolgreiche Beeinflussung der politischen Entscheidungsprozesse in der EU ein gut funktionierendes Netzwerk, verstanden als geregelte und intensive Interaktion verschiedener Akteure zu einem bestimmten Themenkomplex, aus Entscheidern und den Interessengruppen bestehen muss (Newman 2008 122ff). Hierbei rekurriert Newman vor allem auf dem was von vielen Autoren, als *access*, also Zugang zu den Entscheidungsprozessen, beschrieben wird (für einen Überblick vergl. Coen 2007)

Besonders die von der Kommission berufene Interessengruppe, mit der sie sich über einen Zeitraum von zwei Jahren monatlich traf, bot hierfür eine Möglichkeit. Die Gruppe wurde dabei kurz nach der Mitteilung im Juli 2007 eingesetzt und begleitete die Kommission bis zum März 2009.

In der Gruppe vertreten waren neben Konsumentengruppen wie dem BEUC (Bureau Européen des Unions de Consommateurs), der ANEC, die speziell die Interessen der Konsumenten bei Standardisierungen in den Blick nehmen, dem GMB, einem britischen Gewerkschaftsdachverband, UNI, als aggregiertem Vertreter von 900 nationalen Gewerkschaften, und schließlich der EDRi (European Digital Rights), ein Dachverband für NGOs mit einem Fokus auf Datenschutz. Auch die nationalen Datenschützer waren durch ihr französisches Pendant, die Commission nationale de l'informatique et des libertés (CNIL) vertreten.

Weiterhin war die Industrie vertreten durch einzelne Großunternehmen und Dachverbände. Direkt Teil nahmen die folgenden Unternehmen: Carrefour, Deutsche Post World Net, NXP und SAP, das RFID Centre UK und das Traceability Centre. Die Industrie war auch durch die europäischen Unternehmensverbände CLECAT, COCIR, EFPIA und EGA sowie des für das Thema RFID gegründete Informationsforum RFID involviert. Auch die Standardisierungsorganisationen CEN, GS1's EPCglobal, ETSI und das ICT Standards Board nahmen an den Beratungen Teil.³¹

Für die Mitglieder der Interessengruppe, inklusive der Verantwortlichen in der Kommission, war es dabei normal, sich gegenseitig beständig zu kontaktieren. Einer der Interviewpartner ging soweit zu sagen, dass im Netzwerk derer, die sich mit den datenschutzrechtlichen Problemen der RFID Technologie beschäftigten ob der geringen Zahl an Teilnehmern eine Art „Community-Denken“ bestünde, dass es ermöglichte, auch auf „kurzem Dienstweg“ miteinander zu kommunizieren (Interview mit einem Industrievertreter).

Auch genossen die an der Interessengruppe beteiligten Akteure einige Privilegien. Die Kommission teilte mit ihnen im monatlichen Turnus ihre Überlegungen zur Art der Regulierung, die ihr vorschwebte, mit und legte Wert darauf, Feedback zu erhalten. Das so geteilte Wissen war dabei nicht allgemein zugänglich,

³¹ Tabelle 2: Mitglieder der Expertengruppe im Anhang bietet einen Überblick über alle Teilnehmer an der Expertengruppe und beschreibt bei aggregierten Akteuren die Zwecke und Ziele der Organisation.

da die Besprechungen vertraulich waren. Auch wurde der Gruppe einige Wochen vor der Einleitung der 2. öffentlichen Konsultation die Entwurfsfassung der Empfehlung vorgestellt und es wurde den Gruppenteilnehmern die Möglichkeit gegeben, zuerst Stellung zu beziehen (Interview mit einem Mitarbeiter der Kommission).

Generell war es üblich, dass die Kommission ihre Vorstellungen bezüglich der Empfehlung mit den Mitgliedern der Gruppe teilte und von diesen in so genannten „one-pagern“, die oftmals in Gruppen zu erarbeiten waren, Feedback erhielt. Dabei wurden alle für die Empfehlung relevanten Themengebiete angesprochen und sehr offen diskutiert. Generell wurde die Stimmung dabei von allen Interviewten als sehr offen und argumentativ beschrieben.

Der interviewte Mitarbeiter der Kommission verglich die Arbeit mit der Interessengruppe aus Sicht seiner Institution mit einer Laborsituation: „Rather than integrating the feedback we used them, if you allow me the comparison like a laboratory of opinion“ und weiter: “We were trying ideas. We were internally thinking and reflecting on ideas that had been either suggested by one of them or we were refining our own ideas, and we used those meetings to ask them questions” (Mitarbeiter der Kommission).

Insgesamt kann somit von einem sehr hohen und formalisierten Maß an *access* seitens der Mitglieder der Interessengruppe gesprochen werden. Dabei kam es nicht nur zu einer regelmäßigen Konsultation während des gesamten Zeitraums der Entstehung der Empfehlung. Darüber hinaus war auch die Arbeitsatmosphäre in der Gruppe sehr kollegial und argumentativ. Schließlich bestand auch ein Interesse seitens der Kommission, sich die Positionen der Interessengruppen anzuhören und mit deren Antworten zu experimentieren. Dies deutet stark darauf hin, dass es der Kommission nicht nur darum ging, pro forma Konsultationen zu betreiben, sondern ein tatsächliches Interesse an den Positionen der Beteiligten bestand.

Das Bestehen von Zugang allein kann allerdings noch nicht ausreichen, um einen kausalen Zusammenhang zwischen den Präferenzen der nichtstaatlichen Akteure und den Endergebnissen herzustellen. Zugang stellt eine notwendige Bedingung dar, ist für eine Beeinflussung allerdings nicht hinreichend. Daher bedarf es weiterer erklärender Elemente.

4.3.2 Bedürfnis nach Expertise

Vielfach, so unter anderem von Newman (2008: 120f) oder Adler und Haas (1992), wird auf die Bereitstellung von Expertise für eine besonders effektive Einflussnahme abgehoben. Dieser Annahme liegt zu Grunde, dass viele Themen, die politisch bearbeitet werden, erstens hoch komplex sind und zweitens die bestehenden Strukturen nicht ausreichen, um eine adäquate Lösung für das Problem zu finden. Wird dann Expertise bereitgestellt, so geht damit auch eine Übertragung bestimmter Ansichten von Ursache und Wirkung, normativen Überzeugungen und Epistemologie einher (Adler / Haas 1992).

Da es sich bei der RFID Technologie um eine noch nicht vollends entwickelte und eingesetzte Technologie handelt, herrscht allgemein eine gewisse Unsicherheit bei der Diskussion um wirtschaftlichen Nutzen einerseits, und der tatsächlichen Gefährdung der Privatsphäre andererseits (BSI 2004). Auch wird für eine präzise Einschätzung der Anwendbarkeit des gängigen Rechts und die Möglichkeit der Verwendung so genannter Technologien zum Schutz der Privatsphäre (Europäische Kommission 2007c) großes und sehr spezifisches Fachwissen vorausgesetzt.

Daher ist davon auszugehen, dass die Kommission mit ihren teilweise beschränkten Mitteln nicht in der Lage ist, ohne Hilfe von Außen die nötige Expertise zu generieren. Dabei bieten sich der Kommission allerdings auch Möglichkeiten, jenseits der Interessengruppen Wissen zu erlangen. So wurde beispielsweise in der Interessengruppe mehrfach von der Möglichkeit Gebrauch gemacht, externe Experten einzuladen. Darunter waren Sachverständige des BSI, Mitglieder anderer Generaldirektionen, aber auch Experten aus den Vereinigten Staaten und Japan. Darüber hinaus griffen die mit der Empfehlung beschäftigten Kommissionsmitarbeiter auch stark auf die Expertise der Rechtsabteilung und anderer Generaldirektionen zurück (Interview mit Kommissionsmitarbeiter).

Allerdings stellten zu bestimmten Themen auch die Interessenvertreter in der Interessengruppe Studien vor (Interview mit Industrievertreter). Weiterhin verfügten einige der Teilnehmer an der Interessengruppe über großen Sachverstand bezüglich der technischen, juristischen und politischen Fragestellungen, die es für eine sinnvolle Regulierung der RFID zu berücksichtigen gilt. Vor allem die Datenschutzbeauftragten, vertreten als Teilnehmer durch CNIL und als Beobachter durch den europäischen Datenschutzbeauftragten, verfügen Zweck ihres Amtes über ein hohes Maß an Expertise und Anerkennung. Weiterhin besitzen auch die Industrievertreter auf Ebene der betrieblichen Umsetzung und der Einschätzung der ökonomischen Machbarkeit Wissen, das sie exklusiv einbringen können. Schließlich sind auch die vertretenen Standardisierer im Besitz technischen Know-hows, das ihnen was das Wissen über Standards betrifft fast ausschließlich zur Verfügung steht.

Im Interview mit einem Kommissionsmitarbeiter kam die letztlich technokratische Idee, dass die Konsultation der Interessengruppen für eine möglichst gute Regulierung nötig waren, deutlich zum Tragen. So sprach die interviewte Person im Zusammenhang mit der Interessengruppe davon, dass „[W]e needed them to come up with those answers. We would not have come up with those answers by ourselves.“

Die Expertise, die von den Mitgliedern der Interessensgruppe bereit gestellt wurde, scheint somit von der Kommission bereitwillig aufgenommen worden und in die Empfehlung eingegangen zu sein. So sprach derselbe Kommissionsmitarbeiter davon, dass ein komplettes Element der Regulierung fast ausschließlich von den Datenschützern eingebracht worden sei³².

4.3.3. Anerkennung durch nichtstaatliche und transgouvernementale Akteure

In der Debatte um New Modes of Governance (NMG) wird betont, dass neuere Formen des Regierens, in denen es weniger um harte Steuerung als vielmehr um so genanntes ‚soft law‘ geht, nichtstaatliche Akteure sehr viel stärker in die Umsetzung, aber auch schon in die Konzeption von NMGs einbeziehen um so die Akzeptanz der Regeln zu erhöhen. Empfehlungen, wie sie die Kommission verwendet, ähneln dabei in ihrer Funktionsweise und ihrer Entstehungsart jenen NMG, wie sie seit einigen Jahren in den Internationalen Beziehungen und besonders der Europäisierungsforschung beobachtet werden. Nach Kohler-Koch und Rittberger (2006: 36f) lassen sich NMGs mit Hilfe dreier Kriterien identifizieren: 1. Die Instrumente verlassen sich auf ‚soft law‘ anstelle harter Steuerungen über Verordnungen und Richtlinien. 2. Es kommt zu einem Aushandlungsprozess, der zwischen öffentlichen und privaten Akteuren

³² “One opinion [of the Data Protection Authorities] is almost exclusive to the Recommendation” (Interview mit einem Mitarbeiter der Europäischen Kommission).

abgesprochen wird und im Sinne des Subsidiaritätsprinzips von Mitgliedstaaten umgesetzt wird. 3. Alle wesentlichen Akteure sind in die Definition der Ziele und Instrumente einbezogen.

Aus diesen Überlegungen ergibt sich, dass nichtstaatliche und transgouvernementale Akteure auf die Empfehlung der Kommission zu den datenschutzrechtlichen Implikationen Einfluss nehmen konnten, weil ihre Anerkennung notwendig wurde, um mit Hilfe einer weichen Steuerung von Seiten der Kommission zum Erfolg zu kommen.

Damit wird die bereits zitierte Aussage des Kommissionsmitarbeiters, nach der die Interessengruppe eine Art Laboratorium für ihre Ideen war, in ein anderes Licht gerückt: Die Kommission versuchte durch die starke Einbeziehung der nichtstaatlichen Akteure, mit monatlichen Treffen, einer barrierefreien Kommunikation und der Einbindung aller vertretenen Interessengruppen zu einer anerkennungswürdigen Regulation zu kommen. Damit erhielten nichtstaatliche Akteure die Möglichkeit, Teile der Empfehlung in einem konsensualen Prozess mit zu gestalten. Hierfür spricht, dass obwohl die verschiedenen Interessengruppen zu Beginn sehr gegensätzliche Positionen einnahmen, schlussendlich alle die Kommissionsempfehlung lobten und sie als akzeptabel beschrieben: Die Vielzahl an teilweise sehr gegensätzlichen Akteuren führte dabei zu einer zunächst sehr unterschiedlichen Interessenstruktur der in der Gruppe vertretenen Akteure (Interview mit Vertreter einer Datenschutzorganisation, Interview mit einem Vertreter eines in der Interessengruppe vertretenen Industrieverbandes). Während Industrievertreter zunächst die Einstellung vertraten, dass die gängigen datenschutzrechtlichen Regeln ausreichen, waren die Datenschützer der Ansicht, dass die Gefahren für die informationelle Selbstbestimmung dadurch nicht ausreichend bedacht würden. Dies führte gerade zu Beginn der Arbeit in der Interessengruppe „zu heftige[n] Diskussionen zwischen denen, die RFID für eine förderungswürdige Technologie halten und denen, die RFID als Mittel zur Überwachung von Individuen ansehen und zum Monitoring von sozialem Verhalten“ (Interview mit einem Vertreter eines in der Interessengruppe vertretenen Industrieverbandes).

Demgegenüber fallen die Bewertungen der Empfehlung durch alle beteiligten Interessenverbände eindeutig positiv aus. So betonte das Informationsforum RFID in einer Pressemitteilung zur Empfehlung, dass die Ergebnisse „grundsätzlich begrüßt würden“ und weiter: „[P]ositiv würden seitens der Anwenderindustrie, deren Interessen das Informationsforum vertritt, insbesondere die Bemühungen der EU-Kommission um eine Balance zwischen den Interessen der Verbraucher und der Wirtschaft bewertet“. (Informationsforum RFID 2009). Auch ein interviewter Vertreter der Zivilgesellschaft betonte, dass die Empfehlung bei Umsetzung durch die beteiligten Akteure einen sinnvollen Mittelweg zwischen einer Ermöglichung von wirtschaftlicher Nutzung auf der einen und Datenschutz auf der anderen darstellt (Interview mit einem Vertreter der Zivilgesellschaft).

Auch das Verhalten der Kommission zeigt deutlich, dass es ihr um eine größtmögliche Akzeptanz durch transnationale und transgouvernementale Akteure ging: Zwei öffentliche Konsultationen und einmal monatlich stattfindende Treffen mit den Interessengruppen sind ein hohes Maß an Einbindung³³. Interessant erscheint, dass die Kommission, nachdem sie eine erste Entwurfsfassung mit den Mitgliedern der Interessengruppe besprochen hatte und nachdem sie bereits einmal eine öffentliche Konsultation durchgeführt hatte, diesen Entwurf noch einmal von einer weiteren öffentlichen Konsultationsrunde

³³ Leider fehlen für einen Vergleich valide Daten zur sonstigen Einbindungspraxis.

kommentieren ließ. Die Äußerung, dass die Kommission für die Bearbeitung dieser zweiten Konsultation noch einmal vier Monate benötigte (Interview mit einem Kommissionsmitarbeiter) legt nahe, dass sie sich intensiv mit dem Feedback beschäftigte.

Dies geht deutlich über ein Interesse allein an der technokratischen Vorstellung der bestmöglichen Regulierung hinaus und zeigt, dass die Kommission auch auf politische Anerkennung seitens der Interessengruppierungen abzielte. Dazu war sie bereit, auch Teile der Empfehlung entsprechend so zu verfassen, wie es sich die nichtstaatlichen und transgouvernementalen Akteure wünschten. Die bereits angesprochene Nichtaufnahme weiterer sektorenspezifischer Vorgaben, wie sie von der Kommission angedacht worden war, und die Aufnahme eines Elements³⁴, das von den Datenschützern vorgeschlagen worden war, stehen hierfür sinnbildlich.

Zusammenfassend lässt sich somit argumentieren, dass die Kommissionsempfehlung maßgeblich durch nichtstaatliche und transgouvernementale Akteure beeinflusst wurde. Dies bezieht sich sehr viel mehr auf die Inhalte der Regulierung als auf die Wahl einer Empfehlung als Regulierungsinstrument. Denn für letzteres, wie gezeigt wurde, sind einerseits die Präferenzen der Mitgliedstaaten, nicht regulieren zu wollen und der Europäischen Kommission, dennoch Regeln zu schaffen, verantwortlich.

5. Schluss

Die „Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID- gestützten Anwendungen“ stellt einen zentralen Baustein im datenschutzrechtlichen Umgang mit RFID dar. In ihr kommen stark ausgeprägte Formen von Regulation durch die Stakeholder selbst vor. Hiermit betritt die Empfehlung für den Umgang mit datenschutzrechtlich relevanten Technologien Neuland.

Wie versucht wurde zu zeigen, waren nichtstaatliche Akteure aus Industrie und Zivilgesellschaft und die Datenschützer auf Ebene der Mitgliedstaaten und der EU dabei in der Lage, starken Einfluss auf die Kommissionsempfehlung geltend zu machen. Dabei ging es weniger um die Wahl einer Empfehlung als Regulierungsinstrument als vielmehr um die Inhalte die darin zum Ausdruck kommen.

Damit geht die Arbeit über klassische Erklärungsansätze der Integrationsforschung hinaus und zeigt auf, dass unter Umständen auch andere Akteure im System der Europäischen Union ihre Präferenzen zur Geltung bringen können. Mit der Identifikation dreier erklärender Faktoren, nämlich Zugang, die Bereitstellung von Expertise und die Notwendigkeit der Anerkennung der Ergebnisse durch die Interessengruppen, wurde aufgezeigt wie ein solcher Einfluss kausal hergeleitet werden kann. Gerade die Anerkennung sollte im selben Umfang relevanter werden je mehr die Europäische Kommission auf NMGs zurückgreift um ihren Aufgaben nachzukommen.

Damit wird die Untersuchung weiterer Fälle interessant, in denen NMG zum Einsatz kamen und die Umsetzung der Regulierung vom Verhalten nichtstaatlicher und quasi-autonomer transgouvernementaler Akteure abhängt. Denn sollte der in dieser Einzelfallstudie identifizierte Mechanismus bestehen, müssten sich ähnliche Beobachtungen auch in anderen Fällen machen lassen.

³⁴ Worum es sich bei diesem Element handelte, wurde während des Interviews nicht besprochen.

Bibliographie

- Batcheldor, Beth 2007: Audi Uses Semi-Passive Tags to Make TTs, RFID Journal (29.01.2007).
- Boes, Andreas 2005: Informatisierung, in: SOFI; IAB; ISF München; INIFES (Hrsg.):
Berichterstattung zur sozioökonomischen Entwicklung in Deutschland – Arbeits- und
Lebensweisen, Wiesbaden, 211-244.
- Bundesamt für Sicherheit in der Informationstechnik (BSI) 2005: Risiken und Chancen des
Einsatzes von RFID-Systemen, in:
http://www.bsi.bund.de/fachthem/rfid/RIKCHA_barrierefrei.pdf.
- Bundesministerium für Wirtschaft und Technologie 2008: Reflection Paper of the Federal
Government of Germany. From Berlin 2007 to Nice 2008 and Beyond: “RFID – Internet
of Things – Internet of the Future”, in:
http://www.unic.pt/images/stories/publicacoes2/Reflections_on_European_Policy_Outlook_RFID.pdf.
- Choi, Young Jong/ Caporaso, James A. 2002: Comparative Regional Integration, in: Carlsnaes,
Walter/ Thomas Risse/ Simmons, Beth A. (Hrsg.): Handbook of International Relations,
London: Sage, 480-499.
- Coen, David 2007: Empirical and theoretical studies in EU lobbying, Journal of European Public
Policy 14(3), 333–345.
- Deutscher Bundestag 2008: Unterrichtung durch die Bundesregierung. Bericht der
Bundesregierung zu den Aktivitäten, Planungen und zu einem möglichen
gesetzgeberischen Handlungsbedarf in Bezug auf die datenschutzrechtlichen
Auswirkungen der RFID-Technologie, Drucksache 16/7891 (23. 01. 2008).
- Europäischer Datenschutzbeauftragter 2008: Stellungnahme des Europäischen
Datenschutzbeauftragten zu der Mitteilung der Kommission an das Europäische
Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den
Ausschuss der Regionen zum Thema Funkfrequenzkennzeichnung (RFID) in Europa:
Schritte zu einem ordnungspolitischen Rahmen, (KOM(2007) 96), Amtsblatt der
Europäischen Union C 101, 1-11.
- Europäisches Kommission 1990: Commission Communication on the protection of individuals
in relation to the processing of personal data in the Community and information security,
COM(90) 314 final, 13.09.1990.
- Europäische Kommission 2001: European Governance – A White Paper, COM(2001) 428 final.
- Europäische Kommission 2006: RFID Security Data Protection & Privacy, Health and Safety
Issues, Konferenzprogramm, in:
http://www.rfidconsultation.eu/docs/ficheiros/RFID_WS_3_Programme__11May_SM_S_sw2.pdf.
- Europäische Kommission 2007a: Mitteilung der Kommission an das Europäische Parlament, den
Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der
Regionen - Funkfrequenzkennzeichnung (RFID) in Europa: Schritte zu einem
ordnungspolitischen Rahmen, KOM(2007) 96 endgültig.

- Europäische Kommission 2007b: Commission Staff Working Document Results of the Public Online Consultation on Future Radio Frequency Identification Technology Policy "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats". SEC(2007) 312, http://ec.europa.eu/information_society/policy/rfid/documents/rfidswp_en.pdf.
- Europäische Kommission 2007c: Mitteilung der Kommission an das Europäische Parlament und den Rat über die Verbesserung des Datenschutzes durch Technologien zum Schutz der Privatsphäre, KOM(2007) 228 endgültig.
- Europäische Kommission 2008: Commission Staff Working Document. Accompanying document to the Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions. Future networks and the internet. Early Challenges regarding the 'Internet of Things', SEC(2008) 2516, in: http://ec.europa.eu/information_society/eeurope/i2010/docs/future_internet/swp_internet_things.pdf.
- Europäische Kommission 2009a: Empfehlung der Kommission vom 12. Mai 2009 zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID- gestützten Anwendungen, Amtsblatt der Europäischen Union L122, 47-51.
- Europäische Kommission 2009b: Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Internet der Dinge – ein Aktionsplan für Europa, KOM(2009) 278 endgültig (18.6.09).
- Europäische Union 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, Amtsblatt Nr. L 281, 23 November 1995, 31-50.
- Europäische Union 2002: Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, Amtsblatt Nr. L 201, 37-47.
- Europarat 1981: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981, Konvention Nr. 108.
- Farrell, Henry 2003: Constructing the International Foundations of E-Commerce: The EU-U.S. Safe Harbor Arrangement, *International Organization* 57 (2), 277-306.
- FoeBuD 2004: Der Metro Skandal, in: <http://www.foebud.org/rfid/metro>.
- FoeBuD 2009: RFID- Das Problem, in: <http://www.foebud.org/rfid/das-problem>.
- Garstka, Hansjürgen 2003: Informationelle Selbstbestimmung und Datenschutz – Das Recht auf Privatsphäre, in: Schulzki-Haddouti, Christiane (Hrsg.): Bürgerrechte im Netz Bd. 382, Bundeszentrale für politische Bildung, 48–70.
- Haas, Ernst B. (1975) *The Obsolescence of Regional Integration Theory*, Berkeley: Center for International Studies.

- Heisenberg, Dorthée 2005: *Negotiating Privacy – The European Union, the United States and Personal Data Protection*, Boulder: Lynne Rienner.
- Hunt, V. Daniel/ Alber Puglia/ Puglia, Mike 2007: *RFID- A Guide to Radio Frequency Identification*, Hoboken: Wiley.
- Informationsforum RFID 2009: Informationsforum RFID zur Empfehlung der EU-Kommission zu Privatsphäre und Datenschutz bei RFID, in: http://www.presseportal.de/pm/59187/1403785/informationsforum_rfid_e_v, Pressemitteilung vom 12.05.09.
- Moravcsik, Andrew 1991: *Negotiating the Single European Act: National Interests and Conventional Statecraft in the European Community*, *International Organization* 45(1), 19-56.
- Moravcsik, Andrew 1993: *Preferences and Power in the European Community: A Liberal Intergovernmentalist Approach*, *Journal of Common Market Studies* 31 (4), 473-524.
- Moravcsik, Andrew 1997: *Taking Preferences Seriously: A Liberal Theory of International Politics*, *International Organization* 51(4), 513-554.
- Moravcsik, Andrew 1998: *The Choice for Europe. Social Purpose and State Power from Messina to Maastricht*, Ithaca: Cornell University Press.
- Newman, Abraham L. 2008: *Building Transnational Civil Liberties: Transgovernmental Entrepreneurs and the European Data Privacy Directive*, *International Organization* 62, Winter, 103-30.
- O'Connor, Mary Catherine 2009: *Volkswagen de Mexico Employing RFID to Improve Parts Distribution*, *RFID Journal* (20.5.2009).
- OECD 1980: *Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980*.
- OECD, Working Party on the Information Economy 2008: *RFID Applications, Impacts and Country Initiatives*, DSTI/ICCP/IE(2007)13/FINAL.
- Parliamentary Office of Science and Technology 2004: *Postnote. Radio Frequency Identification (RFID) July 2004, Number 225*.
- Rat der Europäischen Union, Europäisches Parlament 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*, Amtsblatt Nr. L 281 vom 23.11.1995, 31–50.
- Rat der Europäischen Union, Europäisches Parlament 1997: *Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation*, Amtsblatt Nr. L 24 vom 30.1.1998, 1-8.

- Rat der Europäischen Union, Europäisches Parlament 2002: Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), Amtsblatt Nr. L 201 vom 31.7.2002, 37–47.
- Reding, Viviane 2006a: The RFID Revolution: challenges and options for action. Rede der Kommissarin für Informationsgesellschaft und Medien auf der CeBIT 2006, Hannover (9.3.2006).
- Reding, Viviane 2006b: RFID: Why we need a European policy EU RFID 2006 Conference: Heading for the Future. Rede der Kommissarin für Informationsgesellschaft und Medien auf der EU RFID 2006 Conference: Heading for the Future, SPEECH/06/597, Brüssel (16. Oktober 2006).
- Reding, Viviane 2007: Grußwort der Europäischen Kommission von Viviane Reding, Kommissarin für Informationsgesellschaft und Medien, in: Bundesministerium für Wirtschaft und Technologie (BMWi): European Policy Outlook RFID, Deutsche Übersetzung des Englischen Originals, Brüssel: Europäische Kommission.
- Regan, Priscilla 1999: Kapitel 10: American Business and the European Data Protection Directive - Lobbying Strategies and Tactics, in: Bennett, Colin J./ Grant, Rebecca (Hrsg.): Visions of Privacy – Policy Choices for the Digital Age, Toronto: Toronto University Press, 199-216.
- RFID im Blick 2007: Auto ID/RFID versprüht Optimismus. Ausgabe 04-07, in: <http://rfid-im-blick.de/Messe-Online/Eingangsbereich/Auto-ID/RFID-verspruht-Optimismus.html>.
- Schweizerisches Bundesamt für Gesundheit 2005: Handlungsbedarf im Zusammenhang mit RFID-Technologie - Bericht in Erfüllung des Postulates 05.3053 Allemann vom 9. März 2005, in: <http://www.bag.admin.ch/themen/strahlung/00053/02644/04794/index.html?lang=de&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVpzLhmfhnappmmc7Zi6rZnqCkkIZ9gneBbKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w==>.
- Sieghart, Paul 1976: Privacy and Computers, London: Latimer.
- Simitis, Spiros 1995: From the Market to the Polis: The EU Directive on the Protection of Personal Data, Iowa Law Review 80, 1994-1995, 445-469.
- Spiegel Online 2008: Chefs spionieren Mitarbeiter deutschlandweit aus, in: <http://www.spiegel.de/wirtschaft/0,1518,547695,00.html> (16.04.08).
- Stone Sweet, Alec/ Sandholtz, Wayne 1998: European Integration and Supranational Governance, Journal of European Public Policy, 4(3), 297-317.
- Stone Sweet, Alec/ Sandholtz, Wayne/ Fligstein, Neil (Hrsg.) 2001: The Institutionalization of Europe, Oxford: Oxford University Press.
- Swedberg, Claire 2009: RFID Plays Crucial Military Role in Middle East, RFID Journal (29.04.2009).

Teknologi Rådet 2006: RFID from production to consumption- Risks and opportunities from RFID-technology in the value chain, in:
<http://whitepapers.zdnet.com/thankyou.aspx?&docid=269727&view=269727&load=1>.

Verbraucherzentrale Bundesverband (VZBV) 2007: Rfid-Technologie: Ohne das Vertrauen der Verbraucher zum Scheitern verurteilt, Pressemitteilung (12.03.2007).

Vereinte Nationen 1990: Richtlinien betreffend personenbezogener Daten in automatisierten Dateien vom 14. Dezember 1990.

Annex

Tabelle 2: Mitglieder der Expertengruppe

Organisation	Art der Organisation
Konsumentenvertretung	
ANEC	Konsumentenorganisation mit Fokus auf Standardisierung
BEUC	Europäische Verbraucherschutzorganisation
GMB	Britische Gewerkschaft
UNI	Gewerkschaftsdachverband
EDRi	Dachverband von Datenschutz-NGOs
CNIL	Französische Datenschutzbehörde
Unternehmensvertretung	
Unternehmen: Carrefour, Deutsche Post World Net, NXP, RFID Centre UK, SAP und Traceability Centre	Europäische Großunternehmen, verschiedene Branchen
Unternehmerverbände: 1. allgemeine Branchenvertretungen: CLECAT, COCIR, EFPIA, EGA, Informationsforum RFID,	CLECAT: Logistikunternehmen COCIR: Medizintechnikunternehmen EFPIA: Pharmazieunternehmen Informationsforum RFID: Deutsche Unternehmen (u.a. Metro Group, DHL, Siemens, T-Systems, Volkswagen, Fraunhofer Institut für Logistik)
Standardisierer	
CEN	Privater Standardisierer
EPCglobal (GS1)	
ETSI	
ICT Standards Board	
Beobachter	
Mitgliedstaaten mit Ratspräsidentschaft: D, F, PT	
Artikel 29 Arbeitsgruppe	Nationale und europäische Datenschützer

Interviews

Die Arbeit stützt sich auf fünf semi-strukturierte Experteninterviews, die im Rahmen ihrer beruflichen Tätigkeiten und ihrer politischen Bearbeitung mit RFID beschäftigt sind. Die Interviews dauerten zwischen 45 und 90 Minuten. Eine Reihe von Experten wurde nach den Interviews erneut angeschrieben um unverständliche Aussagen zu klären.

Folgende Experten wurden interviewt:

Mitglied einer europäischen Datenschutzorganisation. Vertreter einer zivilgesellschaftlichen Datenschutzorganisation bei der EU Expertenkommission.

Mitglied der Europäischen Kommission. Zentraler Vertreter des DG Informationsgesellschaft und Medien an der Konzeption der Mitteilung und der Empfehlung.

Mitarbeiter eines Industrieverbandes. Leitende Rolle im Verband und Vertreter desselbigen in der Expertenkommission.

Mitarbeiter einer Public Affairs Agentur. Mehrjährige Erfahrung mit RFID und der politischen Diskussion um ihre Regulierung. Mitautorschaft in Publikationen zum Thema Regulierung der RFID Technologie auf Ebene der EU.

Verbandsvertreter eines deutschen Mittelstandsverbandes. Leitung eines Konsortiums, das RFID Lösungen für Unternehmen anbietet und umsetzt.

Bei der Auswahl wurde darauf Wert gelegt, dass die Experten sowohl Kenntnis zu den technischen und juristischen Fragestellungen für die RFID Technologie hatten, als auch aktiv in den politischen Diskurs um Fragen des Datenschutzes und der politischen Gestaltung der Technologie eingegriffen haben. Zentral war, eine Auswahl der wesentlichen Akteursgruppen, die an der Policy Formulierung auf Ebene der EU teilgenommen haben, zu gewinnen. Dies gelang teilweise. Neben Vertretern der Industrie und der Datenschützer, konnte auch ein Kommissionsmitarbeiter interviewt werden. Leider gelang es nicht, Vertreter der Mitgliedstaaten zu befragen. Die nationale Herkunft spielte insgesamt eine untergeordnete Rolle; von fünf waren drei Deutsche und zwei Nichtdeutsche vertreten. Vier von fünf Interviews wurden dabei auf Deutsch geführt, eins auf Englisch.