Technische Universität Darmstadt
Fachbereich Rechts- und Wirtschaftswissenschaften
Institut für Rechtswissenschaften
Fachgebiet Öffentliches Recht
Lehrstuhl Prof. Dr. Viola Schmid, LL.M.(Harvard)

Studienarbeit

Informations- und Datenschutzrecht

Deutsches Recht und RFID: Drei Szenarien und die Frage nach neuer Gesetzgebung

von Andreas John

Fachbereich Rechts- und Wirtschaftswissenschaften
Fachrichtung Wirtschaftsinformatik

Gliederung

Glossar und Abkürzungsverzeichnis[1]

BDSG	Bundesdatenschutzgesetz
BGSG	Bundesgrenzschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
CASPIAN	Consumers Against .....
ggf.	gegebenenfalls
HSOG	Hessisches Sicherheits- und Ordnungsgesetz
i.d.R.	in der Regel
i.S.d.	in Sinne des
i.S.v.	im Sinne von
i.V.m,	in Verbindung mit
ICAO	International Civil Aviation Organization
JuSchG	Jugendschutzgesetz
PassG	Passgesetz
PauswG	Personalausweisgesetz
PersAuswMustV	Personalausweismusterverordnung
RFID	Remote Frequency Identification
s.o.	siehe oben
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
USA	United States of Amerika
UWG	Gesetz gegen den unlauteren Wettbewerb
WM	Weltmeisterschaft

[1] Siehe auch Butz, Kirchner (2003): Abkürzungsverzeichnis der Rechtssprache

Literaturverzeichnis

BUTZ, Cornelie (Bearb.) ; KIRCHER, Hildebert (Begr.): **Abkürzungsverzeichnis der Rechtssprache**, 5. völlig neu bearb. und erw. Auflage 2003. Berlin Gruyter, 2003 - ISBN 3 89949 026 6

HEINRICH, Claus: **RFID and Beyond: Growing Your Business Through Real World Awareness**. Vermutl. Hoboken, NJ (USA) : John Wiley & Sons, 2005 - ISBN: 0 7645 8335 2
Hinweis: Der voraussichtliche Veröffentlichungstermin ist im März 2005

IPSEN, Jörn : **Staatsrecht II : Grundrechte**, Siebte, überarbeitete Auflage. Neuwied u.a. : Luchterhand, 2004 – ISBN 3 472 05824 2

MEDERT, Klaus ; Werner Süssmuth: **Pass- und Personalausweisrecht : Kommentar**, 2., überarbeitete Auflage, Köln, Deutscher Gemeindeverlag, 1992 - ISBN 3 555 00899 4

MÜNCH, Ingo (Begr.) ; KUNIG, Philip (Hrsg.): **Grundgesetz-Kommentar**, 5. neubearbeitete Auflage. München : Beck, 2000 – ISBN 3 406 45804 1

RONELLENFITSCH, Michael: **Zweiunddreißigster Tätigekeitsbericht des Hessischen Datenschuzubeauftragten**, 2003

SIMITIS, Spiros (Hrsg.): **Kommentar zum Bundesdatenschutzgesetz**, 5. völlig neu überarbeitete Auflage, Baden Baden : Nomos Verlagsgesellschaft, 2003 - ISBN 3 789 07520 5

TINNEFELD, Marie-Theres ; EHMANN, Eugen ; GERLING, Rainer W.: **Einführung in das Datenschutzrecht**, 4. völlig neu bearbeitete und erweiterte Auflage, München: Oldenbourg, 2004 – ISBN 3 486 27303 5

A Einleitung

Wer genau hinsieht wird erkennen, dass RFID Technik zur Zeit immer mehr in unseren Lebensraum vordringt. In der Geschäftswelt entwickelt sich mit Hilfe von RFID das „Real Time Enterprise“[2]. Im öffentlichen Sektor ist die Anwendung dieser Technik beispielsweise an Reisepässen zu beobachten und letztendlich hält sie auch Einzug in unser privates Leben, denn der Verbraucher steht am Ende der Wertschöpfungskette.
Wir sollten uns auch der Gefahren bewusst sein, denn mehr als je zuvor bietet diese Technik nicht nur die Möglichkeit, Daten zu erheben, sondern verlangt dies auch für ihren effizienten Einsatz. Letztendlich birgt RFID die Gefahr des „gläsernen Menschen“ in sich, dessen digitale Biographie in den Datenbanken der Unternehmen gespeichert sein könnte. Ein guter Grund zu untersuchen, ob und in wie weit das Datenschutzrecht in Deutschland die Privatsphäre des Einzelnen schützt und welche Rechte es für den Einsatz gibt.

B Grundlagen

I. Definition: RFID und Smartcard

Radio Frequency Identification (RFID) ist eine Technologie, die mittels Radiowellen die automatische Erkennung von Personen, Tieren oder Gegenständen ermöglicht. Dabei werden drahtlos Daten von einem Miniatur-Funksender, dem RFID Tag oder Transponder, zu einem RFID Lesegerät, dem RFID Reader oder Transceiver, übermittelt. Es wird zwischen passiven und aktiven RFID Tags unterschieden. Bei passiven RFID Tags variiert die Übertragungsreichweite zwischen einigen Zentimetern bis zu einem theoretischen Maximum von 19,4 Metern[3].

- Passive RFID benötigen keine Batterie, sie beziehen die geringe Menge Energie, die sie zum Senden benötigen, aus elektromagnetischen Wellen, die der RFID Reader beim Leservorgang aussendet.
- Im Gegensatz dazu sind aktive RFID durch eine Batterie gespeist und i.d.R. etwas größer. Sie haben hohe Reichweiten.

[2] Heinrich, Claus (2005): RFID and Beyond: Growing Your Business Through Real World Awareness
[3] Matt Reynolds: Microwave RFID: Passive Scattering and Active Transponders. Internet: http://web.media.mit.edu/~matt/theory.html. Stand: 29.6.2004

Als „Smart Label“ bezeichnet man einen Aufkleber, der mit einem RFID Tag ausgestattet ist. In dieser Arbeit wird hauptsächlich die passive RFID-Technologie betrachtet, da gerade die Verbreitung der passiven Transponder, das Datenschutzrecht vor neue Probleme stellt. RFID Tag ist im Folgenden also als „passives RFID“ zu lesen.
Technisch gesehen kann ein RFID-Transponder wie eine Smartcard verstanden werden. RFID und Smartcards sind eng miteinander verwandt. Der Unterschied besteht weitgehend in der Art der kontaktlosen Stromversorgung und der kontaktlosen Schnittstelle zum Auslesen der Daten, dem so genannten Air Interface. Ebenso wie Smartcards können RFID-Transponder mit zusätzlichen Komponenten ausgestattet werden.

II. Definition: Biometrie

Die Biometrie beschäftigt sich mit der Vermessung quantitativer Merkmale von Lebewesen, insbesondere von Menschen. Aus verschiedenen biometrischen Daten wird auf eine Person geschlossen. Diese kann sich authentifizieren (aus einem definierten Personenkreis), etwa gegenüber Zugangsbeschränkungen, oder sie wird identifiziert (aus einem undefinierten Personenkreis).[4]
Die biometrischen Verfahren sind insofern im Zusammenhang mit der RFID Betrachtung interessant, da eine automatische Erhebung biometrischer Merkmale dem Einsatz von RFID ähnlich ist. Auch mit RFID Technik kann eine eine Authentifizierung oder eine Identifizierung verbunden sein.
Da die Begriffe Authentifizierung und Identifikation (Identifizierung) in der Literatur unterschiedlich definiert und verwendet werden, sollen diese Begriffe hier wie folgt verstanden werden[5]:

1. Authentifizierung

Unter Authentifizierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, in dem bestätigt wird, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

2. Identifikation (Identifizierung)

Unter Identifikation versteht man die Feststellung der Identität einer Person anhand eines eindeutigen Unterscheidungsmerkmals.

---

[4] Vgl. Net-Lexikon: Definition, Bedeutung, Erklärung im Lexikon zum Thema Biometrie. Internet http://www.net-lexikon.de/Biometrie.html. Stand 18.1.2004

[5] Vgl.Ronellenfitsch, Michael (2003): Zweiunddreißigster Tätigkeitsbericht des hess. Datenschutzbeauftragten, Seite 152f.

III. Interessengruppen

Im Rahmen dieser Arbeit wird die Technik auch in Bezug zu den mit ihnen in Berührung kommenden Interessengruppen gestellt. Um Verwechselungen zu vermeiden, seien diese hier kurz beschrieben: Es gibt die Hersteller, die die RFID Tags und Reader entwickeln und produzieren. Unter einem Anwender wird eine „Stelle“ verstanden, die RFID zur Kennzeichnung einsetzt. Weiterhin wird auf den Konsumenten eingegangen, der die RFID Technologie nicht aktiv einsetzt, sondern der Träger von RFID Tags ist. Er kennzeichnet mit RFID nicht, sondern er oder sein Lebensraum wird mit RFID direkt oder indirekt gekennzeichnet.

IV. Stand der Technik

In der Literatur wird RFID gerne rein technisch definiert. Dies allein reicht zur juristischen Betrachtung des Themas nicht aus. Im Folgenden soll das Thema von der technischen Seite so weit betrachtet werden, dass zwischen den verschiedenen Techniken, die sich hinter dem Begriff „RFID“ verbergen, unterschieden werden kann und so eine Bewertung aus der datenschutzrechtlichen Perspektive möglich wird.

1. Historische Entwicklung

Die RFID Technologie hat seit ihrer Invention in den sechziger Jahren des letzen Jahrhunderts heutzutage einen Reifegrad erreicht, der einen praktischen Einsatz und eine Penetration des Marktes möglich macht. Durch die steigenden Produktionsvolumina bei einzelnen Herstellern, ist der Preis pro Tag auf 0,50 – 1,00 US-Dollar gefallen und ein Zielpreis von 0,05 – 0,10 US-Dollar wird erwartet. Dieser Preis wird nicht nur erwartet, sondern auch aktiv von den Grossabnehmern gefordert, um deren Vision vom globalen und universellen Einsatz an jedem „Ding“ auch aus wirtschaftlicher Sicht zu ermöglichen. Mit neuen Produktionstechniken und durch Diversifizierung der Tag-Typen versucht man, dieses Kostenziel zu erreichen.

2. Abmessungen, Bauformen und Komponenten

Die Eigenschaften der Tag-Typen unterscheiden sich in vielen Aspekten. Eine Tendenz zu Miniaturisierung ist bei allen zu erkennen. Das kleinste Exemplar eines in Serie gefertigten RFID-Tags ist der mu-Chip von Hitachi mit nur 0.4mm Durchmesser[6]. Einen solcher RFID ist mit bloßem Auge kaum noch zu erkennen.

[6] Hitachi Website. Internet: http://www.hitachi.co.jp/Prod/mu-chip/. Stand 29.6.2004

Die Tags haben jedoch in vielen Fällen deutlich mehr Möglichkeiten, als nur eine ID zu senden. Die kontaktlose Schnittstelle verbindet das Lesegerät mit weiteren auf dem Tag angebrachten Komponenten. Einige gängige Beispiele sind z.B. Datenspeicher, Mikroprozessoren und Sensoren für Temperatur oder Luftfeuchtigkeit. Diese zusätzlichen Komponenten lassen sich nicht nur kontaktlos auslesen, sondern auch über die gleichen technischen Methoden steuern: Ein Datenspeicher ist beschreibbar, ein Sensor konfigurierbar und ein Mikroprozessor kann Berechnungen durchführen. In diesem Zusammenhang stellt sich die Frage nach Datensicherheit und -schutz. Die ID des Tags ist i.d.R. fest eingespeichert und unveränderlich. Ihr Sinn und Zweck ist es, den Tag aus technischer Sicht von anderen Tags in Reichweite unterscheiden zu können. Sie ist deshalb ohne Schutz auslesbar. Ist über die ID eine Verbindung zum Tag etabliert, können vorhandene zusätzliche Komponenten auf dem Tag über diese angesprochen werden. Auf dieser Ebene ist es technisch möglich, Daten bzw. Komponenten durch kryptographische Verfahren vor dem Zugriff durch Dritte zu schützen. Eine Analyse und Bewertung dieser Verfahren ist kein Bestandteil dieser Arbeit, jedoch sollte festgehalten werden, dass Kryptographie auf RFID-Tags mehr Schwachstellen als auf normalen Rechnersystemen aufweisen, da die Rechenleistung und der zur Verfügung stehende Strom stark limitiert sind.

3. Reichweite und Deaktivierung

Der Technologie ist ein impliziter Schutz gegen das Auslesen durch Dritte eigen, weil die Sendereichweite der Tags stark begrenzt ist: Bei passiven Transpondern kann ein theoretisches Maximum von 19.4 Metern abgeschätzt werden. In der Praxis erzielbare Distanzen liegen zur Zeit zwischen einigen Zentimetern und etwa 1,5 Metern. Je nach Einsatzzweck werden entsprechende Transponder gewählt. Zu unterscheiden ist zwischen Standards, die zur Übertragung von Daten genutzt werden (Protokolle und Frequenzen) und Standards bezüglich der enthaltenen Daten (Dateiformat, ggf. Verschlüsselungsart). Eine Klassifizierung der Tags kann nach Reichweite bzw. Frequenz erfolgen:

Frequenz	Reichweite
125 KHz	1,5 Meter
13,56 MHz	1,5 Meter
UHF (862 MHz -928 MHz)	3 Meter in Europa 7 Meter in USA in Japan keine Zulassung
2.45 GHz	0,1 – 0.7 Meter in Europa

Tabelle 1Typischerweise erreichbare Reichweite bei passiven Tags mit Zulassung in Europa

Die Reichweite hängt auch sehr stark vom eingesetzten Lesegerät bzw. dessen Antennengröße ab. Zur datenschutzrechtlichen Betrachtung sollte festgehalten werden, dass eine Reichweite von 1-1.5 Metern bei den zu erwartenden Standards realistisch ist. Dabei ist es unerheblich, welcher der Standards sich etablieren wird. Alle haben auch gemeinsam, dass

- eine Erhebung der Daten keine Sichtverbindung erfordert und
- das Auslesen durch nicht-metallische Stoffe, z.B. durch eine Einkaufstasche hindurch, möglich ist.

Über den „Ausleseschutz“, der sich durch die begrenzte Reichweite ergibt, hinaus, stellt sich die grundsätzliche Frage der Konturierung und Kontrolle des Auslesevorgangs.

4. Deaktivierung und Kontrolle

Einige Transpondertypen stellen eine Deaktivierungsfunktion zur Verfügung. Hier wird zwischen einem „Dormant Mode“ und einer „Kill Function“ unterschieden. Beide führen zu einer Deaktivierung der Sendefunktion des RFID Tags, jedoch kann diese im Falle des „Dormant Mode“ rückgängig gemacht werden, allerdings ist hierzu spezielle Kenntnis über den Tag notwendig, die meist nur Hersteller oder Anwender haben. Diese verwenden den Begriff „Kill Function“ gerne synonym zu „Dormant Mode“, um besorgten Kunden ein Gefühl von Sicherheit zu geben. Zu unterscheiden ist auch zwischen der Deaktivierung des gesamten Transponders und dem unwiederbringlichen Löschen oder Sperren von Daten auf einem Tag. Eine solche Funktion hat in einige RFID-Standards, die mit Datenspeichern umgehen, Einzug gehalten. Die ID ist auf diesen Tags jedoch nicht löschbar, nur eingespeicherte Daten können unlesbar gemacht werden[7]. Bei Tags, die selbst keine Deaktivierungsfunktion bieten, stellt sich die Frage, welche technischen Möglichkeiten es zur externen Deaktivierung gibt. Zum einen gibt es den Vorschlag zum Einsatz von „RFID Blockern“, die z.B. durch Störsignale das Auslesen von Daten auf in der Nähe befindlichen Tags unterbinden, zum anderen den eines „Transponder Killers“, der einen RFID z.B. durch einen elektromagnetischen Impuls quasi verbrennt. Für beide Typen wurden erste Entwicklungen vorgestellt: Das amerikanische Unternehmen RSA hat einen Blocker Tag vorgestellt[8], dessen Anwendbarkeit noch untersucht wird. Ein Transponder Killer funktioniert etwa wie ein Mikrowellenherd. Wird ein RFID Tag einige Sekunden in einem solchen

[7] Anmerkung: Der Speicherinhalt kann unter einem Elektronenmikroskop ausgelesen werden

[8] Vgl. Juels, Ari; Rivest Ronald L.; Szydlo, Michael: „The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy“. Internet: http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/blocker/blocker.pdf. Stand 29.6.2004

bestrahlt, so verbrennt bzw. explodiert er deutlich sichtbar mit einem kleinen Funkenschlag. Dies basiert auf dem gleichen physikalischen Effekt (Wirbelstrom), der es unmöglich macht, Geschirr mit Goldrand in Mikrowellenherden zu verwenden. Deshalb kann diese Technik nicht global angewendet werden. Die Objekte, an denen der Tag angebracht ist, werden unter Umständen in Mitleidenschaft gezogen[9]. Auch ist das Blockieren durch Ummantelung mit abschirmenden Materialien möglich[10].

5. RFID Anwendungen – überall und allgegenwärtig

Die Penetration der Märkte mit RFID Technologie ist, bedingt durch die Vorteile im Supply-Chain-Management bei Herstellung und Distribution, überall zu beobachten. Die Entwicklung hin zu einer Kennzeichnung von Objekten aller Art ist absehbar: RFID findet sowohl bei großen Dingen, wie z.B. Automobilen, als auch bei kleinen Dingen, wie Coladosen und Geldscheinen, Anwendung. Daraus resultiert eine „Allgegenwärtigkeit“ von Computern in Form der Chips auf den RFID Transpondern. Dies kann als Erweiterung des Cyberspace in die „Real World“ betrachtet werden und wird gerne als Komplement zum Cyberspace gesehen: Im Gegensatz zum Cyberspace-Konzept, bei dem die „Real World“ in Computern abgebildet wird, findet hier eine Durchdringung der „Real World“ mit „kleinen Computern und Sensoren“ statt. Dieses Konzept wird als „Ubiquitous Computing“ oder „Pervasive Computing“ bezeichnet. Das erste meint die Allgegenwätigkeit der Chips, das letztgenannte ist der Fachterminus für Chips, die in Dinge eingelassen sind und deren Funktionen steuern („intelligente Geräte“). Dies zeigt, dass das neue Rechtsgebiet des Cyberlaw eventuell Anwendung in der „Real World“ finden sollte. Auch in der aktuellen Diskussion um Digital Rights Management sollte dieser Aspekt berücksichtigt werden, denn in Verbindung mit RFID eröffnet sich auch für dieses Technologie- und Rechtsgebiet eine neue Dimension.

Die Fragestellung ist so neu, dass es noch keine wissenschaftlichen Prognosen zu Entwicklung und Auswirkungen dieser Technologie gibt. Das Bundesamt für Sicherheit in der Informationstechnik hat erst kürzliche eine Ausschreibung zur Erstellung einer entsprechenden Studie gemacht[11].

---

[9] Ein Beispiel ist der Tag, der in Bekleidung der Marke Benetton eingearbeitet ist

[10] In der populären Literatur wird häufig das „Umwickeln mit Alufolie“genannt.

[11] BSI, Referat Z5: Öffentliche Ausschreibung zu Auftrags-Nr.: 25451/2004. Internet: http://www.bsi.bund.de/ausschr/einkauf/00090.htm. Stand 5.5.2004

6. Standards für unterschiedliche Frequenzen

Die wichtigsten Standards für RFID sind in Tabelle 2 aufgeführt. Für nahezu alle vorstellbaren Einsatzgebiete gibt es mittlerweile öffentlich verfügbare Standards, was eine mögliche Nutzung durch Dritte stark vereinfacht.

Frequenz	Standard
125 KHz	ISO 11784/85 Animal ID Read-only ISO 14223/1 Animal ID R/W FDIS ISO 18000-2 Item Management
13,56 MHz	ISO 15693 RP 1740C IATA recommended practice baggage handling FDIS[12] ISO 18000-3 Item Management
UHF	ANSI MH 10.8.4 Returnable Containers FDIS ISO 18000-6 Item Management/ GTAG
2,45 GHz	FDIS ISO 18000-4 Item Management ANSI MH 10.8.4 Returnable Containers

Tabelle 2Für RFID relevante Standards

7. Standards für die Semantik der RFID-Daten

Es bleibt festzuhalten, dass Transponder immer Daten enthalten. Jedoch gibt es einige Standards, bei denen sich die Datenhaltung auf eine eineindeutige ID beschränkt[13]. Wenn im Folgenden also von Daten gesprochen wird, sind zusätzlich gespeicherte Daten gemeint. Die technisch notwendigen CID oder ID haben die Eigenschaft, dass Zusatzwissen notwendig ist, um sie mit einer dahinterstehenden Information zu verknüpfen. Die Güte der Information kann durchaus vom vorhandenen Zusatzwissen abhängen. Es muss die Frage gestellt werden, welchen Informationsgehalt die Daten auf den Tags in sich bergen bzw. wer mit der Information etwas anfangen kann.

Hierzu sollen kurz die Standards betrachtet werden, mit denen wir in Zukunft höchstwahrscheinlich in Kontakt kommen werden. Allein die Möglichkeit, die Daten aus einem Tag auszulesen, zieht nicht zwangsläufig die Möglichkeit nach sich, diese Daten auch interpretieren zu können. Die Daten bekommen erst Semantik, wenn eine geeignete Zuordnung zwischen Sprache und Daten erfolgen kann. Sind die Daten beispielsweise in der Sprache „Englisch“ kodiert, so kann durch Übersetzung der Sinn der Information verstanden werden. Ist die Information kryptographisch verschlüsselt, so benötigt man zur Übersetzung

[12] FDIS: Final Draft International Standard, Stufe 4 von 5 im ISO Standardisierungsprozess; Stufe 5 entspricht einem „ISO Standard“

[13] Z.B. beim EPC

einen „digitalen Schlüssel“. Ebenso verhält es sich mit einem Produktcode, der bei RFID-basierten Standards eine Zahl zwischen 1 und 2^{128} ist[14]. Um einem mathematischen Laien klar zu machen, wie groß dieser Zahlenraum ist: Mit diesen 128 Bit kann man jedem Kieselstein auf unserem Planeten eine eigene Nummer zuteilen. Die Größe dieses Zahlenraums ist Voraussetzung für eine eineindeutige Identifizierung jedes einzelnen Produktes. Der Begriff „eineindeutig“ stammt aus der Mathematik und bedeutet „umkehrbar eindeutig“ und kann vereinfachend als eine stärkere Form der Eindeutigkeit verstanden werden. Ein griffiges Beispiel für Eineindeutigkeit ist eine Seriennummer für ein Produkt, die es genau einmal gibt. Es kann sowohl vom Produkt auf die Seriennummer geschlossen werden als auch von der Nummer auf das Produkt. Der Unterschied zur Eindeutigkeit soll an folgendem Beispiel klar gemacht werden:
Über ein KFZ-Kennzeichen lassen sich zusammen mit den Informationen der Zulassungsstelle das Fahrzeug und der Halter bestimmen. Unter der Annahme, dass der Halter nur ein Fahrzeug hat, liegt hier Eineindeutigkeit vor, denn man kann über die Personalien der Person das Kennzeichen seines Fahrzeugs ermitteln.
Hat man hingegen zum Fahrzeug nur eine Beschreibung („rotes Auto mit 4 Türen“) zur Hand, jedoch nicht das Kennzeichen, so lässt sich i.d.R. nur eine Menge von möglichen Haltern ermitteln. Hat man den Halter jedoch ermittelt, kann genau auf sein Fahrzeug geschlossen werden („Er hat ein rotes Auto mit 4 Türen“). Hier liegt Eindeutigkeit vor: Die Zuordnung zwischen Halter und Fahrzeug ist eindeutig. Die Umkehrung, also die Zuordnung zwischen Fahrzeug und Halter (aufgrund der Beschreibung des KFZ) ist nicht eindeutig.

8. Zahlenraum der RFID-Standards

Eines haben jedoch alle Tag-Typen gemeinsam: Um technisch einwandfrei funktionieren zu können, müssen sie eine eineindeutige Kennung haben. Dies ist i.d.R. eine Zeichnenkombination, die es in der Welt der Tags nur einmal gibt und eine Identifikation des Tags zweifelsfrei zulässt. Obwohl die Hersteller verschiedene RFID-Systeme und Standards propagieren, werden Überschneidungen der Kennungen zwischen verschiedenen Tag-Typen vermieden.
Der heutzutage existierende Standard zur Produktkennzeichnung (ohne RFID) ist in Europa der EAN. Andere Regionen der Welt haben ähnliche Standards, etwa der UPC in den USA. Um Überschneidungen und damit Mehrdeutigkeit von

[14] Der EPC Standard arbeitet mit 96 Bit Codes, also 2^{96} „Kombinationen“

Codes zu vermeiden, wird mit dem GTIN Standard[15] eine Vereinheitlichung der Codes angestrebt. Diese Harmonisierung der „Nummernkreise“ wird von der Dachorganisation EPCGlobal, Inc. kontrolliert. EPCglobal, Inc. ist ein Unternehmen, das sich auch mit der Vereinheitlichung von Produktcodes auf RFID Basis beschäftigt. Es ist ein Zusammenschluss der EAN International und dem Uniform Code Council, Inc. (UCC) und nahezu alle Unternehmen, die mit dem Supply-Chain-Business zu tun haben, sind Mitglied in diesem Zusammenschluss. Die Marktmacht dieses Standardisierungsgremiums ist so groß, dass zukünftig von einem einheitlichen Standard für Produktcodes ausgegangen werden kann. Existierende „Insellösungen“ werden verschwinden. Der EPC Standard definiert neben der Beschaffenheit des Produktcodes auch ein proprietäres Air Interface. Häufig wird der ISO 18000-6[16] als alternativer Standard zu EPC verstanden, jedoch definiert der ISO 18000-6 nur das Air Interface. Die einheitliche Verwendung der EPC Produktcodes wird sich nach hier vertretener Ansicht etablieren.

9. Zulassungsfreiheit

Der ISO 18000-6 Standard ist auch daraufhin optimiert, den rechtlichen Rahmenbedingungen vieler Staaten der Erde gerecht zu werden. Weiterhin bietet er eine höhere Lesesicherheit und -geschwindigkeit.[17]
Die 125 kHz und 13,56 MHz Standards sind weltweit weitgehend harmonisiert, da die meisten Länder die von der ITU standardisierten Frequenzbänder des Industrial-Scientific-Medical (ISM) Frequenzbandes freihalten, jedoch können im UHF bzw. 2.45 GHz Bereich Kollisionen mit bestehenden Technologien wie Wireless LAN, Bluetooth oder GSM auftreten. In Europa werden nationale Regulierungs- und Zulassungsvorschriften auf Grundlage der Empfehlungen des ERC (European Radiocommunication Commitee) bzw. des ERO (European Radiocommunication Office) gemacht. Das ERC ist wurde 1991 aus der CEPT (European Conference of Postal and Telecommunications) heraus gegründet, mit dem Ziel die Europäische Kommission in Telekommunikationsfragen zu unterstützen. Die CEPT[18] (European Conference of Postal and Telecommunications) wiederum existiert als supernationale Regulierungsinstanz seit 1959 mit dem Ziel Post- und Telekommunikationswesen kompatibel zu halten. Mittlerweile hat die CEPT 26 Mitgliedsstaaten. Die EU-Richtlinie 1999/5/EG (Richtlinie für Funkanlagen und

[15] EAN Internatial (bald: GS 1) Website. Internet: http://www.ean-int.org/products.html, Stand 5.5.2004
[16] Der Arbeitstitel des ISO 18000-6 Standard ist “GTAG“ und ist in der Literatur noch häufig verwendet.
[17] http://www.rfidjournal.com/article/articleprint/325/-1/2/, Stand 5.5.2004
[18] Internet: http://www.cept.org/. Stand 9.8.2004

Telekommunikationsendeinrichtungen) empfiehlt, innerhalb er EU[19] in diesen Sachen den „Sachverstand der CEPT/ERC heranzuziehen“. Die ERC Recommendation 70-03[20] Annex 11 regelt RFID Frequenzen und Sendeleistung für RFID im 2.4 GHz Bereich. In Deutschland hat die RegTP im Sommer 2000 durch Verfügungen den RFID Einsatz in Deutschland in Sinne der Richtlinie 1999/5/EG[21] (RTTE-Richtlinie) geregelt:

- Unter Verfügung 61/2000[22] kann der Einsatz von 125 KHZ RFID subsumiert werden. Der Einsatz ist in Deutschland zulassungsfrei.
- Unter Verfügung 73/2000[23] „Allgemeinzuteilung von Frequenzen für die Benutzung durch die Allgemeinheit für Funkanlagen geringer Leistung des nichtöffentlichen mobilen Landfunks (nömL) in ISM-Frequenzbereichen; SRD (Short Range Devices)“ kann der Einsatz von RFID im 13 MHZ und 2.4 GHZ Frequenzband subsumiert werden. Der Einsatz ist in Deutschland zulassungsfrei.

[19] Die nationale Umsetzung der Richtlinie in Deutschland ist das Gesetz über Funkanlagen und Telekommunikationseinrichtungen (FTEG) vom 31. Januar 2001. Internet: http://bundesrecht.juris.de/bundesrecht/fteg/inhalt.html

[20] ERC/REC 70-03 : Internet: http://www.ero.dk/documentation/docs/docfiles.asp?docid=1622. Stand 9.8.2004

[21] Internet: http://europa.eu.int/comm/enterprise/rtte/dir99-5.htm. Stand 9.8.2004

[22] Internet: http://www.funkmagazin.de/04070.htm. Stand 9.8.2004

[23] Internet: http://www.funkurteile.de/Gesetze_-_Verfugungen_-_Richtl/LPD-ISM-SRD/Verfugung_73_2000/verfugung_73_2000.html. Stand: 8.8.2004

C Aktuelle Anwendungen in der Praxis

I. Personenauthentifizierung

Den „Durchbruch“ erzielte die RFID-Technologie im Jahre 1995, als die Deutsche Lufthansa AG den „Frequent-Traveler“ Ausweis, eine im ID-1 Format[24] gehaltene Chipkarte, mit RFID ausstattete. RFID-basierte Karten werden seit dem verstärkt als Zahlungsmittel, z.B. im öffentlichen Personennahverkehr, oder als Ausweis, z.B. als Firmenausweis oder als Schlüsselkarte, eingesetzt. Seit 1996 ist in der südkoreanischen 12-Millionen Metropole Seoul das bislang größte RFID-basierte Fahrkartensystem in Betrieb genommen worden. Die Karten werden an speziellen Terminals mit Geld aufgeladen und beim Ein- und Umsteigen entsprechend belastet. Ein deutsches Pilotprojekt findet sich seit 1990/91 im Verkehrsverbund KVG Lüneburg-VWG Oldenburg. Dem einen oder anderen Leser werden die Transponder auch vom Wintersport her bekannt sein: Moderne Skiliftanlagen regeln den Zugang zum Lift über entsprechende Skipässe oder Armbanduhren. Die Mensakarte Uni Regensburg nutzt seit langem RFID, um den Zahlvorgang bequem zu gestalten und Wartezeiten an der Kasse zu reduzieren. Um zu zahlen, legt der Gast legt einfach seinen Tag mit auf das Tablett, wenn er an der Kasse vorbeigeht.
Auch einige Hotels nutzen RFID zur Zugangskontrolle. Fertige Schliesssysteme zur Aus- oder Umrüstung sind im Handel problemlos erhältlich. Auch die elektronische Wegfahrsperre beim KFZ ist über einen Tag im Zündschlüssel realisiert.
Eines haben diese beispielhaft genannten Systeme gemeinsam: Sie arbeiten innerhalb abgeschlossener Benutzergruppen und haben keine oder nur wenig Verbindungen zu anderen Systemen. Eine automatisierte Verarbeitung der Daten (§ 3 BDSG, soweit personenbezogene Daten verarbeitet werden) erfolgt zwar, jedoch keine Übermittlung.

II. Übermittlung

Bei dieser Gelegenheit soll kurz der Unterschied zwischen den Begriffen Übermittlung und Übertragung dargelegt werden: Bei der Übertragung handelt es sich um das technische Empfangen oder Senden von Daten, mit Übermittlung hingegen meint der Jurist den Übergang der Verantwortlichkeit für die Daten an einen Dritten. Umgangssprachlich und auch in den technischen Wissenschaften werden diese Begriffe oft synonym verwendet. Eine Übermittlung von Daten ist auch häufig mit der Übertragung verbunden, jedoch erfolgen Übertragungen

[24] Dies entspricht der Größe einer Kreditkarte

sehr häufig, ohne dass eine Übermittlung im Sinne BDSG stattfindet. Man mache sich dies am obigen Fahrkarten-Beispiel klar. Die Daten über die Nutzung des Nahverkehrs werden zwar übertragen, z.B. zwischen Bus und Leitstelle, jedoch nicht übermittelt, da die Daten keinem Dritten zugänglich gemacht werden.

III. Identifikation von Lebewesen

1. Kombinationen von Authentifizierung und Identifikation

Auf der weltgrößten IT-Fachmesse CeBIT 2004 hat die Bundesdruckerei einen Reisepass im ID-1 Kartenformat vorgestellt, der neben den klassischen Sicherheitsmerkmalen auch mit einem Transponder ausgestattet ist[25]. Der Anlass zur Entwicklung ist die im Zuge von Terrorismusbekämpfung und e-Government aufgekommene Forderung der Politik nach digitalen Ausweisdokumenten[26]. Ebenso wird eine Speicherung von biometrischen Daten auf diesen Dokumenten diskutiert und von den USA von der EU sogar gefordert. Erst kürzlich wurde ein Konsens über den zukünftigen Standard gefunden[27]. Eine Kombination mit RFID liegt nahe. Das von der Bundesdruckerei vorgestellte System ermöglicht die Speicherung der Daten zweier Fingerabdrücke und des Gesichts. Das Auslesen ist drahtlos möglich. Damit ist eine Konformität zu den von der ICAO (International Civil Aviation Organization) propagierten Reisedokumenten gegeben[28]. Die ICAO verfolgt das Ziel, Reisenden „unbeaufsichtigten Zugang“ bei Erhöhung der Sicherheitsstandards zu gewähren. Zwei eigentlich gegensätzliche Ziele, die man durch Einsatz von Biometrie, Kryptographie und RFID zu erreichen versucht. Passend zu ihren digitalen Dokumenten hat die Bundesdruckerei hat ein mobiles Gerät zum Auslesen der Daten entwickelt. Mit den sogenannten „Verifier“ kann die Authentizität des Dokumentes geprüft werden und auch etwaige darauf gespeicherte Daten wie z.B. ein Bild des Gesichtes oder Reisevisa.

---

[25] Bundesdruckerei GmbH:Ausführungen von Herrn Ulrich Hamann, Geschäftsführer der Bundesdruckerei GmbH, anlässlich eines Pressegespräches auf der CeBIT 2004. Internet: http://www.bundesdruckerei.de/de/presse/pressemeldungen/rede_ham.html, Stand 04.05.2004

[26] silicon.de GmbH:Der digitale Personalausweis kommt, sagt Schily. Internet: http://www.silicon.de/cpo/news-itsecurity/detail.php?nr=13723&kategorie=news-itsecurity, Stand 04.05.2004

[27] heise online: Neue Passgeneration in den Startlöchern. Internet: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/47189&words=ICAO. Stand 30.6.2004

[28] ICAO: New Technologies and Travel Documents.. Internet: http://www.icao.int/icao/en/atb/fal/fal12/Presentations/TAG12_Biometrics.ppt. Stand 04.05.2004

2. Implantierte RFID-Transponder

Zur Erkennung von Personen wurde sogar ein System entwickelt, welches sich subdermal in den Menschen implantieren lässt: VeriChip von Applied Digital Solutions[29]. Der Hersteller führt eine globale Registrierungsdatenbank. Als Anwendungsgebiete nennt Applied Digital unter anderem Identifkation, Zahlung und Zugangskontrolle zu „geistigem Eigentum“[30]. Die oben genannte Idee eines Digital Rights Management auf RFID Basis scheint technisch gesehen schon entwickelt zu sein. Die Lebensdauer für den Tag wird auf 20 Jahre geschätzt. Die Anwendung beim Menschen ist keine Sciene-Fiction, sondern bereits Realität. Der größte Abnehmer für Chips ist zur Zeit im Lande Mexico zu finden, in dem die Gesellschaft zur Wiederauffindung von Kindern mit einen Rahmenvertrag die Lieferung größerer Mengen VeriChips gesichert hat. In anderen Ländern buhlen zur Zeit Unternehmen um exklusive landesweite Vertriebsrechte[31]. Die Anwendung als Ersatz für einen Personalausweis wurde bisher noch nicht öffentlich gefordert. Mit steigendem Bekanntheitsgrad dieser Technologie ist jedoch damit zu rechnen, dass diese Diskussion entfachen wird. Die Technik, RFID-Tags zu implantieren, ist allerdings nicht neu. Die Anwendung bei Tieren ist schon seit langem standardisiert. Die in der Massentierhaltung verwendeten Glastransponder haben eine signifikant größere Bauform als die des VeriChips, die etwa der Form eines Reiskorns entspricht. Die Anwendung ist auch bei Haustieren zu beobachten. Taubenzüchter setzen gerne Ringe mit Transponder zur Kennzeichnung ihrer Tiere ein. Bei Wettbewerben kann so u.a. eine genaue Ankunftszeit der einzelnen Taube festgestellt werden. Auch für Hunde und Katzen gibt es ein entsprechend standardisiertes System[32]. Es soll helfen, entlaufene oder gestohlene Tiere wieder aufzufinden. Ein Ähnliches System gibt es für die Zeitmessung beim Laufsport: Der Champion-Chip ist ein RFID, der am Schnürsenkel eines Laufschuhs befestigt wird.

IV. Identifikation von „Dingen“ mittels RFID

1. Klebeetiketten im Supply-Chain-Management

Eine weitere Klasse von RFIDs wird zur Kennzeichnung von Gegenständen eingesetzt. Die Technologie ist als Schutz vor Ladendiebstahl aus Kaufhäusern sicher hinreichend bekannt. Die neue Generation von Chips ist jedoch viel

[29] Applied Digital Solutions Incorporated: Website. Internet: http://www.adsx.com/prodservpart/verichip.html, Stand 4.5.2004
[30] Applied Digital Solutions Incorporated: Website.Internet http://www.4verichip.com/applications.htm, Stand 4.5.2004
[31] Volunteers of Indymedia Biotech Webiste. Internet: http://www.biotechimc.org/or/2003/12/2178.shtml, Stand 4.5.2004
[32] Euro I.D. Identifikationssysteme GmbH & Co. KG: Website. Internet: http://www.euroid.com/anwe28.htm, Stand 30.6.2004

kleiner und liefert mehr Information als Ihre Vorgänger. Eine zur Zeit sehr gerne angewandte Bauform ist die des „Smart Labels“, also ein Tag, der in ein Klebeetikett eingelassen ist. Das Smart Label wird im Logistikprozess nicht nur zur Kennzeichnung von einzelnen Produkten verwendet, sondern aus pragmatischen Gründen zur Kennzeichnung von Gebinden und Kartonagen.
Die Forderung nach einheitlicher Kennzeichnung seitens der Hersteller wird in Logistik und Distribution immer lauter. Die Big Player nutzen ihre Machtposition zur Zeit aus, um Druck auf die Hersteller auszuüben. So nimmt Wal-Mart keine Lieferungen ohne RFID-Kennzeichnung mehr an. Auch die Metro Group wird ab Ende 2004 ähnlich verfahren[33]. Ebenso fordert das Department of Defense (DoD) der USA seine Zulieferer auf, zumindest die Kartonagen mit RFID zu kennzeichnen.[34] Spätestens ab 2006 soll jedes einzelne Produkt identifizierbar sein. Es sei an dieser Stelle darauf hingewiesen, dass das DoD nicht nur Kriegswaffen einkauft, sondern zur Versorgung des Soldaten mit ca. 28 Milliarden US-Dollar Umsatz einer der größten Abnehmer von Produkten aller Art ist. Ergo ist der Druck auf die Zulieferer zur Einführung von RFID Kennzeichnung bereits so hoch, dass eine Kennzeichnung der Gebinde und ggf. auch der Produkte durch Smart Labels auch dann zu erwarten ist, wenn der Prozess der RFID Integration in die Endprodukte noch nicht weiter fortgeschritten ist.

2. Über das Suppy-Chain-Management hinaus

Der Einsatz von Smart Labels in großen Warenhäusern nimmt immer weiter zu. Ein in Deutschland gerne genanntes Beispiel ist die Metro Future Initiative[35], die am 28 April 2004 ihr einjähriges Jubiläum feierte. Diese ist ein gemeinsames Projekt der METRO Group, SAP, Intel, IBM sowie weiteren Unternehmen und versteht sich als Plattform zum Test neuer Innovationen im „Retailer Business“. Selbstverständlich gehört der Einsatz von RFID zu diesen Innovationen. Das Pilotprojekt, der Future Store Rheinberg, nutzt Smart Labels zur Kennzeichnung von CD und DVD Produkten, sowie den integrierten Tag in den Verpackungen von Gillette Rasierklingen, Pantene Shampoo und Philadelphia Käse. Weiterhin gab es dort bis vor kurzem eine Kundenkarte, auf der die Kundennummer via RFID auslesbar war. Die Metro Gruppe legt bei diesem „Feldversuch“ auch sehr viel Wert auf Öffentlichkeitsarbeit und versucht, die Konsumenten von ihrem

[33] METRO Group:METRO Group startet die unternehmensweite Einführung von RFID. Internet: http://www.future-store.org/servlet/PB/-s/15k9c5za28j5wasfwsu1dpi2yl2125xy/menu/1002256_pprint_l1/1088551037081.htm?part=null . Stand 12.1.2004

[34] Association for Automatic Identification and Mobilty. Website. Internet: http://www.aimglobal.org/technologies/rfid/resources/articles/oct03/mandate.htm. Stand 16.11.2004

[35] http://www.future-store.org, Stand 5.5.2004

verantwortungsvollen Umgang mit den Tags zu überzeugen. Eine Eigenentwicklung ist der „De-Activator“ der Metro, der den Inhalt der Tags beim Verlassen des Shops mit Nullen überschreibe. Eine Nutzung und damit ein Missbrauch der Tags außerhalb des Stores sei nicht möglich. Jedoch kritisiert die Verbraucherschutzorganistation FoeBuD e.V. die Aussagen der Metro sehr stark und versucht die Unrichtigkeit der Metro-Aussagen zu belegen. Hier soll für keine der beiden Seiten Stellung bezogen werden. Festzuhalten bleibt nur, dass sich beide klischeegerecht verhalten: Beim FoeBuD e.V. kann man eine marktschreierische Informationspolitik, bei der Metro Gruppe eine ignorante Haltung gegenüber den Vorwürfen feststellen.
Das Phänomen ist aber kein rein deutsches, wie der Fall Gillette belegt. Der aus den USA stammende Verbraucherschutzverein CASPIAN[36] ruft aufgrund des stillschweigenden Einsatzes von RFID bei Gillette Produkten zum Boykott von Produkten des Konzerns auf[37]. Es wurden hier nicht nur Tags zum Erfassen von Kaufgewohnheiten eingesetzt, sondern auch mit Kameratechnik gearbeitet, die in die Verkaufsregale integriert waren[38].

3. Anwendung an Geldscheinen

Weiterhin wurde von offizieller Seite aus bestätigt, dass Japan als erstes Land angefangen hat, Geldscheine mit Tags auszustatten. Im neuen 10000[39] Yen Schein ist ein mu-Chip von Hitachi[40] eingelassen, der mit einer Größe von 0.4mm kleiner als ein Stecknadelkopf ist. Die Gerüchte über neue 100 Dollar US-Banknoten mit RFID lassen sich nicht offiziell belegen; die Europäische Zentralbank spricht hingegen von einem laufenden Projekt mit dem Ziel 2005 mit der RFID-Bestückung der Euronoten zu beginnen[41]. Die Fälschungssicherheit der Noten wird dadurch erhöht und weiterhin lassen sich Zähl- und Erkennungsvorgänge besser automatisieren.

4. Sensoren – „Augen und Ohren der RFID“

Es bleibt zu erwähnen, dass die Transponder „Augen und Ohren“ bekommen. Vielfach werden diese mit Sensoren kombiniert, die Temperatur, Luftfeuchtigkeit, Helligkeit oder andere Daten aus ihrer Umgebung aufnehmen, speichern und übertragen. Der spanische Lebensmittelhersteller Campofrio versieht jeden Schinken mit einem Transponder, der während das gesamten

[36] Consumers Against Supermarket Privacy Invasion and Numbering, Homepage: http://www.nocards.org/
[37] http://www.boycottgillette.org/, Stand 4.5.2004
[38] Gillette spricht hier von „Smart Shelves“
[39] 10000 Yen haben einen Gegenwert von etwa 100 US-Dollar
[40] The Register.Japan yens for RFID chips. Internet. http://www.theregister.co.uk/content/55/32061.html. Stand 30.6.2004
[41] myEuro.info. Website. internet: http://www.myeuro.info/rfid.php, Stand 5.5.2004

Reifeprozesses desselben Produktionsdaten, wie z.B. Temperatur und Fettgehalt misst und speichert. Damit erreicht Campofrio ein optimale Steuerung des Reifeprozesses. Der Einsatz der RFID geht damit weit über eine reine Identifizierung hinaus.

V. Zusammenfassung

Alle die genannten Verfahren haben gemeinsam, dass sie technisch ausgereift sind und als in sich abgeschlossene Lösung funktionieren. Aus datenschutzrechtlicher Sicht sollte aber beleuchtet werden, in wie weit die erhobenen Daten untereinander kompatibel sind. Denn wenn diese Kompatibiliät gewährleistet ist, stellt das den Datenschutz vor andere Sachverhalte. Wenn ein Abgleich der Daten untereinander möglich ist, könnte die sich daraus ergebende Information mehr sein als nur die Summe der einzelnen Informationen.
Es wurden einige konkrete Einsatzmöglichkeiten von RFID Technologie geschildert und wahrscheinliche Entwicklungen aufgezeigt. Diese bergen ein großes Nutzenpotential für alle Beteiligten. Jedoch haben die Bedenken gegenüber der Metro Future Store Kundenkarte beispielsweise gezeigt, dass der „Faktor Mensch“ hierbei nicht außer acht gelassen werden sollte. Die von der Metro als „emotional“[42] umschriebenen Bedenken der Konsumenten können auch als „Angst vor der Durchleuchtung“ oder „Verlust der Privatsphäre“ interpretiert werden. Um so mehr macht es Sinn, sich diesem Thema von der rechtlichen Sicht zu nähern und einige grundlegende mögliche Szenarien zu untersuchen.
Zur Betrachtung wurden selektiv zwei Szenarien gewählt, deren technische Voraussetzungen gegeben sind und deren tatsächliches Eintreten keine reine Fiktion ist. Diese wurden gezielt so gewählt, dass die rechtliche Bewertung auf der Ebene des Bundesrechts durchzuführen ist.

D Rechtliche Bewertung (Szenario 1)

I. Szenariobeschreibung: „Personalausweis“

In diesem Szenario werden auf dem deutschen Personalausweis Daten digital gespeichert. Die im Ausweismuster durch das Personalausweisgesetz (PAuswG) vorgeschriebenen Angaben über die Person (§ 1 Abs. 2 PAuswG) werden nicht nur in das Dokument gedruckt, sondern zusätzlich auf einem RFID- Chip gespeichert.

[42] Metro Website:“RFID in customer cards: test discontinued“. Internet: http://www.future-store.org/servlet/PB/menu/1002376_l2/index.html. Stand 14.8.2004

§ 1 PAuswG Ausweispflicht
(…)
(2) Der Personalausweis und der vorläufige Personalausweis sind nach einheitlichen Mustern mit Lichtbild auszustellen; sie erhalten eine Seriennummer. Der Ausweis enthält neben dem Lichtbild des Ausweisinhabers und seiner Unterschrift ausschließlich folgende Angaben über seine Person:
1. Familienname und ggf. Geburtsname,
2. Vornamen,
3. Doktorgrad,
4. Ordensname/Künstlername,
5. Tag und Ort der Geburt,
6. Größe,
7. Farbe der Augen
8. gegenwärtige Anschrift,
9. Staatsangehörigkeit.
(3) Der Personalausweis erhält eine Zone für das automatische Lesen. Diese darf lediglich enthalten:
1. Die Abkürzung "IDD" für "Identitätskarte der Bundesrepublik Deutschland",
2. den Familiennamen,
3. den oder die Vornamen,
4. die Seriennummer des Personalausweises, die sich aus der Behördenkennzahl
der Personalausweisbehörde und einer fortlaufend zu vergebenden Ausweisnummer zusammensetzt,
5. die Abkürzung "D" für die Eigenschaft als Deutscher,
6. den Tag der Geburt,
7. die Gültigkeitsdauer des Personalausweises,
8. die Prüfziffern und
9. Leerstellen.
(4) Der Personalausweis darf neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden. Auch die in Absatz 2 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in
den Personalausweis eingebracht werden.
(5) Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 4 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz
geregelt. Eine bundesweite Datei wird nicht eingerichtet.
(6) Für die erstmalige Ausstellung des Personalausweises sowie für die Neuausstellung nach Ablauf der Gültigkeitsdauer ist eine Gebühr von acht Euro zu erheben. Die erstmalige Ausstellung des Personalausweises an Personen, die das 21. Lebensjahr noch
nicht vollendet haben, ist gebührenfrei. Von der Erhebung einer Gebühr kann abgesehen
werden, wenn der Gebührenpflichtige bedürftig ist.
(7) Die Muster der Ausweise bestimmt das Bundesministerium des Innern durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf. Der Personalausweis ist Eigentum der Bundesrepublik Deutschland.

Weiterhin werden im Chip biometrische Daten der Person gespeichert (zwei Fingerabdrücke sowie das Gesicht). Im Ausweis ist ein Transponder enthalten, der ein kontaktloses Lesen der Daten mittels eines kleinen portablen Gerätes[43] (im Folgenden Reader genannt) aus einer Entfernung von ca. 3 Metern ermöglicht.

[43] Beispielsweise der Verifier der Bundesdruckerei GmbH

Der Bundesgrenzschutz (im Folgenden BGS genannt) kontrolliert während der Fußball WM 2006 stichprobenartig die Identität der Passagiere auf deutschen Bahnhöfen, um den Zugverkehr und die Wettbewerbe vor bekannten Hooligans zu schützen. Im Beispielsszenario liegen sehr genaue Kenntnisse vor, dass sich eine große Menge von Hooligans unter die anreisenden Zuschauer mischen wird. Die Hooligans planen nach den Lageberichten der Sicherheitsbehörden erhebliche Krawalle bereits bei der Anreise, an Bahnhöfen und/oder während der Zugfahrt. Da viele Fußballfans anlässlich des Fußballspektakels Mützen tragen und ihre Gesichter in Landes- oder Vereinsfarben angemalt haben, ist eine Identitätsfeststellung mittels des Passbildes für die BGS Beamten schwieriger als im „Normalfall“. Der BGS nutzt deshalb den Reader, um die Identität einzelner Passagiere mittels des Ausweises festzustellen. Es besteht lediglich eine Ausweispflicht, jedoch keine Pflicht zur Mitführung eines Ausweises. D.h. es besteht eine Pflicht zum Besitz eines Ausweises, aber niemand ist verpflichtet, seinen Ausweis ständig bei sich zu führen[44].

PAuswG § 1 Ausweispflicht
(1) Deutsche im Sinne des Artikels 116 Abs. 1 des Grundgesetzes, die das 16. Lebensjahr vollendet haben und nach den Vorschriften der Landesmeldegesetze der allgemeinen Meldepflicht unterliegen, sind verpflichtet, einen Personalausweis zu besitzen und ihn auf Verlangen einer zur Prüfung der Personalien ermächtigten Behörde vorzulegen; dies gilt nicht für Personen, die einen gültigen Paß besitzen und sich durch diesen ausweisen können. Der Ausweispflicht kann auch durch Vorlage eines vorläufigen Personalausweises genügt werden.

Die Kontrolle der BGS-Beamten erstreckt sich daher auf diejenigen, die überhaupt einen Ausweis mitführen. Mit den biometrischen Daten des Gesichtes wird dann lediglich festgestellt, ob der Betroffene auch wirklich seinen Personalausweis mitführt und nicht etwa einen geliehenen oder gestohlenen. Von einer detaillierten technischen Beschreibung des Readers soll hier abgesehen werden. Das fiktive Gerät im Szenario ist an den Verifier der Bundesdruckerei GmbH angelehnt. Es sei angemerkt, dass in der Praxis Daten wie etwa Namen und Adresse für den BGS Beamten nutzbar sind, die Nutzung der biometrischen Daten jedoch Zusatzwissen bzw. zusätzlichen technischen Aufwand nach sich zieht. Bei der rechtlichen Betrachtung soll davon ausgegangen werden, dass das Gerät die notwendige Technik bietet. Hier ist z.B. vorstellbar, dass das Gerät selbsttätig „erkennt“, ob der Betroffene auch tatsächlich einen Personalausweis bei sich trägt, der auf ihn ausgestellt ist: Das Gerät führt dazu eine Gesichtserkennung und einen automatischen Abgleich mit den biometrischen Daten (Template des Gesichts im Ausweis) durch. Vorstellbar wäre z.B. ein Gerät, dass auf einem kleinen Bildschirm die im Pass

[44] Medert/Süßmuth, Einführung, Rn 5

gespeicherten Daten anzeigt und zusätzlich eine Information „Identität verifiziert“ bzw. „Identität nicht verifiziert“ anzeigt.
Zusammenfassend wird festgehalten, dass Name und Identität einer Person zielsicher festgestellt werden kann ohne dass eine Verknüpfung mit externen Datenbanken, wie etwa einer „Hooligan-Datei“ oder dem Einwohnermeldeamt, durchgeführt werden muss. Das Gerät arbeitet autark. Der Einsatz des Gerätes ist für den Betroffen nicht zwangsläufig erkennbar. Eine Identifikation ist für den BGS Beamten auch „von hinten“ möglich. Ein Hinweis auf das Auslesen der Daten, etwa durch eine Ansage mit dem Megaphon, erfolgt nicht.
Nachdem Fußballfan F vom BGS in Gewahrsam genommen wird, weil er einem der BGS Beamten als Hooligan namentlich bekannt[45] ist seine Identität in der Menge ausgelesen wurde, geht F zum Rechtsanwalt. Ihn bewegt[46], dass

- seine Ausweispapiere mit RFID ausgestattet sind und
- sein Personalausweis mit biometrischen Daten -ohne seine Kenntnis- ausgelesen wurde.

II. Exkurs: Ein realitätsnaher Sachverhalt?

Das Szenario basiert auf einer fiktiven technischen Gerätschaft, dem Reader. Die rechtliche Prüfung dieses Sachverhalts erscheint nur sinnvoll, wenn eine mittelfristige Realisierbarkeit der technischen Voraussetzungen des Szenarios plausibel erscheint. Deshalb sollen hier kurz die derzeitigen Rahmenbedingungen dargelegt werden.
Die Diskussion über den Einsatz biometrischer Daten in Ausweispapieren ist schon länger im Gange. Insbesondere die umstrittene[47] Einigung über digitale Reisedokumente zwischen EU, den USA und der ICAO zeigt, dass der Einsatz von Biometrie und RFID-Technik im Zusammenhang realistisch ist[48].
Ebenso wurde schon dargelegt, dass die Bundesdruckerei GmbH eine neues Produkt mit der Bezeichnung „Verifier“ zur Kontrolle von digitalen Ausweisen mit RFID entwickelt hat. Es ist demzufolge naheliegend, die Funktionen dieses Gerätes genauer unter die Lupe zu nehmen.
Zuerst wurde im Internet auf der Website der Bundesdruckerei GmbH recherchiert.

---

[45] In der Praxis gibt es tatsächlich Beamte, die einige der Hooligans wiedererkennen können, wenn diese häufiger als Störer aufgefallen sind.
[46] Die Ingewahrsamnahme soll hier nicht rechtlich überprüft werden. Die Art und Zulässigkeit gerichtlichen Rechtschutzes soll ebenfalls nicht rechtlich überprüft werden.
[47] Vgl. Gundermann, in Die Flugdaten-Affäre. Internet: http://www.datenschutz.de/feature/detail/?featid=3. Stand 13.10.2004
[48] Schulzki-Haddouti, in Neue Reisepässe: Mit Sicherheit teuer. Internet: http://www.sicherheit-heute.de/index.php?cccpage=Verkehr. Stand 13.11.2004

Dort findet sich ein Produktdatenblatt[49] aus dem sich ergibt, dass der Verifier in verschiedenen Varianten (Standard, Basic, Compact, All-in-One) verfügbar ist. Diese unterscheiden sich in Puncto Funktionalität und vermutlich auch in der Bauform (zu den Abmessungen ist nichts Konkretes zu finden). Alle Varianten bieten diverse Funktionen zur Echtheitsprüfung von Ausweisdokumenten, z.B. mittels Infrarotlicht oder hochauflösender Kamera. Ebenso bieten alle Varianten optional die Funktion „RFID-Chips auslesen“ und sind kompatibel zu ICAO-konformen sowie anderen digitalen Ausweisen. Über die Reichweite des RFID-Readers ist leider nichts zu finden. Ebenso bleibt unklar, ob es eine tragbare Variante des Gerätes gibt.
In einem anschließenden Telefonat mit der Bundesdruckrei [50]GmbH war zu erfahren, dass es zur Zeit noch kein tragbares Gerät in Form eines „Handapparates“ gäbe. Die kleinste Variante sei derzeit für den mobilen Einsatz in Kraftfahrzeugen konzipiert. Die Reichweite der RFID-Lesefunktion hinge stark von den physikalischen Gegebenheiten ab. Über die eingesetzten kryptographischen Verfahren wollte man telefonisch keine Auskunft erteilen. Zum Einsatz der optischen Echtheitsprüfung muss der Ausweis unverdeckt vor den Verifier gehalten werden. Ob der RFID-Reader als einzelne Funktion nutzbar ist, d.h. ob das Gerät den RFID-Transponder eines Ausweises auch unabhängig von der optischen Echtheitsprüfung ausliest, konnte nicht in Erfahrung gebracht werden. Dies wäre jedoch ohnehin eine künstliche Limitierung der Funktionalität und ist deshalb in der Machbarkeitsbetrachtung ohne Belang. Ein Auslesen der biometrischen Daten aus dem RFID-Tag und eine Verifikation mittels Gesichtserkennung durch Vergleich mit den so genannten Livedaten ist im Verifier vorgesehen.
Zusammenfassend ist zu sagen, dass durch die uneinheitliche Berichterstattung und die Informationspolitik der Bundesdruckerei GmbH der Eindruck entsteht, als handele es sich um Gerät, dessen Eigenschaften mit dem Anwendungsfall variieren.
Da das Gerät erst kürzlich am Markt eingeführt wurde, kann hier von einer „Erstserie“ gesprochen werden. Im Zuge der Weiterentwicklung des Produktes wird dies sicherlich besser, zuverlässiger und kleiner werden. Was die Bundesdruckerei GmbH hier bietet, kann als das „Ford Model T“ der digitalen und biometrischen Ausweisdokumente angesehen werden.[51]

---

[49] Bundesdruckerei GmbH. Website.
Internet: http://www.bundesdruckerei.de/de/support/download/veri_d.pdf. Stand 25.9.2004
[50] Datum des Telefonats:16.09.2004, etwa um 14:35.
[51] Schneider, Bruce, in Schneier on Security. Internet:
http://www.schneier.com/blog/archives/2004/10/rfid_passports.html bzw.
http://www.iht.com/articles/541711.html. Stand 13.10.2004

Der fiktive Reader im Szenario ist technisch gesehen nur eine „verbesserte“ Version des tatsächlich existierenden Verifiers. Das Szenario ist deshalb keinesfalls „Science-Fiction“, sondern in greifbarer Nähe.

III. Rechtliche Prüfung der Ausstellung eines RFID-Personalausweises – de lege lata

1. Rechtsgrundlage

Zunächst ist die Rechtmäßigkeit der Ausstellung eines mit RFID-Technik ausgestatteten Personalausweises zu prüfen. Die Ausstellung eines mit RFID-Technik ausgestatteten Personalausweises stellt einen Verwaltungsakt dar.
Die Ausstattung des Personalausweises mit RFID-Technik und biometrischen Merkmalen wäre nur dann rechtmäßig, wenn sie auf einer ihrerseits verfassungsmäßigen Rechtsgrundlage beruht.
Als Rechtsgrundlage kommt § 1 Abs. 2-5 PAuswG i.V.m. § 1 Personalausweismusterverordnung sowie i.V.m. den jeweiligen Durchführungsbestimmungen der Länder in Frage. Als Beispiel hierfür sei die Durchführungsverordnung in Hessen genannt.

§ 1 Hessisches Ausführungsgesetz zum Gesetz über Personalausweise
(1) Die nach § 1 Abs. 1 des Gesetzes über Personalausweise in der Fassung vom 21. April 1986 (BGBl. I S. 548) bestehende Pflicht, einen Personalausweis oder vorläufigen Personalausweis (Ausweis) zu besitzen und ihn auf Verlangen einer zur Prüfung der Personalien ermächtigten Behörde vorzulegen, gilt für alle Personen, die nach dem Hessischen Meldegesetz vom 14.Juni 1982 (GVBl. I S.126), zuletzt geändert durch Gesetz vom 27. Juli 1993 (GVBl. I S. 344), meldepflichtig sind, und für Personen, die sich in Hessen gewöhnlich aufhalten, ohne eine Wohnung zu haben.
(2) Personen, deren Lebensumstände nicht erwarten lassen, dass ein Ausweis für die Feststellung der Identität und für die Verwendung im Rechtsverkehr erforderlich ist, können von der Ausweispflicht befreit werden. Diese Tatsache darf nur zur Feststellung der Personalien dieser Personen den dazu ermächtigten öffentlichen Stellen mitgeteilt werden.
(3) Deutsche, die der Ausweispflicht nicht unterliegen, können auf Antrag einen Ausweis erhalten.
(4) Niemand darf mehr als einen Ausweis besitzen.
§ 5 Hessisches Ausführungsgesetz zum Gesetz über Personalausweise
(1) Der Ausweis wird auf Antrag ausgestellt. Dazu ist das persönliche Erscheinen erforderlich, soweit die Personalausweisbehörde keine Ausnahme aus wichtigem Grund zuläßt.
(2) Jugendliche sind drei Monate vor Vollendung des 16. Lebensjahres fähig zur Vornahme von Verfahrenshandlungen nach diesem Gesetz. Für minderjährige ausweispflichtige Personen, die es unterlassen, einen Ausweis zu beantragen, oder für ausweispflichtige Personen, die aus rechtlichen Gründen nicht fähig zur Vornahme von Verfahrenshandlungen sind, hat diejenige Person den Antrag zu stellen, die als Sorgeberechtigte den Aufenthalt zu bestimmen hat.
(3) Bei der Antragstellung sind die nach §1 Abs. 2 Satz 2 des Gesetzes über Personalausweise in den Ausweis aufzunehmenden Angaben zu machen und die Nachweise zu erbringen, die zur Feststellung der Identität und Staatsangehörigkeit notwendig sind. Soweit dies zur Bearbeitung des Antrags erforderlich ist, sind auch Angaben zu machen über Aufenthaltsort, Ausstellungsbehörde, -datum und Gültigkeitsdauer des zuletzt ausgestellten Ausweises sowie Vor- und Familienname, Doktorgrad, Anschrift und Tag der Geburt des gesetzlichen Vertreters. Es sind die erforderlichen Unterschriften zu leisten und ein Lichtbild in der Größe von 45 mm x 35 mm in Hochformat ohne Rand abzugeben, das aus neuerer Zeit stammen und das Gesicht in einer Höhe von mindestens 20 mm zweifelsfrei erkennen lassen muss. Das Lichtbild muss die Person ohne Kopfbedeckung zeigen, soweit die Personalausweisbehörde keine Ausnahme zuläßt. Der Hintergrund muss heller als die Gesichtspartie sein.
(4) Die Personalausweisbehörde kann Auskünfte von anderen öffentlichen Stellen einholen, wenn dies zur Feststellung der Identität erforderlich ist. Reichen diese Maßnahmen nicht aus, kann die Personalausweisbehörde Gegenüberstellungen durchführen oder erkennungsdienstliche Maßnahmen im Sinne des § 19 Abs. 1 des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung in der Fassung vom 31. März 1994 (GVBl. I S. 174) durch die Polizeibehörde veranlassen. Die dabei anfallenden Unterlagen dürfen zu keinem anderen Zweck verwendet werden und sind nach Feststellung der Identität zu vernichten.

Hinsichtlich der auf den RFID-Chips gespeicherten Angaben ist zu berücksichtigen, dass gemäß § 1 Abs. 7 S. 1 PAuswG die Ausweismuster durch das Bundesministerium des Innern per Rechtsverordnung festzulegen sind. Nach § 1 Personalausweismusterverordnung ist der Personalausweis nach dem in Anlage 1 beigefügtem Muster auszustellen.

§ 1 PersAuswMustV Muster für den Personalausweis
Der Personalausweis der Bundesrepublik Deutschland ist nach dem in der Anlage 1 abgedruckten Muster auszustellen.

Die Ausstattung mit RFID-Technik ist bislang nicht in der Anlage 1 zu § 1 Personalausweismusterverordnung geregelt. Dementsprechend ist zum jetzigen Zeitpunkt eine solche Ausstattung nach dem PAuswG unzulässig. Damit ist auch die Erfassung der Angaben auf dem RFID-Chip des Ausweises nicht zulässig. Entsprechendes gilt für die Durchführungsbestimmungen der Länder. Eine Ausstattung des Personalausweises mit RFID-Technik ist nach der gegenwärtigen Gesetzeslage somit nicht erlaubt.
Für die Ausstattung mit biometrischen Merkmalen fehlt es zum einen an einer entsprechenden PersAuswMustverordnung. Zum anderen ist die Einbringung

solcher Merkmale zwar in § 1 Abs. 4 PAuswG grundsätzlich zugelassen. Aber § 1 Abs. 5 PAuswG verlangt zur Festlegung der Arten und weiterer Einzelheiten der biometrischen Merkmale ein Bundesgesetz. Auch an diesem fehlt es. Auch aus diesem Grund wäre die Einbringung biometrischer Merkmale daher unzulässig. Mithin wäre die Maßnahme „Ausstellung eines RFID-Personalausweises mit Biometriemerkmalen“ nach aktueller Gesetzeslage rechtswidrig.

IV. Rechtliche Prüfung der Ausstellung eines RFID-Personalausweises – de lege ferenda

Allerdings besteht die Möglichkeit, dass ein entsprechendes „Biometrieausweisgesetz“ beschlossen wird, dass die Anforderungen des § 1 Abs. 5 PAuswG erfüllt. Zudem könnte das zuständige Bundesministerium des Innern eine entsprechende Verordnung erlassen. Für die weitere Prüfung wird davon ausgegangen, dass eine Änderung des PAuswG beschlossen und eine Verordnung erlassen wird, die den Einsatz von RFID-Technik und die Einbringung biometrischer Daten im Ausweis im geschilderten Umfang für zulässig erachten. Diese könnten wie folgt gefasst werden:

§ 1 PAuswG Ausweispflicht
(…)
(4) Der Personalausweis darf neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden. Auch die in Absatz 2 Satz 2 aufgeführten Angaben über die Person dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Personalausweis eingebracht werden.
(5) ~~Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Absatz 4 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt.~~

[neu] Der Personalausweis enthält eine biometrische Erfassung des Gesichts sowie die biometrische Erfassung der Fingerabdrücke des Daumens der rechten Hand und des Daumens der linken Hand des Ausweisinhabers.
Eine bundesweite Datei wird nicht eingerichtet.
[neu] (6) Die gemäß Absätze 3-5 enthaltenen Daten werden zusätzlich mittels eines RFID-Chips auf dem Personalausweis erfasst.
(7) Für die erstmalige Ausstellung des Personalausweises sowie für die Neuausstellung nach Ablauf der Gültigkeitsdauer ist eine Gebühr von acht Euro zu erheben. Die erstmalige Ausstellung des Personalausweises an Personen, die das 21. Lebensjahr noch nicht vollendet haben, ist gebührenfrei. Von der Erhebung einer Gebühr kann abgesehen werden, wenn der Gebührenpflichtige bedürftig ist.
(8) Die Muster der Ausweise bestimmt das Bundesministerium des Innern durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf. Der Personalausweis ist Eigentum der Bundesrepublik Deutschland.

§ 1 PersAuswMustV Muster für den Personalausweis
Der Personalausweis der Bundesrepublik Deutschland ist nach dem in der Anlage 1 abgedruckten Muster auszustellen. [neu] Die Ausstattung des Personalausweises mit RFID-Chip und biometrischen Merkmalen erfolgt nach den in Anlage 2 aufgeführten technischen Musterspezifikationen.[52]

Es wird davon ausgegangen, dass die länderechtlichen Bestimmungen ebenfalls entsprechend angepasst werden.

Fraglich ist, ob die Ausweisausstellung bei dieser erfundenen Rechtslage zulässig wäre. [53]

1. Rechtsgrundlage

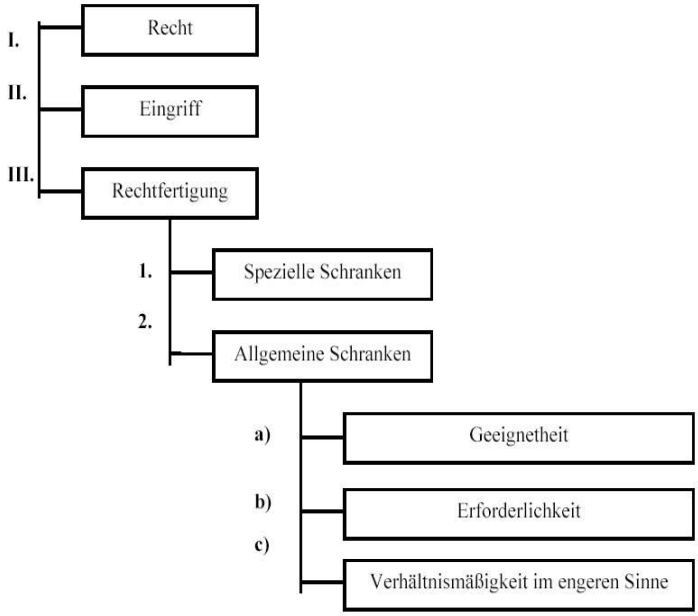
Es ist zu untersuchen, ob das fiktive PAuswG eine wirksame Rechtsgrundlage wäre.

a) Formelle Verfassungsmäßigkeit

Das PAuswG ist hinsichtlich Kompetenz, Form und Verfahren des Gesetzgebungsverfahrens verfassungsgemäß ergangen.[54]

b) Materielle Verfassungsmäßigkeit: Vereinbarkeit mit Grundrechten[55]

Zur Erläuterung: Prüfungsschema Grundrechtsprüfung



[52] Es wird davon ausgegangen, dass in der Anlage 2 entsprechende Vorgaben geregelt werden.

[53] Dabei wird auf die Prüfung der formellen und materiellen Rechtmäßigkeit der Personalausweismusterverordnung verzichtet. Denn hierbei handelt es sich um eine akzessorische Konkretisierung des PAuswG. Auf eine eingehende Prüfung der länderechtlichen Vorschriften wird nach Absprache mit den Betreuern verzichtet.

[54] Auf die eingehende Prüfung der formellen Verfassungsmäßigkeit wird nach Absprache mit den Betreuern verzichtet.

[55] S. Viola Schmid, Skript Grundzüge des Öffentlichen Rechts WS 03/04.

aa) Recht

Betroffen sein könnten die Grundrechte auf freie Entfaltung der Persönlichkeit, Art. 2 Abs. 1 GG und das Recht auf informationelle Selbstbestimmung, Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG. Das Recht auf allgemeine Handlungsfreiheit tritt hinter das Recht auf informationelle Selbstbestimmung zurück.[56] Das Bundesverfassungsgericht hat hierzu entschieden[57], dass das Grundrecht auf informationelle Selbstbestimmung die Befugnis des Einzelnen gewährleistet, grundsätzlich über die Preisgabe seiner persönlichen Daten zu bestimmen. Jedoch ist dies nicht schrankenlos gewährleistet – er muss Einschränkungen dieses Rechts zu Gunsten eines überwiegenden Allgemeininteresses hinnehmen. Weiter könnte das Grundrecht auf Freizügigkeit, welches Art. 11 Abs. 1 GG gewährleistet, betroffen sein. Durch dieses Grundrecht wird die Freiheit, einen bestimmten Ort aufzusuchen bzw. sich an einem bestimmten Ort aufzuhalten, garantiert.[58] Dazu könnte auch die Freiheit, dies ohne staatliche Beobachtung tun zu können. Kern des Grundrechtsschutzes ist aber der „Zug“ von einem Ort zum anderen, etwa zum Wohnungswechsel. Die Ausstellung von Ausweisen, mit RFID-Technik oder ohne, betrifft diese Freiheit nicht. Eine Beschränkung des „freien Zuges“ liegt nicht vor. Zwar kann eine Identifizierung durch Ausweise ein Hilfsmittel sein, dass Maßnahmen erleichtert, die zu einer Beschränkung der Fortbewegungsfreiheit führen. Beispiel ist etwa die Festsetzung von Straftätern aufgrund der Identifizierung. Dabei erfolgt die Beeinträchtigung jedoch nicht unmittelbar[59]. Aus diesen Gründen ist der Schutzbereich des Art. 11 Abs. 1 GG nicht eröffnet.

bb) Eingriff

Die Erfassung personenbezogener Daten (Namen, Geburtsdatum, Fingerabdrücke, ...) stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar.

cc) Rechtfertigung

(a) Spezielle Schranken

Der Eingriff könnte gerechtfertigt sein.

Als Rechtfertigung kommt die spezielle Schranke des Art. 2 Abs. 1 GG in Frage. Art. 2 Abs. 1 GG schränkt die freie Entfaltung der Persönlichkeit zugunsten der Rechte anderer, der verfassungsmäßigen Ordnung oder des Sittengesetzes ein. Hier kommt die Schranke „verfassungsmäßige Ordnung“ in Betracht. Der

[56] Eine eingehende Darstellung der Konkurrenzfragen unterbleibt nach Absprache mit den Betreuern.
[57] BverfGE 65,1 (43)
[58] Kunig, in: Münch/Kunig, GGK I, 5 Aufl. 2000, Rn 11 zu Art. 11
[59] Kunig, in: Münch/Kunig, GGK I, 5 Aufl. 2000, Rn 19 zu Art. 11

Begriff der „verfassungsmäßigen Ordnung“ ist weit auszulegen. „Verfassungsmäßige Ordnung“ umfasst die gesamte Rechtsordnung, soweit sie formell und materiell mit der Verfassung im Einklang steht (Verfassungsmäßigkeit). Das Recht auf informationelle Selbstbestimmung kann durch das PAuswG als spezieller Schranke eingeschränkt werden, wenn dieses der Schranken-Schranke „Verhältnismäßigkeit im weiteren Sinne“ entspricht. [60]

Geeignetheit	Eingriff muss geeignet sein, um Schutz des Rechtsguts, das Eingriffsrechtfertigung bildet (Rechtfertigungsrechtsgut), zu bewirken – Tauglichkeit des Mittels für den Zweck
Erforderlichkeit	Negativ/Positiv: Es darf keine Maßnahme geben, die für den Schutz des Rechtfertigungsrechtsguts genauso geeignet und weniger eingreifend ist
Verhältnismäßigkeit im engeren Sinne	Eingriff in das Eingriffsrechtsgut darf nicht außer Verhältnis zum Schutz des Rechtfertigungsrechtsguts stehen – Grundrechtseingriff darf in seiner Intensität nicht außer Verhältnis zum angestrebten Ziel stehen

(b) Legitimer Zweck und Geeignetheit (Allgemeine Schranke)

Der Eingriff in die informationelle Selbstbestimmung muss geeignet sein, um den Schutz des Rechtfertigungsrechtsguts (öffentliche Sicherheit, Schutz des Eigentums und der Gesundheit der Bevölkerung) zu bewirken. Zweck der Gesetztesänderung ist es, Ausweispapiere zu schaffen, die eine eindeutige Identifikation der Inhaber ermöglichen. Ausweispapiere sollen fälschungs- und missbrauchssicher sein. Durch eindeutige Identifikation sollen insbesondere Sicherheitsinteressen verfolgt werden. Das Gesetz soll dazu beitragen, die Funktionsfähigkeit staatlicher Einrichtungen, die Gesundheit der Bevölkerung und den Schutz des Eigentums vor Angriffen zu gewähren. Das PAuswG ermöglicht, Missbräuche effektiv festzustellen. Es erleichtert die Identifikation potenzieller Straftäter durch die Möglichkeit des kontaktlosen Auslesens der Ausweisdaten. Es ist somit geeignet, zur Zweckerreichung beizutragen.

(c) Erforderlichkeit (Allgemeine Schranke)

Es ist zu prüfen, ob es eine Maßnahme gibt, die dem Rechtfertigungsrechtsgut ebenso dient, aber weniger das Eingriffsrechtsgut („informationelle Selbstbestimmung“) beschränkt .

[60] S. Viola Schmid, Skript Grundzüge des Öffentlichen Rechts WS 03/04; Vgl. Ipsen, Rn 303

Als erstes ist hier die „klassische“ Identitätsfeststellung zu nennen. Die BGS Beamten machen Stichproben, um die Hooligans aufzufinden. Alle Stichproben sind mit Zeitaufwand verbunden. Die Kontrolle kann in der kurzen zur Verfügung stehenden Zeit am Bahnhof (der Bahnsteig muss für die Passagiere der folgenden Züge wieder frei sein), bei weitem nicht so effizient wie mit RFID Technik durchgeführt werden. Weiterhin könnte dieses Verfahren beim Betroffenen als unangenehm empfunden werden: Er wird öffentlich von einer staatlichen Stelle kontrolliert. Dies könnte u.a. das Bild seiner Persönlichkeit bei den Mitreisenden verändern, da insbesondere er zur Kontrolle ausgesucht wurde. Alternativ könnte anstatt Stichproben auch eine Art Schleuse zum Einsatz kommen, etwa ein Drehkreuz, das die Passagiere zur Ausweiskontrolle passieren müssen. Dies würde dem Persönlichlichkeitsbild des Einzelnen nicht schaden, jedoch ist mit noch erheblicheren Verzögerungen zu rechnen, als bei der Kontrolle durch Stichproben. Die klassische Identitätsfeststellung ist aus diesen Gründen nicht als gleichwertig anzusehen.
Weiterhin ist der Einsatz von Smartcards mit biometrischen Daten als Ausweisdokument in Betracht zu ziehen. Der Vorteil dieser Smartcard im Vergleich zum klassischen Personalausweis ist die Überprüfung der Identität des Betroffenen. Es ist ein Reader vorstellbar, der ähnlich dem Reader im Szenario arbeitet, jedoch muss der Betroffene zum Auslesen seiner Daten den Ausweis in den Reader einführen. Die Smartcard hat zwar deutliche Vorteile in Puncto Identitäts- und Echtheitsprüfung, jedoch muss hier in allen anderen Punkten wie beim Einsatz des klassischen Personalausweises argumentiert werden (siehe oben). Der Smartcard-Personalausweis ist deshalb nicht als gleichwertig anzusehen.
Ebenso sollte ein reines[61] Biometrieverfahren zur Identitätsfeststellung in Betracht gezogen werden. Hierzu wäre ein zentrale Datei biometrischer Merkmale aller Bundesbürger notwendig.[62] Die Lesegeräte der BGS Beamten ermitteln dann mittels Bild- und/oder Tonaufnahmen und Abgleich mit der zentralen Datei die Identität des Betroffenen. Jedoch ist die Fehlerrate der biometrischen Identifikationsverfahren mit Ausnahme des Iris-Scan noch relativ hoch, wobei der Iris-Scan ein Auflegen des Auges auf einen Scanner mit sich bringt. Eine Identitätsfeststellung ist für den Betroffenen damit noch weitaus unangenehmer als bei Vorzeigen eines Ausweises. Auch könnte argumentiert werden, dass dem Betroffenen die Möglichkeit genommen wird, seinen „Ausweis“ nicht mit sich zu führen. Eine klare Antwort hierzu ist an dieser Stelle

[61] Es ist ein Verfahren gemeint, bei dem der Betroffene seine biometrischen Daten nicht mehr auf einem Medium (etwa einer Smartcard) mit sich führen muss.
[62] Im Rahmen der Erforderlichkeit wird davon abgesehen, dass eine Zentrale Datei biometrischer Daten ist in PAuswG explizit verboten ist.

in Kürze nicht möglich, da diese grundlegend rechtsphilosophisch betrachtet werden müsste. Jedoch reicht der erste Kontrapunkt schon aus, um dieses Verfahren abzulehnen.
Die Ausstattung der Ausweispapiere mit RFID-Technik ist also erforderlich. Eine gleich wirksame mildere Möglichkeit ist nicht ersichtlich.
Es kann der Einschätzungsprärogative des Gesetzgebers überlassen werden, die Möglichkeit, RFID-Chips technisch kontaktlos auszulesen, für wirksamer zu halten als die persönliche Auslegung schriftlicher Ausweisdaten.

(d) Verhältnismäßigkeit im engeren Sinne (Allgemeine Schranke)

Weiter ist der Qualität des Eingriffs in das Eingriffsrechtsgut die Qualität der Förderung des Rechtfertigungsrechtsguts gegenüberzustellen.
Rechtfertigungsrechtsgut sind die Sicherheitsinteressen des Staates, die sich mit dem Funktionieren der staatlichen Einrichtungen, dem Eigentumsschutz und dem Schutz der Gesundheit der Bevölkerung umschreiben lassen. Dem stehen die beeinträchtigten Grundrechte gegenüber. Zwar sind die informationelle Selbstbestimmung und das Recht auf Freizügigkeit wichtige Freiheitsgrundrechte. Durch die bloße Erfassung von Ausweisdaten mittels RFID-Chip wird aber nicht sehr intensiv in diese eingegriffen. Zwar können die Daten unbemerkt und kontaktlos ausgelesen werden und der Inhaber selbst kann nicht einmal die Daten überprüfen, also selbst auslesen. Doch auch bei einer Folgebetrachtung, die Missbrauchsgefahren berücksichtigt, ergibt sich kein anderes Bild. Denn ein stärkerer Eingriff kann insbesondere durch gesetzliche Regelungen zur Nutzung der RFID-Ausweise unterbunden werden. Das gilt auch für die Gefahr eines Missbrauchs der immensen neuen Datenmengen. Diese müssen wirksam durch technische und organisatorische Maßnahmen geschützt werden. [63] Dagegen wiegt das Interesse des Staates an effizienter Identifizierung möglicher Straftäter sehr hoch. Um seine Steuerungs- und Schutzaufgaben verwirklichen zu können ist der Staat auf effektive Mittel angewiesen. Diese dienen zudem zugleich dem Schutz der Bevölkerung. Wegen der ohnehin bestehenden Ausweispflicht und den damit korrespondierenden polizeilichen Befugnissen zur Identitätsfeststellung, spricht nichts Entscheidendes dagegen, auch die effiziente Identifizierung mittels RFID und Biometrie zuzulassen. Letztlich kann hier aufgrund der Einschätzungsprärogative des Bundes die Angemessenheit bejaht werden.

[63] Vgl. § 9 BDSG nebst Anlage.

2. Formelle Rechtmäßigkeit

Die Ausstellung des Personalausweises ist hinsichtlich Kompetenz, Verfahren und Form des Verwaltungsverfahrens ordnungsgemäß erfolgt.[64]

3. Materielle Rechtmäßigkeit

Die Voraussetzungen der fiktiven Rechtsgrundlage (PersAuswMustVO i.V.m. PAuswG) sind eingehalten. Das gilt auch für die Voraussetzungen, die die länderrechtlichen Durchführungsvorschriften stellen.[65]

4. Ergebnis: Ausstellung von Biometrie-RFID-Ausweisen.

Bei Zugrundelegung der fiktiven Rechtslage wäre die Ausstellung des Personalausweises mit RFID-Technik und biometrischen Merkmalen rechtmäßig.

V. Rechtmäßigkeit des Auslesens von Biometrie-RFID-Ausweisen.

Sowohl das Bundesdatenschutzgesetz (BDSG) als auch das Hessische Gesetz für Sicherheit und Ordnung (HSOG) oder das Telekommunikationsgesetz (TKG) könnten einschlägige Vorschriften für den zu prüfenden Fall enthalten. Das Bundesgrenzschutzgesetz ist jedoch als Spezialgesetz für den Bundesgrenzschutz erlassen worden und daher vorrangig zu untersuchen. Es stellt sich die Frage, um welche Art Maßnahme es sich beim Auslesen von RFID-Ausweisen handelt –und ob diese rechtmäßig erfolgen kann.

1. Identitätsfeststellung

Beim Auslesen könnte es sich um eine Identitätsfeststellung im Sinne des BGSG handeln.

a) Rechtsgrundlage

Das Auslesen der Ausweise kann auf § 23 Abs. 3 S. 1 i.V.m. Abs. 1 BGSG beruhen.

---

[64] Auf die eingehende Prüfung der formellen Rechtmäßigkeit wird nach Absprache mit den Betreuern verzichtet.

[65] Auf die eingehende Prüfung der weiteren Voraussetzungen der Ausweisausstellung wird nach Absprache mit den Betreuern verzichtet.

§ 23 BGSG Identitätsfeststellung und Prüfung von Berechtigungsscheinen
(1) Der Bundesgrenzschutz kann die Identität einer Person feststellen
1. zur Abwehr einer Gefahr,
2. zur polizeilichen Kontrolle des grenzüberschreitenden Verkehrs,
3. im Grenzgebiet bis zu einer Tiefe von dreißig Kilometern zur Verhinderung oder Unterbindung unerlaubter Einreise in das Bundesgebiet oder zur Verhütung von Straftaten im Sinne des § 12 Abs. 1 Nr. 1 bis 4,
4. wenn die Person sich in einer Einrichtung des Bundesgrenzschutzes (§ 1 Abs. 3), einer Anlage oder Einrichtung der Eisenbahnen des Bundes (§ 3), einer dem Luftverkehr dienenden Anlage oder Einrichtung eines Verkehrsflughafens (§ 4), dem Amtssitz eines Verfassungsorgans oder eines Bundesministeriums (§ 5) oder an einer Grenzübergangsstelle (§ 61) oder in unmittelbarer Nähe hiervon aufhält und Tatsachen die Annahme rechtfertigen, dass dort Straftaten begangen werden sollen, durch die in oder an diesen Objekten befindliche Personen oder diese Objekte selbst unmittelbar gefährdet sind, und die Feststellung der Identität auf Grund der Gefährdungslage oder auf die Person bezogener Anhaltspunkte erforderlich ist, oder
5. zum Schutz privater Rechte.
(…)
(3) Der Bundesgrenzschutz kann zur Feststellung der Identität die erforderlichen Maßnahmen treffen. Er kann den Betroffenen insbesondere anhalten, ihn nach seinen Personalien befragen und verlangen, dass er Ausweispapiere zur Prüfung aushändigt. Bei der polizeilichen Kontrolle des grenzüberschreitenden Verkehrs kann derBundesgrenzschutz ferner verlangen, dass der Betroffene Grenzübertrittspapiere vorlegt. Der Betroffene kann festgehalten und zur Dienststelle mitgenommen werden,wenn seine Identität oder seine Berechtigung zum Grenzübertritt auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten festgestellt werden kann. Unter den Voraussetzungen des Satzes 4 können der Betroffene sowie die von ihm mitgeführten Sachen nach Gegenständen, die der Identitätsfeststellung dienen, durchsucht werden.
(4) Der Bundesgrenzschutz kann, soweit es zur Erfüllung seiner Aufgaben erforderlich ist, verlangen, dass Berechtigungsscheine, Bescheinigungen, Nachweise oder sonstige Urkunden zur Prüfung ausgehändigt werden, wenn der Betroffene auf Grund einer Rechtsvorschrift verpflichtet ist, diese Urkunden mitzuführen.

b) Formelle Rechtmäßigkeit

Das Auslesen der RFID-Ausweise erfolgt hinsichtlich Zuständigkeit, Kompetenz und Verfahren des Verwaltungsverfahrens rechtmäßig.[66]

c) Materielle Rechtmäßigkeit

aa) Anlass

(a) Alternative 1: § 23 Abs. 1 Nr. 1 BGSG

Es müsste danach eine konkrete Gefahr für die öffentliche Sicherheit oder Ordnung bestehen. Diese müsste im Aufgabenbereich des BGS vorliegen (§ 14 Abs. 2 BGSG).

§ 14 BGSG Allgemeine Befugnisse
(1) Der Bundesgrenzschutz kann zur Erfüllung seiner Aufgaben nach den §§ 1 bis 7 die notwendigen Maßnahmen treffen, um eine Gefahr abzuwehren, soweit nicht dieses Gesetz die Befugnisse des Bundesgrenzschutzes besonders regelt.
(2) Gefahr im Sinne dieses Abschnitts ist eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit oder Ordnung im Bereich der Aufgaben, die dem Bundesgrenzschutz nach den §§ 1 bis 7 obliegen. Eine erhebliche Gefahr im Sinne dieses Abschnitts ist eine Gefahr für ein bedeutsames Rechtsgut, wie Bestand des Staates, Leben, Gesundheit, Freiheit, wesentliche Vermögenswerte oder andere strafrechtlich geschützte Güter von erheblicher Bedeutung für die Allgemeinheit.

Zunächst müsste der BGS im Rahmen seiner Aufgaben tätig werden. Im Szenario kommt eine Aufgabenzuweisung nach § 3 Abs. 1 S. 1 BGSG in Betracht.

[66] Auf die eingehende Prüfung der formellen Rechtmäßigkeit wird nach Absprache mit den Betreuern verzichtet.

BGSG § 3 Bahnpolizei
(1) Der Bundesgrenzschutz hat die Aufgabe, auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes Gefahren für die öffentliche Sicherheit oder Ordnung abzuwehren, die
1. den Benutzern, den Anlagen oder dem Betrieb der Bahn drohen oder
2. beim Betrieb der Bahn entstehen oder von den Bahnanlagen ausgehen.

(b) Örtlicher Geltungsbereich des BGSG

Da der Einsatzbereich des BGS sich im Szenario auf das Gebiet der Bahnanlagen der Eisenbahnen des Bundes beschränkt, ist der örtliche Geltungsbereich des BGSG eröffnet.

(c) Sachlicher Geltungsbereich: Gefahr für die öffentliche Sicherheit oder Ordnung

Voraussetzungen für die Eröffnung des sachlichen Geltungsbereiches ist das Vorliegen einer Gefahr für die öffentliche Sicherheit und Ordnung (§ 3 Abs. 1 i.V.m. § 14 Abs. 2 S. 1 BGSG).
Die öffentliche Sicherheit umfasst die gesamte Rechtsordnung, den Staat und seine Einrichtungen, sowie die Rechtsgüter der Einzelnen. Die Gefahr liegt im Szenario in der Wahrscheinlichkeit eines Schadenseintritts, sofern der BGS nicht eingreift. So könnte es während der Zugfahrt zu von Hooligans provozierten Auseinandersetzungen mit den Passagieren oder zu Sachbeschädigungen kommen. Durch die damit verbundenen Straftaten Körperverletzung (§§ 223f StGB) bzw. Sachbeschädigung (§ 303 StGB) würden die Rechtsordnung (StGB als Teil der Rechtsordnung) und die Rechtsgüter Einzelner verletzt. Eine Gefahr für die öffentliche Sicherheit besteht. Diese ist auch hinreichend konkret, da aktuell Straftaten mit hoher Wahrscheinlichkeit begangen werden sollen.
Das BGSG findet jedoch nur Anwendung, wenn die Gefahr den Benutzern, den Anlagen oder dem Betrieb der Bahnen droht (§ 3 Abs. 1 Satz 1 BGSG). Die Gefahr droht den Passagieren der Bahn, die im Sinne der Vorschrift als Benutzer der Anlagen gesehen werden. Weiterhin sind die Bahnanlagen selbst gefährdet. Damit ist der sachliche Geltungsbereich eröffnet.
Demnach liegen die Voraussetzungen des § 23 Abs. 1 Nr. 1 BGSG vor.

(d) Alternative 2: § 23 Abs. 1 Nr. 4 BGSG

Alternativ könnte ein Recht zur Identitätsfeststellung auch auf § 23 Abs. 1 Nr. 4 gestützt werden. In Betracht kommt hier der Fall, dass sich Personen in einer Anlage oder Einrichtung der Eisenbahnen des Bundes aufhalten. Das ist gegeben. Es besteht nach der Szenariobeschreibung auch auf Tatsachen begründeter Verdacht, dass die dort befindlichen Personen durch bevorstehende Straftaten unmittelbar gefährdet werden.

bb) Identitätsfeststellung

Der BGS kann die zur Identitätsfeststellung erforderlichen Maßnahmen treffen. Dazu kann er insbesondere den Betroffenen nach seinen Personalien fragen und die Aushändigung der Ausweispapiere zur Prüfung verlangen (§ 23 Abs. 3 BGSG).
Es stellt sich zunächst die Frage, ob eine Überprüfung mittels RFID und Biometrie noch unter den Begriff „Identitätsfeststellung“ im Sinne dieser Vorschrift fällt. Dem reinen Wortlaut nach kann das bejaht werden. Historisch ist unter Identitätsfeststellung eine Überprüfung der Personalien zu verstehen. Dies kann etwa anhand eines klassischen Ausweispapiers geschehen. In systematischer Hinsicht ist zunächst § 24 BGSG zu beachten. Dieser ermöglicht erkennungsdienstliche Maßnahmen, soweit eine Identitätsfeststellung auf andere Weise nicht möglich ist.

BGSG § 24 Abs. 1 „Erkennungsdienstliche Maßnahmen“
(1) Der Bundesgrenzschutz kann erkennungsdienstliche Maßnahmen vornehmen, wenn
*1. eine **nach § 23 Abs. 1 oder 2 zulässige Identitätsfeststellung** auf andere Weise nicht oder nur unter erheblichen Schwierigkeiten möglich ist oder*
2. dies zur Verhütung von Straftaten im Sinne des § 12 Abs. 1 erforderlich ist, weil der Betroffene verdächtig ist, eine solche Straftat begangen zu haben und wegen der Art oder Ausführung der Tat die Gefahr einer Wiederholung besteht.

Erkennungsdienstliche Maßnahmen sind etwa die Abnahme von Fingerabdrücken oder das Anfertigen von Lichtbildern. Zwar könnte man argumentieren, der Abgleich von Biometriedaten und tatsächlichen biometrischen Merkmalen der Person sei etwa dem Abnehmen von Fingerabdrücken zur Identifizierung vergleichbar. Deswegen bedürfe er einer eigenen Regelung. Dagegen sprechen aber verschiedene Gründe. Zum eine erfordert die Identifizierung anhand von erkennungsdienstlichen Maßnahmen Zusatzwissen, etwa anhand von Dateien. Die Identifizierung einer Person anhand ihrer biometrischen Merkmale ist demgegenüber mit der klassischen Identifizierung anhand eines Lichtbildes vergleichbar. Sie ist jedoch deutlich effizienter. Das kann für Unbeteiligte sogar den Vorteil haben, dass sie weniger Umstände bei der Kontrolle haben. Wenn zur Identitätsfeststellung erkennungsdienstliche Maßnahmen ergriffen werden können, weil eine „übliche“ Identitätsfeststellung nicht oder nur unter erheblichen Schwierigkeiten möglich ist, spricht dies dafür, dass erkennungsdienstliche Maßnahmen insbesondere dann vorgenommen werden können, wenn eine Überprüfung etwa anhand eines Lichtbildausweises nicht möglich ist. Im vorliegenden Szenario erfolgt die Überprüfung aber gerade anhand des Ausweises. Für den Fall, dass jemand keinen Ausweis bei sich führt, käme allerdings die Überprüfung anhand erkennungsdienstlicher Maßnahmen in Betracht. Zwar nennt § 23 Abs. 3 als Beispiel für eine Maßnahme zur Identitätsfeststellung das Aushändigen der Ausweispapiere. Bei der im Szenario

beschriebenen Kontrolle erfolgt die Überprüfung hingegen automatisch. Aber das Aushändigen wird nur als eine mögliche - „insbesondere“- Maßnahme beschrieben. Darüber hinaus sind weitere Maßnahmen durchaus zulässig. Problematisch ist weiter, dass eine Identitätsfeststellung auf den beschriebenen, klassischen Wegen, i.d.R. offen erfolgt. Bei RFID-Biometrieausweisen ist eine heimliche Kontrolle möglich. Eine Beschränkung auf offene Kontrollen ist aber weder durch Gesetzeswortlaut noch Sinn und Zweck zwingend. Insbesondere ist vorstellbar, dass eine Identitätsfeststellung etwa bei Bewusstlosen erfolgt, also gerade nicht offen gegenüber dem Adressaten der Maßnahme. Dies ist der RFID-Kontrolle vergleichbar. Letztlich handelt es sich also bei der Kontrolle des RFID-Biometrie-Ausweises um eine Identitätsfeststellung, die von § 23 BGSG erfasst wird.

cc) Ermessen und Verhältnismäßigkeit

Die Kontrolle muss ermessensgerecht und verhältnismäßig erfolgen (§§ 15,16 BGSG).

§ 15 BGSG Grundsatz der Verhältnismäßigkeit
(1) Von mehreren möglichen und geeigneten Maßnahmen ist diejenige zu treffen, die den einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt.
(2) Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.
(3) Eine Maßnahme ist nur solange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

§ 16 BGSG Ermessen, Wahl der Mittel
(1) Der Bundesgrenzschutz trifft seine Maßnahmen nach pflichtgemäßem Ermessen.
(2) Kommen zur Abwehr einer Gefahr mehrere Mittel in Betracht, so genügt es, wenn eines davon bestimmt wird. Dem Betroffenen ist auf Antrag zu gestatten, ein anderes ebenso wirksames Mittel anzuwenden, sofern die Allgemeinheit dadurch nicht stärker beeinträchtigt wird.

Anzeichen für eine Ermessensüberschreitung liegen nicht vor. Die Maßnahme ist auch verhältnismäßig. Sie ist insbesondere erforderlich im Sinne des § 23 Abs. 1 Nr. 4 BGSG aufgrund der Gefährdungslage und im Sinne des § 23 Abs. 3 S. 1 BGSG als Maßnahme zur Identitätsfeststellung. Bei der Verhältnismäßigkeitsprüfung ist zu beachten, dass es hier besonders auf die Wahrscheinlichkeit der drohenden Gefahr und das drohende Ausmaß eines Schadens ankommt, um im jeweiligen Einzelfall die Angemessenheit zu bejahen. Hier kann nach der Szenariobeschreibung von einem ausreichenden, konkreten Gefahrenpotenzial ausgegangen werden.

dd) Ergebnis

Die Überprüfung ist als Identitätsfeststellung zulässig.

2. Datenerhebung bei öffentlichen Veranstaltungen oder Ansammlungen

Das Auslesen der Daten könnte weiter eine zulässige Datenerhebung im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen darstellen.

§ 26 BGSG Datenerhebung bei öffentlichen Veranstaltungen oder Ansammlungen
(1) Der Bundesgrenzschutz kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen an der Grenze oder den in § 23 Abs. 1 Nr. 4 bezeichneten Objekten personenbezogene Daten auch durch Anfertigung von Bild- und Tonaufzeichnungen von Teilnehmern erheben, wenn Tatsachen die Annahme rechtfertigen,dass bei oder im Zusammenhang mit einer solchen Veranstaltung oder Ansammlung erhebliche Gefahren für die öffentliche Sicherheit an der Grenze oder die Sicherheit der in § 23 Abs. 1 Nr. 2 bezeichneten Objekten entstehen. Die Erhebung kann auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

In dieser Vorschrift werden die Rechte des BGS um ein Recht zur Anfertigung von Bild- und Tonaufnahmen erweitert, wenn die Annahme gerechtfertigt ist, dass erhebliche Gefahren für die öffentliche Sicherheit zu erwarten sind. Dies ist insbesondere auch zulässig, wenn Dritte dabei unvermeidbar betroffen werden.

a) Rechtsgrundlage

Als Rechtsgrundlage kommt § 26 Abs. 1 S. 1 BGSG in Betracht.

b) Formelle Rechtmäßigkeit

Das Auslesen erfolgt hinsichtlich Zuständigkeit, Form und Verfahren des Verwaltungsverfahrens rechtmäßig.[67]

c) Materielle Rechtmäßigkeit

aa) Aufgabenbereich

Der Aufgabenbereich ist eröffnet (Begründung siehe oben)

bb) Gefährdungslage

(a) Ansammlung

Das Auslesen der RFID-Ausweise erfolgt anlässlich einer Ansammlung an einem der in § 23 Abs. 1 Nr. 4 BGSG genannten Objekte (Anlagen der Eisenbahnen des Bundes).

(b) Erhebliche Gefahr

Die Gefahr für die Sicherheit der genannten Objekte (Bahnanlagen, Bahnen, etc...) müsste erheblich sein. Der Begriff „erhebliche Gefahr“ ist legal definiert.

[67] Auf die eingehende Prüfung der formellen Rechtmäßigkeit wird nach Absprache mit den Betreuern verzichtet.

§ 14 BGSG Allgemeine Befugnisse

(...)

(2) Gefahr im Sinne dieses Abschnitts ist eine im Einzelfall bestehende Gefahr für die öffentliche Sicherheit oder Ordnung im Bereich der Aufgaben, die dem Bundesgrenzschutz nach den §§ 1 bis 7 obliegen. Eine erhebliche Gefahr im Sinne dieses Abschnitts ist eine Gefahr für ein bedeutsames Rechtsgut, wie Bestand des Staates, Leben, Gesundheit, Freiheit, wesentliche Vermögenswerte oder andere strafrechtlich geschützte Güter von erheblicher Bedeutung für die Allgemeinheit.

Die Bedrohung durch eine organisierte, bewaffnete Menge Gewalt suchender Hooligans gefährdet Leben und Gesundheit Dritter sowie erhebliche Vermögenswerte (Bahnen und Bahnanlagen). Damit liegt eine erhebliche Gefahr i.S.d. Gesetzes vor.

cc) Bild- oder Tonaufnahmen

Es stellt sich jedoch die Frage, ob es sich beim Auslesen von RFID-Chips um Bild- oder Tonaufnahmen handelt. Insbesondere unter den Begriff „Bildaufnahme“ könnte das Auslesen zu subsumieren sein.

(a) Grammatische Auslegung

Der Wortlaut spricht gegen eine Einbeziehung der RFID-Datenübertragung. Die Übertragung von Daten ist im Allgemeinen keine Bild- und Tonaufzeichnung.

(b) Historische Auslegung

Nach der Begründung des BGSG sollen „Bild- und Tonaufzeichnungen verwendet werden, weil sie sich nach „einsatzpolizeilichen praktischen Erfahrungen“ als „geeignetes Mittel“ herausgestellt haben[68]. Praktische polizeiliche Erfahrungen hinsichtlich RFID liegen naturgemäß nicht vor. Effektivitätserwägungen könnten aber für einen Einsatz von RFID bei Großveranstaltungen sprechen (z.B. sichere, schnelle Identifizierung trotz etwaiger Maskierung). Auf der anderen Seite ist bei der letzten Gesetzesänderung (5.5.2004) keine Regelung zu RFID- auch nicht andeutungsweise- erfolgt. Bedenkt man, dass zu dieser Zeit der Einsatz von RFID-Technik durchaus bekannt war (siehe Flughafenkontrolle Frankfurt am Main), hätte man hier eine Regelung erwarten können. Insgesamt lässt sich bei historischer Betrachtung kein überzeugendes Argument für oder gegen die Einbeziehung von RFID finden.

(c) Systematische Auslegung

Auch eine systematische Betrachtung führt zu keinem konkreten Ergebnis. Lediglich der Umstand, dass im Gesetzteszusamenhang verschiedene detaillierte Maßnahmen zur Erfassung von Personen genannt sind, legt den Schluss nahe, dass auch RFID einzeln geregelt wäre. Beispielsweise finden sich Regeln zu

[68] Deutscher Bundestag, Drucksache 12/7562 vom 17.05.1994 Seite 55ff.

selbsttätigen Bildaufnahme und Bildaufzeichnungsgeräten (§ 27 BGSG), sowie zu besonderen Mitteln der Datenerhebung (§ 28 BGSG)

(d) Teleologische Auslegung

Mit § 26 BGSG können zwei Zielrichtungen verfolgt werden: Zum einen dient die Überwachung präventiv der Vorbeugung von Straftaten. Hierzu sollen per Bildaufnahme (etwa Video) verdächtige Personen und Taten erfasst werden können, um so drohende Gefährdungen erkennen und verhindern zu können. Hierunter könnte auch die Identifizierung mittels RFID und Biometrie zu verstehen sein. Denn durch die Identifizierung bekannter Hooligans kann es gelingen, Gefahrenpotenziale abzuschwächen. Für diese Interpretation spricht zudem, dass in § 26 Abs. 3 BGSG eine Pflicht zur Vernichtung der Aufzeichnungen baldmöglichst nach Erfüllung ihres Zwecks verankert ist.

BGSG § 26 Datenerhebung bei öffentlichen Veranstaltungen oder Ansammlungen
(3) Nach den Absätzen 1 und 2 entstandene Aufzeichnungen sowie daraus gefertigte Unterlagen sind unverzüglich nach Beendigung der Veranstaltung oder Ansammlung zu vernichten, soweit sie nicht benötigt werden
1. zur Verfolgung einer Ordnungswidrigkeit von erheblicher Bedeutung oder einer Straftat oder
2. zur Verhütung von Straftaten bei oder im Zusammenhang mit Versammlungen,öffentlichen Veranstaltungen oder Ansammlungen, weil die betroffene Person verdächtig ist, solche Straftaten vorbereitet oder begangen zu haben und deshalb Grund zu der Annahme besteht, dass sie auch künftig solche Straftaten begehen wird.
Die Vernichtung kann ferner unterbleiben, wenn eine Störung der öffentlichen Sicherheit bei oder im Zusammenhang mit der Veranstaltung oder Ansammlung eingetreten ist und die Aufzeichnungen ausschließlich zum Zwecke der polizeilichen Aus- und Fortbildung oder zur befristeten Dokumentation des polizeilichen Handelns verwendet werden. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu anonymisieren. Sofern eine Anonymisierung nicht möglich ist, sind Aufzeichnungen, die ausschließlich zum Zweck der Dokumentation verwendet werden, nach spätestens zwei Monaten zu vernichten.

Da die im Szenario vorgestellten autarken Lesegeräte mangels Schnittstelle keine Möglichkeit zur Übertragung und zur zentralen Speicherung bieten, wird weniger invasiv mit den Rechten Dritter umgegangen, als bei einer Videoaufzeichnung. Dies folgt dem Grundsatz der Verhältnismäßigkeit, die in § 15 BGSG normiert ist.

BGSG § 15 Grundsatz der Verhältnismäßigkeit
(1) Von mehreren möglichen und geeigneten Maßnahmen ist diejenige zu treffen, die den einzelnen und die Allgemeinheit voraussichtlich am wenigsten beeinträchtigt.
(2) Eine Maßnahme darf nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht.
(3) Eine Maßnahme ist nur solange zulässig, bis ihr Zweck erreicht ist oder sich zeigt, dass er nicht erreicht werden kann.

Die „Vernichtung“ der erhobenen Daten Dritter (z.B. biometrische Daten eines Passagiers, der kein Hooligan ist) erfolgt im Szenario unmittelbar nach der Nutzung. Entweder der BGS Beamte identifiziert einen Hooligan und ergreift weitere Maßnahmen oder das Lesegerät wird auf den nächsten Passagier angewendet, wobei die Daten der vorigen Erhebung gelöscht werden. Speicherung, Nutzung und Löschung im Sinne von § 3 Abs. 4 BDSG der Daten sind quasi untrennbar miteinander verbunden. Effektiv wird nur die Identität festgestellt. Dabei ist jedoch zu beachten, dass eine „traditionelle“

Bildaufzeichnung i.d.R. noch keine sichere Identifizierung ermöglicht. Als Vorfeldmaßnahme dient sie erst dazu, erforderliche Maßnahmen vorzubereiten. Zu diesen kann dann die Identifizierung einer verdächtigen Person gehören. Insoweit liegt bei der identifizierende RFID-Kontrolle ein stärkerer Eingriff vor.
In § 26 BGSG ist keine Hinweispflicht auf die Aufnahme zu finden. Dies spricht für eine Anwendbarkeit von § 26 BGSG auf das untersuchte Szenario, da dieser Aspekt bei der Identitätsfeststellung durch Videoaufzeichnungen und der Identitätsfeststellung durch das RFID-Ausweislesegerät gleich ist: Der betroffene Dritte bemerkt die Maßnahme nicht. Dies ist bei der Bildaufzeichnung auch zulässig, § 26 Abs. 1 S. 2 BGSG.
Demgegenüber könnte stehen, dass § 26 BGSG auch repressive Zwecke verfolgt. Es soll ermöglicht werden, Störer greifbar zu machen, nachdem sich Schädigungen ereignet haben. Dazu sollen die Bildaufnahmen bei Großereignissen auch dienen. Allerdings kann aus § 26 Abs. 3 BGSG der Schluss gezogen werden, dass die Überwachung zu einem überwiegenden Teil präventiven Zwecken dient.
Ansonsten wäre die Normierung von Aufbewahrungspflichten speziell für repressive Zwecke in § 26 Abs. 3 BGSG (etwa Strafverfolgung) nicht erforderlich. Vielmehr soll präventiv versucht werden, drohende Gefahren frühzeitig zu erkennen und ihnen zu begegnen. Somit führt eine teleologische Auslegung ebenfalls nicht zu klaren Ergebnissen.

(e) Zwischenergebnis

Im Hinblick auf den klaren Wortlaut und das Gebot der Normenklarheit erscheint es angemessen, das Auslesen von RFID-Ausweisen nicht als Bildaufnahme einzuordnen. Demnach kann § 26 BGSG keine wirksame Rechtsgrundlage bilden.

d) Ergebnis

Das Auslesen kann nicht auf § 26 BGSG gestützt werden.

3. Datenspeicherung

Beim Auslesen könnte zudem eine Datenspeicherung erfolgen.

a) Rechtsgrundlage

Hier kommt § 29 BGSG als Rechtsgrundlage in Frage.

b) Formelle Rechtmäßigkeit

Das Auslesen erfolgt hinsichtlich Zuständigkeit, Form und Verfahren des Verwaltungsverfahrens rechtmäßig.[69]

c) Materielle Rechtmäßigkeit

§ 29 BGSG Speicherung, Veränderung und Nutzung personenbezogener Daten
(1) Der Bundesgrenzschutz kann personenbezogene Daten speichern, verändern und nutzen, soweit dies zur Erfüllung seiner jeweiligen Aufgabe erforderlich ist. Er kann ferner personenbezogene Daten speichern, verändern und nutzen, soweit dies zur Erledigung besonderer Ersuchen nach § 17 Abs. 2 des Bundesverfassungsschutzgesetzes erforderlich ist. Die Speicherung, Veränderung und Nutzung darf nur für den Zweck erfolgen, für den die Daten erlangt worden sind. Die Speicherung, Veränderung und Nutzung für einen anderen Zweck ist zulässig, soweit der Bundesgrenzschutz die Daten für diesen Zweck nach diesem Gesetz oder einer anderen Rechtsvorschrift erheben dürfte. Sind personenbezogene Daten mit den besonderen Mitteln des § 28 Abs. 2 erhoben worden, ist ihre Verwendung für einen anderen Zweck nur zulässig, soweit dies zur Abwehr einer erheblichen Gefahr erforderlich ist; die Vorschriften der Strafprozeßordnung bleiben unberührt.

aa) Aufgabenzuweisung

Der BGS wird innerhalb seines Aufgabenbereichs tätig (s.o.).

bb) Datenverarbeitung

Der BGS müsste ferner ein personenbezogene Daten speichern, verarbeiten oder nutzen, also „organisieren“. Zur Definition kann hier ergänzend dass BDSG herangezogen werden. Ob eine Spezialität des BGSG gegenüber dem BDSG anzunehmen ist, ist eine Frage des Einzelfalls, die sich erst bei der jeweiligen Norm stellt. Grundsätzlich findet das BDSG Anwendung, soweit nicht eine spezielle Regelung im BGSG vorhanden ist bzw. die Anwendbarkeit des BDSG explizit ausgeschlossen ist.

§ 37 Geltung des Bundesdatenschutzgesetzes
Bei der Erfüllung der dem Bundesgrenzschutz nach den §§ 1 bis 7 obliegenden Aufgaben finden § 3 Abs. 2 und 8 Satz 1, § 4 Abs. 2 und 3, §§ 4b, 4c, 10 Abs. 1, §§ 13, 14 Abs. 1, 2 und 5, §§ 15, 16, 18 Abs. 2 Satz 2 und 3 sowie §§ 19a und 20 des Bundesdatenschutzgesetzes keine Anwendung

(a) Personenbezogene Daten

Bei der Auslesung der Ausweisdaten handelt es sich um personenbezogene Daten nach § 3 Abs. 1 BDSG.

§ 3 Abs. 1 BDSG
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Name, Geburtsdatum, etc. sind unproblematische Einzelangaben über persönliche Verhältnisse einer bestimmten Person.

(b) Datenspeicherung

[69] Auf die eingehende Prüfung der formellen Rechtmäßigkeit wird nach Absprache mit den Betreuern verzichtet.

Im beschriebenen Szenario kommt allenfalls die Alternative Datensspeicherung in Betracht.

§ 3 Abs. 4 BDSG
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgehen gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

Beim Auslesen der Daten handelt es sich um ein Aufnehmen personenbezogener Daten auf einen Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Dieses „ Aufnehmen“ ist als Speichern und damit als Verarbeitung zu qualifizieren.

cc) Zweckbindung

Die Daten dürfen jedoch nur für Zwecke gespeichert, für die sie erhoben wurden bzw. für die eine die Erhebung erlaubende Rechtsgrundlage besteht, § 29 Abs. 1 S. 3, 4. Fehlt es an einer Rechtsgrundlage für die Erhebung oder Erlangung, kann keine rechtmäßige Speicherung erfolgen.

(a) Identitätsfeststellung und Erhebung

Die Daten sind gemäß § 23 BGSG zur Identitätsfeststellung erfasst worden. Damit liegt eine Rechtsgrundlage für die Speicherung zu diesem Zweck vor. Es stellt sich die Frage, ob auch eine zulässige Datenerhebung gemäß § 21 BGSG vorliegt, die eine Speicherung zu einem bestimmten Zweck zuließe. § 21 BGSG bildet eine Generalklausel für die Datenerfassung.

(b) Rechtsgrundlage der Erhebung

Als Rechtsgrundlage kommt § 21 BGSG in Betracht.

(c) Formelle Rechtmäßigkeit der Erhebung

Das Auslesen erfolgt hinsichtlich Zuständigkeit, Form und Verfahren des Verwaltungsverfahrens rechtmäßig.[70]

(d) Materielle Rechtmäßigkeit der Erhebung

- **Erhebung personenbezogener Daten**

Zur Datenerhebung findet sich eine Begriffsbestimmung in § 3 Abs. 3 BDSG.

[70] Auf die eingehende Prüfung der formellen Rechtmäßigkeit wird nach Absprache mit den Betreuern verzichtet.

§ 3 Abs. 3 BDSG
(3) Erheben ist das Beschaffen von Daten über den Betroffenen.

Durch die Erfassung der Ausweisdaten beschafft sich der BGS personenbezogene Daten über die Betroffenen. Darin ist eine Datenerhebung i.S.d. § 3 Abs. 3 BDSG zu sehen.

- **Anlass der Datenerhebung**

BGSG § 21 Erhebung personenbezogener Daten
(1) Der Bundesgrenzschutz kann, sofern in diesem Abschnitt nichts anderes bestimmt ist, personenbezogene Daten erheben, soweit dies zur Erfüllung einer ihm obliegenden Aufgabe erforderlich ist.
(2) Zur Verhütung von Straftaten ist eine Erhebung personenbezogener Daten nur zulässig, soweit Tatsachen die Annahme rechtfertigen, dass
1. die Person Straftaten im Sinne des § 12 Abs. 1 mit erheblicher Bedeutung begehen will und die Daten zur Verhütung solcher Straftaten erforderlich
sind oder
2. die Person mit einer in Nummer 1 genannten Person in einer Weise in Verbindung steht oder eine solche Verbindung hergestellt wird, die erwarten läßt, dass die Maßnahme zur Verhütung von Straftaten im Sinne der Nummer 1 führen wird und dies auf andere Weise aussichtslos oder wesentlich erschwert wäre.
(3) Personenbezogene Daten sind offen und beim Betroffenen zu erheben. Sie können bei anderen öffentlichen oder bei nicht-öffentlichen Stellen erhoben werden, wenn die Erhebung beim Betroffenen nicht möglich ist oder durch sie die Erfüllung der dem Bundesgrenzschutz obliegenden Aufgaben gefährdet oder erheblich erschwert würde. Eine Datenerhebung, die nicht als Maßnahme des Bundesgrenzschutzes erkennbar sein soll, ist nur zulässig, wenn auf andere Weise die Erfüllung der dem Bundesgrenzschutz obliegenden Aufgaben erheblich gefährdet wird oder wenn anzunehmen ist, dass dies dem überwiegenden Interesse der betroffenen Person entspricht.
(4) Werden personenbezogene Daten beim Betroffenen oder bei nicht-öffentlichen Stellen erhoben, sind diese auf Verlangen auf den Umfang ihrer Auskunftspflicht und auf die Rechtsgrundlage der Datenerhebung hinzuweisen. Der Hinweis kann unterbleiben, wenn durch ihn die Erfüllung der Aufgaben des Bundesgrenzschutzes gefährdet oder erheblich erschwert würde. Sofern eine Auskunftspflicht nicht besteht, ist auf die Freiwilligkeit der Auskunft hinzuweisen.

Die Datenerhebung erfolgt, um drohende Straftaten i.S.d. § 12 Abs. 1 Nr. 5 BGSG zu verhindern.

§ 12 Abs. 1 BGSG Verfolgung von Straftaten
(1) Der Bundesgrenzschutz nimmt die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung (§§ 161, 163 der Strafprozeßordnung) wahr, soweit der Verdacht eines Vergehens (§ 12 Abs. 2 des Strafgesetzbuches) besteht, das
1. gegen die Sicherheit der Grenze oder die Durchführung seiner Aufgaben nach
§ 2 gerichtet ist,
2. nach den Vorschriften des Paßgesetzes, des Ausländergesetzes oder des Asylverfahrensgesetzes zu verfolgen ist, soweit es durch den Grenzübertritt oder in unmittelbarem Zusammenhang mit diesem begangen
wurde,
3. einen Grenzübertritt mittels Täuschung, Drohung, Gewalt oder auf sons trechtswidrige Weise ermöglichen soll, soweit es bei der Kontrolle des grenzüberschreitenden Verkehrs festgestellt wird,
4. das Verbringen einer Sache über die Grenze ohne behördliche Erlaubnis als gesetzliches Tatbestandsmerkmal der Strafvorschrift verwirklicht, sofern dem Bundesgrenzschutz durch oder auf Grund eines Gesetzes die Aufgabe der
Überwachung des Verbringungsverbotes zugewiesen ist,
5. auf dem Gebiet der Bahnanlagen der Eisenbahnen des Bundes begangen wurde und gegen die Sicherheit eines Benutzers, der Anlagen oder des Betriebes der Bahn gerichtet ist oder das Vermögen der Bahn oder ihr anvertrautes
Vermögen betrifft,
6. dem deutschen Strafrecht unterliegt und Strafverfolgungsmaßnahmen auf See außerhalb des deutschen Küstenmeers im Rahmen des § 6 erforderlich macht, darüber hinaus, soweit der Verdacht eines Verbrechens nach Nummer 2 oder nach § 315
Abs. 3 Nr. 1 des Strafgesetzbuches besteht sowie in Fällen der Nummer 6. Das Bundesministerium des Innern bestimmt das Nähere über die unter Satz 1 fallenden Straftaten durch Rechtsverordnung im Einvernehmen mit dem Bundesministerium der Justiz und mit Zustimmung des Bundesrates. Soweit Satz 1 Nr. 4 betroffen ist,
(...)

- **Durchführung**

Die Durchführung muss offen und beim Betroffenen erfolgen. Das ist der Fall, wenn die Betroffenen auf die Erfassung hingewiesen werden. Eine Datenerhebung, die nicht als Maßnahme des BGS zu erkennen ist, ist nur zulässig, wenn ansonsten die Erfüllung der Aufgaben des BGS erheblich erschwert würde oder dies dem überwiegendem Interesse der betroffenen Person entspricht. Es nicht ersichtlich, dass eine offenen Vorgehensweise die Arbeit des BGS übermäßig erschweren könnte. Denn der BGS kann die Situation auf den Bahnanlagen kontrollieren. Einer Verweigerung der Kontrolle könnte nachgegangen werden. Die Lage ist insgesamt mit der „klassischen „ Kontrolle von Ausweispapieren zu vergleichen. Weiter sprechen auch nicht überwiegende Interessen der Betroffenen gegen eine offenen Vorgehensweise. Mithin ist die heimliche Kontrolle unzulässig gemäß § 21 BGSG.

(e) Ergebnis

§ 21 BGS bildet keine ausreichende Grundlage für das Auslesen der Daten. Damit kann der Erhebungszweck keine Rechtsgrundlage für die Datenspeicherung bilden.

(f) Datenhebung bei Versammlungen und Ansammlungen

Auf § 26 BGSG kann die Speicherung ebenfalls nicht gestützt werden, da diese Norm nicht einschlägig ist.

dd) Ermessen

Die BGS-Beamten müssten ihr Ermessen („kann“) fehlerfrei ausgeübt haben. Dabei müssten sie auch den Verhältnismäßigkeitsgrundsatz gewahrt haben. Insbesondere muss die Maßnahme sich im Rahmen des für die Aufgabenerfüllung erforderlichen halten, d.h. nur zu dem zulässigen Zweck erfolgen (§ 29 Abs. 1 BGSG). Die Speicherung erfolgt nur kurzfristig und zweckgebunden zur Identitätsfeststellung und ist daher verhältnismäßig.

d) Ergebnis

Die Speicherung der Daten zur Identitätsfeststellung erfolgt somit rechtmäßig.

4. Gesamtergebnis „Auslesen“

Das Auslesen des RFID-Ausweises ist mithin rechtmäßig erfolgt. Grundlage sind § 23 BGSG (Identitätsfeststellung) und § 29 BGSG (Datenspeicherung).

E Rechtliche Bewertung (Szenario 2 und 3)

I. Beschreibung der Szenarien

1. „RFID-Kundenkarte“ (Szenario 2)

In diesem Szenario wird Kunden eines Großmarktes eine Kundenkarte mit RFID-Transponder ausgehändigt. Diese dient dem Zweck, den Jugendschutz in der Multimedia-Abteilung sicherzustellen. Dort gibt es die Möglichkeit in Filme „hereinzuschnuppern“: Dazu hält der Kunde seine Kundenkarte am „Multimedia Terminal“ vor das entsprechende Medium und kann sich auf einem Sichtfenster ausgewählte Sequenzen des Werkes vor dem Kauf ansehen, sofern er das nötige Mindestalter aufweist. Erst danach trifft der Kunde eine Kaufentscheidung. Die Kundenkarte wird nur Personen mit einem Mindestalter von 16 Jahren ausgehändigt. Der Transponder auf der Kundenkarte enthält nur die Kundennummer. Das Auslesen dieser erfolgt kontaktlos, nachdem der Kunde seine Kundenkarte am Multimedia Terminal vor das entsprechende Medium gehalten hat. Der Kunde hat keine Möglichkeit zu prüfen, welche Daten tatsächlich auf der Karte gespeichert sind bzw. welche Daten von dem Multimedia Terminal ausgelesen werden.
Der Kunde wird bei Aushändigung der Karte nicht darauf hingewiesen, dass diese einen Transponder enthält. Auch an der Karte selbst lässt sich dies nicht ohne Hilfsmittel erkennen.

2. Ein tatsächlicher Sachverhalt

Dieses Szenario entspricht -soweit dies in Erfahrung gebracht werden konnte- dem tatsächlichen Einsatz im Metro Future Store. Es ist anzumerken, dass es dem Foebud e.V. nach eigenen Aussagen möglich war, die Kundennummer (und zwar nur diese) mittels eines handelsüblichen RFID-Readers[71] aus der Kundenkarte auszulesen.
Wie oben erwähnt ist unter anderem auf Druck des Verbraucherschutzverbands Foebud e.V. der Einsatz RFID-Kundenkarte bei der Metro beendet worden. Laut Stellungnahme der Metro habe man diesen Schritt nicht aufgrund von rechtlichen Problemen getätigt[72]. Ob diese Meinung so nachvollziehbar ist, soll im Folgenden untersucht werden.

---

[71] Megaset Elektronik AG & Co. Website. Internet: http://www.megaset.com/RFID_1356MHz_ISO-Reader-Box.pdf. Stand 18.9.2004

[72] Metro Website. Internet: http://www.future-store.org/servlet/PB/menu/1002376_l1/1083794427060.html, Stand 5.5.2004

Die Kundenkarte der Metro - deutlich ist das Payback Logo zu sehen[73], der RFID Transponder ist nicht zu erkennen.

3. Eine fiktive Ergänzung zu Szenario 2 (Szenario 3)

Als Ergänzung zum Szenario 2 soll untersucht werden, wie der Einsatz der RFID-Kundenkarte an der Kasse des Metro Marktes zu bewerten ist (Szenario 3). Der Kunde steht vor der Kasse des Marktes. Das Kassensystem liest aus seiner Kundenkarte die Kundennummer aus und bucht den Warenkorb des Kunden auf sein Kundenkonto. Angemerkt sei an dieser Stelle, dass dieses Szenario vorläufig fiktiv ist.

Zuerst soll jedoch der reale Sachverhalt aus Szenario 2 bearbeitet werden.

II. Szenario 2: Aufgliederung des Szenarios in Teilaspekte

Aus rechtlicher Sicht ist das Szenario in zwei Themengebiete zu untergliedern:

1. Datenschutz

Hier soll die Frage geprüft werden, ob

- die Ausstellung der Kundenkarte mit RFID an sich rechtmäßig ist und
- das Auslesen der Kundennummer zulässig ist und

[73] Foebud e.V. Website. Internet: http://www.foebud.de/. Stand17.9.2004.

- ob dem Kunden K durch Metro eine Prüfung der Daten auf dem Transponder ermöglicht werden muss.

2. Datensicherheit

Hierunter soll die Problematik fallen, die erhobenen Daten vor dem Zugriff durch Dritte zu schützen. Die Grundfrage von B ist, ob die ausgebende Stelle nicht dazu verpflichtet ist, für Datensicherheit in Form von einem Schutz vor einem (unzulässigen) Auslesen durch Dritte sicherzustellen.

III. Ausstellung der Kundenkarte

Unter „Ausstellung“ der Kundenkarte soll das Anbringen der Kundennummer an einer Karte im ID1 Format in gedruckter Form und ebenso ein Anbringen in digitaler Form auf dem in die Karte eingelassenen Transponder verstanden werden. Wie oben dargelegt, ist der Einsatz von RFID unter Einhaltung von Standards[74] in der EU ohne Genehmigungsverfahren rechtmäßig.
Die Ausstellung lässt sich wie folgt untergliedern:

- Die Ausstellung der Kundenkarte im „klassischen“ Sinne. Die Kundenkarte in Szenario enthält auch unabhängig von der RFID-Thematik die üblichen Merkmale einer Kundenkarte (Name, Adresse, Geburtsdatum …).
- Weiterhin wird aus den erhobenen Daten die Kundennummer im RFID-Transponder gespeichert (als einziges Datum – also etwa 1234567879XYZ)

1. Voraussetzungen

In Frage kommen § 4 BDSG (ggf. i.V.m. § 4a BDSG), § 6c BDSG und § 28 BDSG in Betracht.

2. Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (§ 4 BDSG)

a) Örtlicher Anwendungsbereich

Der örtliche Anwendungsbereich ist in § 1 Abs. 2 Nr. 3 BDSG normiert, da es sich bei Metro evident um eine nicht-öffentliche Stelle handelt.

[74] Die Metro setze Transponder ein, die dem ISO-15693 Standard entsprechen.

BDSG § 1 Zweck und Anwendungsbereich des Gesetzes
(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.
(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch
1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
a) Bundesrecht ausführen oder
b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Der örtliche Anwendungsbereich bei nicht-öffentlichen Stellen wird in § 1 Abs. 2 Satz 3 nicht eingeschränkt, also erstreckt sich der Geltungsbereich auf die gesamte Bundesrepublik Deutschland. Das es sich um einen Inlandssachverhalt handelt ist der örtliche Anwendungsbereich eröffnet.

b) Sachlicher Anwendungsbereich

BDSG § 1 Abs. 2 Nr. 3
(...)
nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder dafür erheben oder die Daten in oder aus nicht automatisierten Dateien verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausschließlich für persönliche oder familiäre Tätigkeiten.

Bei der Ausstellung der Kundenkarte erfolgt eine Erhebung der Metro-Kundennummer des Betroffenen. Es ist festzustellen, dass

1. der Einsatz der der RFID-Kundenkarte bei einer nicht-öffentlichen Stelle und
2. bei der Feststellung der Kundennummer zwangsläufig eine Datenerhebung im Sinne von § 3 Abs. 3 BDSG erfolgt. Der Geltungsbereich des BDSG ist damit grundsätzlich eröffnet.

Es ist zu prüfen, ob die Voraussetzungen die eine Anwendbarkeit des § 4 BDSG erfüllt sind:

BDSG § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
(1) Die Erhebung, Verarbeitung und Nutzung ***personenbezogener*** *Daten sind nur zulässig, soweit dieses Gesetz oder eine* ***andere Rechtsvorschrift*** *dies erlaubt oder anordnet* ***oder*** *der* ***Betroffene eingewilligt*** *hat.*
(...)

Es sei an dieser Stelle nochmals darauf hingewiesen, dass hier lediglich der Einsatz RFID-Transponders untersucht werden soll. Das erhobene Datum, das auf dem RFID-Transponder gespeichert wird, ist die Kundennummer des Betroffenen. Es ist zu prüfen, ob dieses Datum im Szenario personenbezogen ist. In § 3 Abs. 1 BDSG werden personenbezogene Daten als „Einzelangaben über persönliche oder sachliche Verhältnisse“ legal definiert.

BDSG § 3 Weitere Begriffsbestimmungen
(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Zwar wird eine Kundennummer in der Literatur als personenbezogenes Datum explizit erwähnt[75], jedoch ist diese Betrachtungsweise im Szenario aus zweierlei Gründen abzulehnen:

1. Eine Kundennummer für sich allein gestellt - also nicht im Zusammenhang mit einem Datensatz, der einen direkten Personenbezug zulässt - ist nicht als personenbezogenes Datum anzusehen.
2. Im Kommentar zum BDSG[76] wird der Personenbezug der Kundennummer aus ihrer Sigmatik (Hinweiswirkung) hergeleitet, jedoch ist diese nur dann gegeben, wenn ein Dritter den „Hinweis“ ohne Zusatzwissen versteht. Als Beispiel für eine solche Zusatzinformation sei hier die Sozialversicherungsnummer genannt, aus welcher sich das Alter des Betroffenen leicht ermitteln lässt. Im vorliegenden Fall besteht die Kundennummer lediglich aus einer Anreihung von Zahlen, aus welcher sich keinerlei personenbezogene Informationen ermitteln lassen. Auch sieht man der Nummer nicht an, dass es sich zwangsläufig um eine Nummer der Metro handelt. Eine Sigmatik der Kundennummer kann hier nicht festgestellt werden: Eine Kundennummer ist eine Verkettung alphanumerischer Zeichen, etwa „123456789XYZ“ (und nicht etwa „M-E-T-R-O-123456789XYZ“, denn diese Kundennummer hätte eine sigmatische Wirkung).

Der sachliche Anwendungsbereich ist demnach nicht eröffnet, da es sich bei der Speicherung der Kundennummer im RFID-Transponder der Karte nicht um ein personenbezogenes Datum handelt.
Da die Paragraphen der alternativen Voraussetzungen alle im BDSG zu finden sind, brauchen sie an dieser Stelle nicht mehr geprüft zu werden, da der Anwendungsbereich des BDSG folglich auch bei diesen nicht eröffnet werden kann.

3. Zusammenfassung: Ausstellung der Kundenkarte

Zusammenfassend ist zu sagen, dass die „einschlägigen“ §§ des BDSG mangels Personenbezug des Datums „Kundennummer“ keine Anwendung finden. Es spricht also rechtlich nichts gegen Die Ausstellung der RFID-Kundenkarte; die Ausstellung demnach ist zulässig.

[75] Vgl. Simits u.a., BDSG/Dammann § 3 Rdnr. 10
[76] Vgl. Simits u.a., BDSG/Dammann § 3 Rdnr. 10

IV. Auslesen der Kundennummer am Multimedia Terminal

Wie oben gezeigt, ist die Ausstellung der RFID-Kundenkarte zulässig.
Laut Aussage der Metro ist bisher keine anderweitige Nutzung als die der Alterskontrolle mittels RFID-Transponders erfolgt. Eine eventuelle Nutzung des „klassischen“ (also des nicht-RFID) Teils der Karte soll hier nicht berücksichtigt zu werden. Es geht hier ausschließlich um eine Nutzung des RFID-Transponders.
Die Nutzung der Daten setzt sich im Szenario aus zwei Stufen zusammen:

1. Ein Auslesen der Daten mittels RFID-Technik
   Der Kunde hält die Kundenkarte vor das Medium, von welchem er die Vorschau sehen möchte.
2. Eine nachgelagerte Verarbeitung der Daten
   Wenn eine Kundenkartennummer erkannt wird, wird die Vorschaufunktion aktiviert.

1. Voraussetzungen

In Frage kommen § 4 BDSG (ggf. i.V.m. § 4a BDSG), § 6c BDSG und § 28 BDSG. Betrachtet man jedoch die Anwendungsbereiche dieser §§, so wird die Prüfung der Anwendungsbereiche die gleichen Ergebnisse liefern wie zuvor liefern: Die RFID-Kundenkarte des Betroffenen enthält nach der hier vertretenen Ansicht kein personenbezogenes Datum. Laut Aussage der Metro wurde an den Multimedia Terminals mittels des RFID nur festgestellt, ob eine Kundenkarte vorhandenen ist. Unklar ist, wie und ob die „Echtheit“ der Nummer verifiziert wurde. Ein Abgleich mit einer Liste von „echten“ Nummern oder durch eine Prüfsumme ist datenschutzrechtlich als unproblematisch anzusehen.
Festzuhalten ist: Solange das Datum nicht mit der Kundendatenbank der Metro verknüpft wurde, ist es nicht personenbezogen.

Die Prüfung der alternativ in Frage kommenden §§ kann hier entfallen, da deren Anwendungsbereich der entsprechenden Gesetze nicht eröffnet werden kann:

- 4 BDSG
- § 6c BDSG
- § 28 BDSG

2. Zusammenfassung: Auslesen der Kundennummer am Multimedia Terminal

Zusammenfassend ist zu sagen, auch hier mangels Personenbezug des Datums „Kundennummer“ die in Frage kommenden §§ nicht angewendet werden können. Das Auslesen der Kundennummer am Multimedia Terminal ist also zulässig.

V. Datensicherheit

Datenschutz geht einher mit Datensicherheit. Es ist eine logische Kette zu bilden:

- Datensicherheit ist Voraussetzung für Datenschutz,
- Datenschutz ist Voraussetzung für den Schutz personenbezogener Daten,
- dieser ist wiederum Voraussetzung für Privatheit

Da das „strittige Datum“im Szenario nicht personenbezogen ist, kann folglich auch keine Pflicht für Datensicherheit des RFID-Transponders auf der Kundenkarte abgeleitet werden.

VI. Zusammenfassung (Szenario 2)

Wie gezeigt wurde, ist sowohl die Ausstellung der Kundenkarte als auch das Auslesen der Kundennummer am Multimedia Terminal zulässig.
Der „Metro Skandal“, wie der Foebud e.V. das Szenario beschreibt, kann aus rein juristischer Sicht so nicht bezeichnet werden.

VII. Szenario 3: Eine fiktive Ergänzung

Als Ergänzung zum Szenario 2 soll untersucht werden, wie der Einsatz der RFID-Kundenkarte an der Kasse des Metro Marktes zu bewerten ist (Szenario 3). Der Kunde steht vor der Kasse des Marktes. Das Kassensystem liest aus seiner Kundenkarte die Kundennummer aus und bucht den Warenkorb des Kunden auf sein Kundenkonto. Angemerkt sei an dieser Stelle nochmals, dass dieses Szenario vorläufig fiktiv ist.

VIII. Ausstellung der Kundenkarte und Zahlvorgang

1. Voraussetzungen

In Frage kommen § 4 BDSG (ggf. i.V.m. § 4a BDSG), § 6c BDSG und § 28 BDSG in Betracht.

2. Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke (§28 BDSG)

Ein Erlaubnistatbestand könnte aus § 28 BDSG hervorgehen.

BDSG § 28 Datenerhebung, -verarbeitung und -nutzung für eigene Zwecke
(1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung ***als Mittel für die Erfüllung eigener Geschäftszwecke*** *ist zulässig*
1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder ***vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen*** *dient,*
2. soweit es zur ***Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist*** *und kein Grund zu der Annahme besteht, dass das* ***schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt****, oder*
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.
Bei der Erhebung personenbezogener Daten sind die Zwecke, für die die Daten verarbeitet oder genutzt werden sollen, konkret festzulegen.
(2) Für einen anderen Zweck dürfen sie nur unter den Voraussetzungen des Absatzes 1 Satz 1 Nr. 2 und 3 übermittelt oder genutzt werden.
(3) Die Übermittlung oder Nutzung für einen anderen Zweck ist auch zulässig:
1. soweit es zur Wahrung berechtigter Interessen eines Dritten oder
2. zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist, oder
3. für Zwecke der Werbung, der Markt- und Meinungsforschung, wenn es sich um listenmäßig oder sonst zusammengefasste Daten über Angehörige einer Personengruppe handelt, die sich auf
a) eine Angabe über die Zugehörigkeit des Betroffenen zu dieser Personengruppe,
b) Berufs-, Branchen- oder Geschäftsbezeichnung,
c) Namen,
d) Titel,
e) akademische Grade,
f) Anschrift und
g) Geburtsjahr beschränken
und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat, oder
(...)

a) Örtlicher Anwendungsbereich

Der örtliche Anwendungsbereich ist in § 1 Abs. 2 BDSG normiert. Der örtliche Anwendungsbereich ist eröffnet (Begründung siehe oben).

b) Sachlicher Anwendungsbereich

Der Anwendungsbereich von § 28 BDSG Abs. 1 ist zu prüfen. Voraussetzung für die Eröffnung des Anwendungsbreiches ist die Datenerhebung ist Nutzung der Daten zur Erfüllung eigener Geschäftszwecke.
Die Ausstellung der RFID-Kundenkarte dient dem Geschäftszweck der Metro, den Zahlungsvorgang zu beschleunigen und damit den Kauf für beide Seiten bequemer zu gestalten. Eine effizientere Abwicklung ist als Geschäftszweck zu verstehen, insbesondere, wenn man die damit verbundenen Einsparungsmaßnahmen in Betracht zieht: Die daraus resultierende Gewinnsteigerung ist demzufolge als Geschäftszweck einzustufen.

Weiterhin müssen die Bedingungen von § 28 Abs. 1 Nr. 1-3 erfüllt sein.

aa) § 28 Abs. 1 Nr. 1 BDSG

Die RFID Kundenkarte soll hier zur Zahlung eingesetzt werden. Die Zahlung ist ein Bestandteil des Kaufvertrags, den der Kunde mit der Metro beim Kauf der

Produkte an der Kasse eingeht. Der Zweck der Datenerhebung ist also die Abwicklung der Zahlung. Insofern kann argumentiert werden, dass der sachliche Anwendungsbereich eröffnet ist. Andererseits ist eine Speicherung des Warenkorbs in Zusammenhang mit dem Kundenkonto nicht nötig, wenn der Kunde Barzahlung wünscht. Hierzu wäre lediglich die Ermittlung eines Gesamtpreises notwendig (Dazu könnten zukünftig die EPC Transponder der Produkte eingesetzt werden). Werder der Warenkorb noch der Gesamtpreis sollten im Falle einer Barzahlung mit der Kundennummer des Kunden verknüpfbar sein. Eine Zweckbestimmung wäre in diesem Fall also nicht gegeben. Schon die Existenz dies einen Falles reicht aus, um den Anwendungsbereich des § im Allgemeinen abzulehnen.

bb) § 28 Abs. 1 Nr. 2 BDSG

Die zulässige Nutzung der Daten ist nur dann gegeben, wenn diese zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist. Die Abwicklung eines Zahlvorgangs ist als ein solches zu verstehen.
Demgegenüber steht ggf. ein schutzwürdiges Interesse des Betroffenen. In grammatischer Auslegung darf kein Grund zu der Annahme bestehen, dass ein schutzwürdiges Interesse des Betroffenen am Ausschluss der Verarbeitung bzw. Nutzung überwiegt. Die Annahme, dass der Kunde möglicherweise Barzahlung wünscht, ist demnach hinreichend um eine Anwendung dieses § abzulehnen. Auch der aufkommende Widerstand gegen den Einsatz von RFID Technik in der Bevölkerung und der damit verbundenen Medienrummel um den Einsatz der Kundenkarte lässt zweifelsfrei erkennen, dass ein Interesse des Betroffenen an einem Schutz vor Erhebung der Daten vorliegt. Eine Schutzwürdigkeit könnte aus dem allgemeinen Persönlichkeitsrecht abgeleitet werden, denn ein Warenkorb kann starke Rückschlüsse auf die Lebensumstände eines einer Person zulassen.

cc) § 28 Abs. 1 Nr. 3 BDSG

Auch sind die erhobenen Daten weder allgemein zugänglich, noch dürften sie veröffentlicht werden. Es wird als vertragliche Nebenpflicht angesehen werden, dass beim Kauf von Waren im angemessenen Masse Diskretion gewahrt wird. Schon die Information über den Kauf eines einzelnen bestimmten Produktes kann in den „falschen Händen“ unangenehme Folgen für den Käufer haben. (Beispielsweise Geburtstagsgeschenke, Zigaretten, etc.)

c) Ergebnis der Prüfung von § 28 BDSG.

Im Szenario kann die Zulässigkeit der Ausstellung einer RFID-Kundenkarte nicht auf § 28 BDSG gestützt werden.

Es bleibt, als Alternative, Zulässigkeit nach § 4 BDSG zu prüfen.

3. Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung (§ 4 BDSG)

a) Örtlicher Anwendungsbereich

Der örtliche Anwendungsbereich ist in § 1 Abs. 2 BDSG normiert. Der örtliche Anwendungsbereich ist eröffnet (Begründung siehe oben).

b) Sachlicher Anwendungsbereich

BDSG § 4 Zulässigkeit der Datenerhebung, -verarbeitung und -nutzung
*(1) Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine **andere Rechtsvorschrift** dies erlaubt oder anordnet **oder** der **Betroffene eingewilligt** hat.*
*(2) Personenbezogene Daten sind **beim Betroffenen** zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn*
1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt oder
2. a) die zu erfüllende Verwaltungsaufgabe ihrer Art nach oder der Geschäftszweck eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder
b) die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.
(3) Werden personenbezogene Daten beim Betroffenen erhoben, so ist er, sofern er nicht bereits auf andere Weise Kenntnis erlangt hat, von der verantwortlichen Stelle über
*1. die **Identität der verantwortlichen** Stelle,*
*2. die **Zweckbestimmungen** der Erhebung, Verarbeitung oder Nutzung und*
3. die Kategorien von Empfängern nur, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss, zu unterrichten. Werden personenbezogene Daten beim Betroffenen aufgrund einer Rechtsvorschrift erhoben, die zur Auskunft verpflichtet, oder ist die Erteilung der Auskunft Voraussetzung für die Gewährung von Rechtsvorteilen, so ist der Betroffene hierauf, sonst auf die Freiwilligkeit seiner Angaben hinzuweisen. Soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, ist er über die Rechtsvorschrift und über die Folgen der Verweigerung von Angaben aufzuklären.

Um den sachlichen Anwendungsbereich eröffnen zu können, müssen die folgenden drei Kriterien erfüllt sein:

- Personenbezug
- Erhebung, Verarbeitung und Nutzung
- Einwilligung des Betroffenen oder
- Erlaubnis durch Rechtsvorschrift

aa) Personenbezug

Auch in diesem Szenario wird nur die Kundennummer des Betroffenen auf dem RFID Transponder gespeichert. Obwohl hier nur die Ausstellung der RFID-Kundenkarte geprüft wird, es wichtig, die spätere Verwendung zu betrachten. Im

Gegensatz zum „tatsächlichen Szenario“ wird hier die Kundennummer mit dem Zweck erhoben, diese später zu Abrechnungszwecken zu verwenden. Bei diesem Zweck wird das Datum „Kundennummer“ erhoben und dem Betroffenen zugeordnet (z.B. um die Waren auf dessen Kundenkonto zu buchen und dieses ggf. via Bankeinzug zu begleichen). Es ist deshalb als personenbezogen anzusehen. Das Kriterium des Personenbezugs ist erfüllt.
(„Stellvertreterfunktion“ der Kundennummer)

bb) Erhebung, Verarbeitung und Nutzung

Der Anwendungsbereich erstreckt sich auf

- Erhebung,
- Verarbeitung und
- Nutzung

von personenbezogenen Daten.
Die Termini sind in § 3 BDSG legal definiert.

§ 3 Abs. 3-5 BDSG
(3) Erheben ist das Beschaffen von Daten über den Betroffenen.
(4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:
1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,
2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,
3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass
a) die Daten an den Dritten weitergegeben werden oder
b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,
4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,
5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.
(5) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

Erheben von Daten im Sinne von § 3 Abs. 3 BDSG liegt im Szenario vor.
Die Speicherung der Kundennummer in RFID-Transponder kann als Aufbewahrung zur späteren Nutzung verstanden und deshalb unter § 3 Abs. 4 Satz 1 BDSG subsumiert werden, sie fällt also nicht in die Kategorie „Verarbeitung“. Eine Verarbeitung liegt hier also nicht vor.
Die Nutzung ist in § 3 Abs. 5 BDSG als jegliche Verwendung der Daten definiert, die nicht in die Kategorie Verarbeitung fällt. Im Szenario ist diese Nutzung die (direkte) Ermittlung des Kundenkontos und die (indirekt) damit zusammenhängenden Zahlungsfunktionen.
Der Anwendungsbreich deckt den gesamten Vorgang der Kartenausstellung ab (Erhebung + Speicherung).

cc) Einwilligung des Betroffenen

Die Einwilligung im Sinne des BDSG ist in § 4a BDSG legal definiert.

BDSG § 4a Einwilligung
*(1) Die **Einwilligung** ist nur wirksam, wenn sie auf der **freien Entscheidung** des Betroffenen beruht. Er ist auf den **vorgesehenen Zweck der Erhebung,** Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie besonders hervorzuheben.*
(2) Im Bereich der wissenschaftlichen Forschung liegt ein besonderer Umstand im Sinne von Absatz 1 Satz 3 auch dann vor, wenn durch die Schriftform der bestimmte Forschungszweck erheblich beeinträchtigt würde. In diesem Fall sind der Hinweis nach Absatz 1 Satz 2 und die Gründe, aus denen sich die erhebliche Beeinträchtigung des bestimmten Forschungszwecks ergibt, schriftlich festzuhalten.
(3) Soweit besondere Arten personenbezogener Daten (§ 3 Abs. 9) erhoben, verarbeitet oder genutzt werden, muss sich die Einwilligung darüber hinaus ausdrücklich auf diese Daten beziehen.

In formeller Hinsicht muss die Einwilligung in Schriftform erfolgen. Weiterhin muss diese besonders hervorgehoben sein, wenn sie zusammen mit anderen Erklärungen erfolgt. Im Beispiel ist mindestens zu fordern, dass die Metro dem Kunden bei Aushändigung der Karte ein entsprechendes Formblatt abzeichnen lässt. Darin muss die Willenserklärung besonders hervorgehoben werden und der Zweck der Datenerhebung definiert sein. Zu einem anderen Zweck als dem definierten ist eine Verwendung der Daten nicht zulässig. An dieser Stelle soll nochmals auf das Szenario 2 zurückgeblickt werden:
Laut Website des Foebud wurden in der Multimedia-Abteilung der Metro Aufkleber an den Medien selbst angebracht, die auf eine Erhebung der Daten zur Alterskontrolle hinweisen. Ein solcher Hinweis ist selbstverständlich nicht schädlich, jedoch lässt sich daraus beim Erheben personenbezogener Daten mittels einer Kundenkarte keine Zulässigkeit ableiten. Ein „Hinweisschild“ an der Kasse der Metro genügt also nicht, um den Betroffenen über den Zweck der Datenerhebung nach § 4a BDSG zu informieren.
Sollte die Metro bei der Ausstellung der Karte nicht auf diesem Zweck hingewiesen haben, so ist zu wäre der Einsatz nicht zulässig (Verfolgt
In materieller Hinsicht muss die Einwilligung des Betroffenen auf einer freien Entscheidung beruhen. Daraus wird nach herrschender Meinung ein „Kopplunsgverbot“ zwischen der Teilnahme an einem etwaigen Bonusprogramm und einer Einwilligung in die Verarbeitung der personenbezogenem Daten zu Werbe- und Marketingzwecken abgeleitet. Die Entscheidung wäre also nicht als frei anzusehen, wenn die Erhebung der Daten an die Teilnahme an „Payback“ gekoppelt wäre. Der Payback-Aspekt soll hier aber nicht weiter untersucht werden, da er von Thema RFID wegführt. RFID-Kundenkarte hat in dieser Betrachtung nur den Zweck, den Zahlungsvorgang an der Kasse zu vereinfachen.
§ 4a BDSG fordert die genaue Nennung des Zwecks. Hier wäre der Kunde also über den Zweck der Datenerhebung hinzuweisen. Eine Hinweispflicht über die technischen Details des Auslesevorgangs kann hier nicht abgeleitet werden (also

etwas ein Hinweis auf RFID-Technik), jedoch ist eine genaue Angabe der Art und Weise des Auslesevorgangs zu fordern, da der Betroffene nur so ein Recht auf informationelle Sebstbestimmung anwenden kann (z.B. die Karte auch nicht zu verwenden). Die logische Konsequenz ist, dass der Betroffene ggf. auch auf einen nicht durch den aktiven Gebrauch der Karte veranlassten Auslesevorgang zu informieren ist. Sollte also der Zahlvorgang an der Kasse ausgelöst werden, indem der „mit der Karte in der Tasche“ vor der Kasse steht, muss der Betroffene auf die Umstände (Ort, Reichweite, Dauer etc.) dieser schon bei der Ausstellung der Kundenkarte bzw. der Einwilligung hingewiesen werden.
Wenn RFID-Kundenkarte eine zwingende Voraussetzung zum Kauf von Multimedia-Produkten bei der Metro gewesen ist (also ein Kunden ohne RFID-Kundenkarte an der Kasse nicht zahlen könnte), läge ebenso keine freie Entscheidung vor. Die Entscheidungsmöglichkeiten des Kunden wären dann nur die, Käufe im Metro Markt zu tätigen oder nicht zu tätigen. Jedoch fordert § 4a BDSG eine freie Entscheidung in der Frage der Datenerhebung. Eine freie Entscheidung wäre hier also nicht gegeben.
Unter der Annahme, dass auch andere Zahlunsgmethoden ermöglicht werden und die formellen Kriterien eingehalten werden, ist eine Einwilligung nach § 4a BDSG möglich und die Ausstellung der RFID-Kundenkarte zulässig.

dd) Zwischenergebnis

Die Rechtmäßigkeit kann sowohl unter gewissen Rahmenbedingungen durch Einwilligung des Betroffenen begründet werden (§ 4a BDSG).

c) Datenorganisation

Die Daten werden beim Betroffenen erhoben. Dies ist i.S.v. § 4 Abs. 2 BDSG.
Unklar ist, ob der Betroffene seine Kundennummer tatsächlich kennt. Sollte die Kundennummer bei der Ausstellung der Karte durch die Metro ermittelt werden, jedoch wäre die Metro nur als Verrichtungsgehilfe bei der Ermittlung der Kundennummer anzusehen. Die Erhebung erfolgt deshalb auch in diesem Fall direkt beim Kunden.
Die Identität der verantwortlichen Stelle ist dem Kunden bekannt, denn er ist bereits Kunde des Future Store, welcher die Karte ausstellt. (§ 4 Abs. 3 Satz 1).

d) Zusammenfassung

Die Ausstellung der Kundenkarte ist unter Einwilligung des Betroffenen zulässig. Die Einwilligung Bedarf gewisser Rahmenbedingungen. (Siehe oben)

4. Transparenzanforderungen an RFID als mobile personenbezogene Speicher- und Verarbeitungsmedien (§ 6c BDSG)

BDSG § 6c Mobile personenbezogene Speicher- und Verarbeitungsmedien
(1)Die Stelle, die ein mobiles personenbezogenes Speicher- und Verarbeitungsmedium ausgibt oder ein Verfahren zur automatisierten Verarbeitung personenbezogener Daten, das ganz oder teilweise auf einem solchen Medium abläuft, auf das Medium aufbringt, ändert oder hierzu bereithält, muss den Betroffenen
(...)

a) Örtlicher Anwendungsbereich

Der örtliche Anwendungsbereich ist in § 1 Abs. 2 BDSG normiert. Der örtliche Anwendungsbereich ist eröffnet (Begründung siehe oben).

b) Sachlicher Anwendungsbereich

Es bleibt also zu prüfen, ob hier ein „mobiles personenbezogenes Speicher- und Verarbeitungsmedium“ vorliegt. Dies ist in § 3 Abs. 10 legal definiert.

§ 3 Abs. 10 BDSG
(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,
1. die an den Betroffenen ausgegeben werden,
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.

Die Legaldefiniton fordert wie im BDSG üblich die Verarbeitung eines personenbezogenen Datums. Im Szenario ist einen Personenbezug der Kundennummer gegeben, da diese mit dem Kundenkonto und folglich dem Kunden zugeordnet wird.
§ 3 Abs. 10 Nr. 1 Nr. 1 BDSG ist erfüllt, denn der Transponder auf der Kundenkarte enthält einen Speicher[77] und wird an den Betroffenen ausgegeben. Weiterhin müsste das Medium derart beschaffen sein, dass der Betroffene die Verarbeitung nur durch den Gebrauch des Mediums beeinflussen könnte (§ 3 Abs. 10 Nr. 3). Zur Verdeutlichung: Als „Gebrauch“ wäre hier etwa das Einstecken einer Karte in ein Lesegerät zu verstehen. Ein Platzieren der Kundenkarte vor einem Lesegerät[78] wäre dem im rechtlichen Sinne gleichzusetzen. Die Möglichkeit zur Beeinflussung der Verarbeitung dürfte auch nicht über den Gebrauch hinausgehen. Ein Medium, bei dem der Betroffene die Verarbeitung über den Gebrauch hinaus beeinflussen könnte, erfüllt die Voraussetzung von § 3 Abs. 10 Satz 3 nicht. Beispiele hierfür sind PDAs[79] oder

[77] Es kam ein Transponder nach ISO 15693 zum Einsatz, also einen Speichermedium ohne eigenen Prozessor
[78] Als Platzieren kann auch dichtes „Vorbeiziehen“ verstanden werden.
[79] PDA sind Personal Digital Assistants. Hierunter fallen Palm, PocketPC, Psion usw.

Notebooks, die eine Beeinflussung der Verarbeitung über Tastatur oder Griffel ermöglichen.[80]
Drittens wird in § 3 Abs. 10 Nr. 3 BDSG gefordert, dass auf dem dem Medium personenbezogene Daten verarbeitet werden „können“. Der reine Speichervorgang ist i.S.v. § 3 Abs. 4 Nr. 1 keine Verarbeitung (Die Daten werden lediglich zur späteren Verarbeitung „aufbewahrt“).
Zur Art und Weise des Auslesevorgangs gibt es im BDSG keine konkreten Regelungen. Insbesondere ist ist bei der Legaldefinition belanglos, ob der dieser kontaktbehaftet oder kontaktlos erfolgt. Da der Transponder nicht über einen Prozessor verfügt, fehlt dem Medium im Szenario die notwendige Voraussetzung einer Verarbeitungsmöglichkeit (§ 3 Abs. 10 Nr. 2)
Der sachliche Anwendungsbereich kann nicht eröffnet werden.

5. Ergebnis

Die Ausstellung der Kundenkarte und die damit verbundenen Datenerhebung sowie die Nutzung der Karte an der Kasse im Szenario 3 ist nur mit Einwilligung des Betroffenen i.S.v. § 4a BDSG zulässig.

IX. Datensicherheit

Die Daten (Kundennummer) aus dem RFID-Transponder der Kundenkarte können durch Dritte mit handelsüblichen Readern gelesen werden.
Hier sei ebenfalls nochmals angemerkt, dass dieses Szenario fiktiv ist. Zwar war es dem Foebud e.V. möglich, diese Kundenkarte auszulesen und zu beschreiben, jedoch hatte diese Karte im realen Szenario keine Zahlungsfunktion.

1. Voraussetzungen

Es kommt § 9 BDSG nebst Anlage in Betracht.

[80] Vgl. Simitis, BDSG/Bizer Rdnr. 275

BDSG § 9 Technische und organisatorische Maßnahmen
Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

2. Technische und organisatorische Maßnahmen (§ 9 BDSG)

a) Örtlicher Anwendungsbereich

Der örtliche Anwendungsbereich ist in § 1 Abs. 2 BDSG normiert. Der örtliche Anwendungsbereich ist eröffnet (Begründung siehe oben).

b) Sachlicher Anwendungsbereich

Der Anwendungsbereich erstreckt sich auf öffentliche als auch auf nicht-öffentliche Stellen, die personenbezogene Daten verarbeiten. Wie oben gezeigt liegt im Szenario eine solche Verarbeitung vor; auch handelt es sich bei der Metro um eine nicht-öffentliche Stelle. Der sachliche Anwendungsbereich ist grundsätzlich eröffnet. Der § verpflichtet das Unternehmen zu technischen und organisatorischen Maßnahmen, die nötig sind, um die Regelungen des BDSG einhalten zu können. Hier lässt sich im Allgemeinen der Aspekt der Datensicherheit subsumieren, denn ohne Datensicherheit ist Datenschutz nicht möglich. Dafür spricht auch, dass der § die Unternehmen verpflichtet, insbesondere die in der Anlage zum § 9 BDSG Satz 1 aufgeführten Punkte zu gewährleisten.
Über die innerbetrieblichen Maßnahmen ist im Szenario nichts bekannt. Es soll davon ausgegangen werden, dass die Datenverarbeitungssysteme, die nicht direkt mit der Übertragung von mit RFID zusammenhängen den Anforderungen aus § 9 BDSG genügen (Hier sind z.B. die Computerkasse, das Warenwirtschaftssystem etc. gemeint)
Es bleibt, die folgenden Punkte daraufhin zu prüfen, ob der Schutz der Daten, welche auf dem Transponder gespeichert sind, i.S.v. § 9 BDSG angemessen ist:

- Datenübertragung beim Zahlvorgang
- „Mit sich führen“ der Kundenkarte (auch außerhalb des Metro-Geländes)

aa) Datenübertragung beim Zahlvorgang

Im Szenario liegen zur Bewertung keine ausreichenden Informationen über den Zahlvorgang vor. Im Szenario 2 wurde eine Kundenkarte eingesetzt, die keine

verschlüsselte Übertragung der Daten erlaubte. Es soll deshalb weiterhin davon ausgegangen werden, dass die gleiche Karte zum Einsatz kommt.
Ein hier vorliegendes Problem der Datensicherheit ist sicherlich das Fälschen einer Kundennummer durch einen Angreifer zum Zwecke des Betrugs bei der Zahlung (Der Warenkorb wird auf das Kundenkonto eines Dritten gebucht und die Rechnung durch diesen ohne dessen Wissen beglichen). Zur Fälschung der Kundennummer könnte diese zuvor durch einen unberechtigten Dritten ausgelesen werden.[81] Der Angreifer kennt dabei jedoch keine weiteren Daten des Betroffenen. Für den Angreifer ist es deshalb nicht personenbezogen. Es ist also zu prüfen, ob dies in den Anwendungsbereich des BDSG fällt. Im „Dreiecksverhältnis“ zwischen Betroffenem, Metro und Angreifer ist das Datum als personenbezogen anzusehen: Das Datum ist während des Zahlvorgangs personenbezogen, da Metro es mit weiteren Daten verknüpft. Selbst wenn dem Angreifer diese Verknüpfung verborgen bleibt, ergibt sich für den Betroffenen eine Beeinträchtigung seines Persönlichkeitsrechts. Genau darauf erstreckt sich der Schutzbereich des BDSG. Dieser in ist in § 1 BDSG normiert: Der Einzelne soll davor geschützt werden, dass durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird (Die Beeinträchtigung ergibt sich aus den unerwünschten Kontenbewegungen des Betroffenen und dem damit verbundenen Aufwand, eine Richtigstellung zu erwirken). Der sachliche Anwendungsbereich vom § 9 BDSG ist folglich eröffnet. Hieraus ergibt sich eine Pflicht zu Datensicherheit, um der Metro überhaupt zu ermöglichen, die Regelungen des BDSG einzuhalten. Eingeschränkt wird diese Pflicht in § 9 BDSG nur durch die Verhältnismäßigkeit. Da es sich bei dem „Schutzobjekt“ um das Girokonto des Betroffenen handelt, steht außer Frage, dass die Schutzmaßnahmen nicht ausreichend sind (Denn faktisch gibt es keine[82]). Welche Schutzziele diese Maßnahmen erreichen sollten, ist in der Anlage z § 9 BDSG festgehalten. Dies wird im nächsten Punkt noch eingehender dargestellt werden.

bb) „Mit sich führen“ der Kundenkarte

Im Gegensatz zum Zahlungsvorgang könnte der Transponder von Dritten ausgelesen werden. Hier kann im Grunde genommen wie oben argumentiert werden. Ein Angreifer könnte die Nummer des Betroffenen auslesen. Da die Kundennummer für sich jedoch nicht personenbezogen ist, kann eine

[81] Alternativ könnte der Betrüger natürlich auch versuchen, fremde Nummern zu erraten. Insbesondere scheint dieser Weg einfach, wenn es sich um fortlaufende Nummern handelt. Es soll aber davon ausgegangen werden, dass der Betrüger eine Nummer auslesen möchte, um tatsächlich eine „passende“ Nummer zu erhalten.

[82] Lediglich die begrenzte Reichweite des Transponders und die Notwendigkeit für einen Angreifer, einen Reader zu kaufen schützen die Daten des Betroffenen

Anwendbarkeit von § 9 BDSG nur daraus hergeleitet werden, dass der Auslesevorgang durch den Angreifer in Nähe der Metro , z.B. beim Verlassen des Geländes, durchgeführt wird. Der Angreifer kann den Zusammenhang zwischen Kudennummer und Metro recht einfach erkennen. Dieser Aspekt muss an dieser Stelle jedoch nicht weiter verfolgt werden, da die Anwendbarkeit von § 9 BDSG bereits oben hergeleitet wurde.

Die Anlage zu § 9 Satz 1 BDSG führt folgende Schutzziele an:

- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeitskontrolle

BDSG Anlage (zu § 9 Satz 1)
Werden personenbezogene Daten automatisiert verarbeitet oder genutzt, ist die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,
1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),
6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

Die zu treffenden Maßnahmen richten sich nach der Art der zu schützenden personenbezogen Daten.

(a) Zutrittskontrolle

Es ist eine Eigenart der RFID-Kundenkarte, dass diese an dem Kunden ausgegeben wird. Eine Zutrittskontrolle (im Sinne einer Zugriffskontrolle) kann

durch die Metro nicht durchgeführt werden – schließlich könnte der Betroffene außerhalb Metrogeländes Opfer eines Taschendiebstahls werden. Eine Verantwortung der Metro hierfür muss abgelehnt werden.

(b) Zugangskontrolle

Der Wortlaut des § besagt, dass die Nutzung der Datenverarbeitungsanlage durch Unbefugte zu verhindern ist. Der Transponder ist jedoch keine Datenverarbeitungsanlage. Es handelt sich im hier vorgestellten Szenario um ein reines Speichermedium, welches i.S.v. § 3 Abs. 10 BDSG keine Verarbeitung (Begründung siehe oben). Eine Zugangskontrolle kann hier nicht gefordert werden.

(c) Zugriffskontrolle

Auch ist in der Anlage von Datenverarbeitungsanlagen die Rede. Einen Anwendungs dieser Nummer ist deshalb anzulehnen.

(d) Weitergabekontrolle

Es ist zu gewährleisten, dass personenbezogene während ihres Transports auf einem Datenträger nicht unbefugt gelesen werden können. Unter diesen Punkt lässt sich die Kundenkarte subsumieren. Es handelt sich bei den eingesetzten Karten um Datenträger. Dass dieser transportiert wird, ist offensichtlich. Dass der Transport durch den Betroffenen selbst durchgeführt wird, ist dabei nicht von Bedeutung: Der Transport unterliegt hier den gleichen Gefahren, wie bei einem Transport durch die Metro oder einen Dritten, z.B. einen professionellen Dienstleister wie die Deutsche Post AG.

(e) Eingabekontrolle

Dieses Schutzziel fordert, dass nachvollziehbar ist, wer personenbezogene Daten in Datenverarbeitungsanlagen verändert, eingegeben oder entfernt hat. Auch hier handelt es sich dem Wortlaut nach um Datenverarbeitungsanlagen. Deshalb trifft die Forderung auf die von der Metro eingesetzten RFID-Schreibvorrichtungen zu, jedoch nicht auf den „Datenträger RFID-Kundenkarte“.

(f) Auftragskontrolle

Eine Verarbeitung der personenbezogen Daten „in Auftrag“ liegt im Szenario ohnehin nicht vor.

(g) Verfügbarkeitskontrolle

Die personenbezogen Daten sollen gegen Verlust und Zerstörung geschützt sein. Das Medium selbst ist „State-of-the-Art“ und deutlich unempfindlicher gegen Umwelteinflüsse als vergleichbare Medien. Die Metro kommt der Anforderung nach Schutz gegen Zerstörung angemessen nach. Den Schutz vor Verlust, kann

die Metro nicht gewährleisten. Dies liegt im Verantwortungsbereich des Betroffenen.

c) Zwischenergebnis

Die Kundenkarte im Szenario wird den Anforderungen zur Datensicherheit nicht gerecht: Das Schutzziel der Weitergabekontrolle ist verletzt.

3. Ergebnis

Der Einsatz der RFID-Kundenkarte im Szenario ist unzulässig.
Hier sei darauf hingewiesen, dass es sich in diesem fiktiven Szenario um einen Basisfall des Einsatzes von RFID-Kundenkarten handelt. Deshalb kann dieses Ergebnis nicht ohne Weiteres auf andere Fälle dieser Art bezogen werden. Die Unzulässigkeit ergibt sich in der Fallprüfung nur dadurch, dass der eingesetzte RFID-Transponder seiner Beschaffenheit nach nicht geeignet ist, eine Weitergabekontrolle i.S.v. § 9 BDSG zu gewährleisten. Schon durch Einsatz alternativer Transpondertypen könnte die RFID-Kundenkarte im Hinblick auf die Datensicherheitsanforderungen dem BDSG gerecht werden. Als Beispiel wären hier Karten nach dem ISO-14443 Standard zu nennen, sofern diese von der in Standard verankerten Möglichkeit einer Verschlüsselung Gebrauch machen. Wenn man eine solche Karte annimmt, wäre nach obiger Argumentation der Einsatz der RFID-Kundenkarte im Szenario unter Annahme der Einwilligung des Betroffenen wahrscheinlich zulässig.
Die Betrachtung dieses „plain case“ soll die grundsätzlichen Probleme beim Einsatz von RFID-Technik aufzeigen. Die Prüfung möglicher Abweichungen zum Szenario soll den einsetzenden Unternehmen und Datenschützern überlassen werden.

F Kritik

Wie bei der rechtlichen Bewertung der Szenarien aufgezeigt wurde, ist der Einsatz von RFID Technik unter gewissen Voraussetzungen sowohl im öffentlich-rechtlichen als auch im privatrechtlichen Umfeld nach geltendem Recht zulässig. Allerdings wurde die Rechtmäßigkeit anhand von Gesetzen begründet, zu deren Entstehungszeit ein so weitreichender Einsatz von RFID nicht voraussehbar war. Gerade für den Bereich des Cyberlaw hat sich gezeigt, dass neue spezialisierte Gesetzte notwendig sein können, wie beispielsweise das Teledienstegesetz. Wie oben dargelegt wurde, vollzieht sich bei RFID Technologie durch Verschmelzung mit dem Internet ein Wandel zum ubiquitous und pervasive Computing. Deshalb sollte RFID jetzt schon als Teil des Cyberlaw

verstanden werden. Jedoch kennt die bestehende deutsche Gesetzgebung keine Spezialgesetzgebung für RFID. Diese wird vom Bundesdatenschuzbeauftragten in der letzten Zeit immer wieder gefordert[83] [84], jedoch sind bisher noch keine konkreten Vorschläge für Gesetzesänderungen von ihm vorgebracht worden. Im Gegensatz dazu hat der Verbraucherschutzverband CASPIAN in den USA einen konkreten Vorschlag zur Änderung der bestehenden Gesetze gemacht. An der aktuellen „kleinen Anfrage“ der FDP zum Thema RFID[85] lässt sich ableiten, dass man in der Politik die neuartigen Fragen an die Rechtswissenschaft beim Einsatz von RFID Technik erkannt hat.
Im Folgenden soll versucht werden einen Beitrag in der Diskussion um mögliche Gesetzesänderungen zu leisten. Wichtig bei der Entwicklung dieses Vorschlages war es, einen Kompromiss zu finden, der die Rechte der Betroffenen schützt, aber trotzdem eine sinnvolle Anwendung von RFID durch die Anwender zulässt.

I. BDSG

1. Legaldefinitionen

Im ersten Schritt sollte eine Legaldefinition für „RFID“ geschaffen werden. Die Legaldefinitionen technischer Begriffe sind in § 3 BDSG „Weitere Begriffsbestimmungen“ zu finden. Es wird vorgeschlagen, § 3 Abs. 10 wie folgt zu ändern:

Bundesdatenschutzgesetz § 3 Abs. 10: Weitere Begriffsbestimmungen
(10) Mobile personenbezogene Speicher- und Verarbeitungsmedien sind Datenträger,
1. die der Betroffene bei sich tragen kann
2. auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und
3. bei denen diese Verarbeitung durch den Gebrauch des Mediums beeinflusst werden kann.

Der bisherige Wortlaut § 3 Abs. 10 Nr. 1 BDSG lautet in der derzeitigen Fassung: „die an den Betroffenen ausgegeben werden“. Jedoch ist damit zu rechnen, dass zukünftig sehr viele Dinge mit RFID ausgestattet sein werden. Von einem „Ausgeben“ an den Betroffen kann dann nicht mehr gesprochen werden. Es werden Dinge in den Besitz des Betroffenen gelangen, die mit RFID ausgestattet sind. Der Betroffene nimmt das Ding samt dem Transponder an sich. Es liegt im Allgemeinen also keine aktive Entscheidung des Betroffenen vor, den RFID-Transponder anzunehmen. Jedoch genau dies würde der Begriff „ausgeben“ suggerieren.

[83] Vgl. Focus Website. Internet: http://focus.msn.de/F/FM/FMB/FMBA/fmba.htm?snr=3484. Stand 16.8.2004
[84] Entschließung der Datenschutzbeauftragten des Bundes und der Länder: Entschließung zu Radio-Frequency Identification. Internet: http://www.bfd.bund.de/information/DS-Konferenzen/67dsk_ent5.pdf.Stand 08.12.2004
[85] Deutscher Bundestag. 15 Wahlperiode. Drucksache 15/3025 vom 28.04.2004. Internet: http://dip.bundestag.de/btd/15/030/1503025.pdf. Stand 22.08.2004

Zu § 3 Abs. 10 Nr. 2 BDSG ist zu sagen, dass diese im Rahmen der aktuellen Diskussion um Datenschutz bei RFID Technik am meisten umstritten ist. Damit ein RFID-Transponder unter § 3 Abs. 10 Nr. 2 BDSG als mobiles personenbezogenes Speicher- und Verarbeitungsmedium zu subsumieren ist, muss der Transponder personenbezogene Daten verarbeiten. Eine reine Speicherung ist hier nicht ausreichend. Als besonders problematisch wird jedoch gesehen, dass der Anwender die eineindeutige Kennung des RFID-Tags mit den Datenbanken verknüpfen kann und den Betroffenen so eineindeutig identifizieren könnte. Hier wird jedoch von einer Änderung des § 3 Abs. 10 Nr. 2 BDSG abgesehen.

a) Legaldefinition: RFID-Transponder (§ 3 Abs. 11 BDSG)

Die Legaldefinition wurde in § 3 Abs. 11 BDSG eingefügt.

Bundesdatenschutzgesetz § 3 Abs. 11 BDSG: Weitere Begriffsbestimmungen
(11) RFID (Remote Frequency IDentification) ist eine Technik, die an ein Speichermedium oder ein Verarbeitungsmedium gebunden ist,
1. das an oder in Objekten und auch Lebewesen verwendet werden kann und
2. dessen Abmessungen eine für die Betroffenen nicht erkennbare An- oder Einbringung erlauben, und
3. das eine Übertragung der Daten

a) ohne Berührung

b) über eine begrenzte Entfernung

c) auch durch undurchsichtige Materialien ermöglichen kann.

Hier wurde das Akronym „RFID“ gewählt, da es in der technischen Fachliteratur am weitesten verbreitet ist und einen Gattungsbegriff für diese Technik darstellt. Im Gegensatz zu synonymen Begriffen wie „Transponder“, „Spychip“ oder „ID-Tag“ ist der Begriff bzw. sind seine Bestandteile selbst nicht technizistisch und beschreiben ihre Funktion quasi selbst. Lediglich der Umstand, dass die erklärenden Bestandteile aus dem Englischen kommen, lassen sie in der deutschen Gesetzgebungssprache etwas deplatziert wirken.
Die Definition soll sowohl RFID-Transponder mit Speicherkapazität, als auch solche mit Prozessoren und weiteren Funktionen erfassen. Deshalb wurden die Begriffe „Speichermedium“ und „Verabeitungsmedium“ aufgenommen.
Weiterhin soll die Definition die universelle Verwendung an Personen, Tieren und Gegenständen umfassen. Dieser Gedanke ist in § 3 Abs. 11 Nr. 1 BDSG zu finden. Ebenso soll als Eigenschaft von RFID-Transpondern aufgefasst werden, dass diese i.d.R. „winzig“ sind, zumindest in Relation zum Träger des Transponders. Eine erkennbare Anbringung in einem KFZ kann also durchaus mit größeren Transpondern erfolgen als die zur Kennzeichnung eines Menschen eingesetzten. Dieser Aspekt und auch die Möglichkeit, Transponder in Lebewesen zu implantieren spiegeln sich in § 3 Abs. 11 Nr . 2 BDSG wieder.

§ 3 Abs. 11 Nr. 3 a) und c) BDSG entsprechen den technischen Gegebenheiten und bedürfen hier keiner Erklärung. Jedoch sollte auf § 3 Abs. 11 Nr. 2 b) eingegangen werden:
Das Problem ist, so präzise zu definieren, dass alle RFID Techniken jedoch keine nicht-RFID Techniken, wie etwa schnurlose Telefone oder Bluetooth-Gertäte, erfasst werden. Eine Einschränkung auf Chips ohne eigene Batterie oder Stromversorgung würde (passive) RFID-Tags von diesen abgrenzen, jedoch ist davon auszugehen, dass die Hersteller RFID-Chips mit integrierter Stromversorgung produzieren würden, um nicht unter die Legaldefinition von RFID zu fallen. Es stellt bei heutigem Stand der Technik kein Problem dar, einen Akku oder eine Kapazität auf einen Chip zu integrieren.

b) Legaldefinition: RFID-System (§ 3 Abs. 12 BDSG)

Es wird vorgeschlagen, in § 3 BDSG eine Definition für den Terminus „RFID-System“ als § 3 Abs. 12 BDSG einzufügen. Der Definition liegt die Idee zugrunde, die Verarbeitung personenbeziehbarer Daten innerhalb eines „geschlossenen“ RFID-System zuzulassen, sofern diese mittels RFID erhoben wurden und diese das System nicht „verlassen“. Hier ist keine Beeinträchtigung des Persönlichkeitsrechts des Betroffenen zu erwarten, da die Daten nicht mit anderen Datenverarbeitungsanlagen verknüpft werden können.

Bundesdatenschutzgesetz § 3 Abs. 12 BDSG: Weitere Begriffsbestimmungen
(12) RFID-System bezeichnet alle Komponenten und Datenverarbeitungsanlagen,
1. die mit RFID erhobene Daten verarbeiten, speichern oder übertragen,und
2. die zum Speichern oder Auslesen von Daten mittels RFID notwendig sind, sowie
3. solche, die erhobene Daten in keiner direkten oder indirekten Form aus dem RFID-System hinaus übertragen.

Die Definition erfasst sowohl die Transponder als auch die Reader, die in einem RFID-System zum Einsatz kommen können.
Weiterhin ist es notwendig, Sensoren, Speicher, Displays und Ähnliches in die Definition aufzunehmen, da diese in der Praxis häufig mit den Readern verbunden sind. Auch eine Integration direkt in den Transponder ist möglich. Auf jeden Fall ist festzuhalten, dass zwischen den Komponenten Daten übertragen werden. Sofern diese jedoch keine personenbeziehbaren Daten aus dem RFID-Systems hinaus übertragen, sollte diese sozusagen als Bestandteil des Systems gewertet werden, denn sie bereiten für den Datenschutz keine Probleme. Diese Regelung ermöglicht es den Anwendern, datenverarbeitende Komponenten an das System anzuschließen ohne für diese besondere Vorkehrungen für den Datenschutz treffen zu müssen (Dies wird im unten folgenden Ergänzungsvorschlag noch genauer dargelegt)

aa) Beispiel

Dieses Paradigma der „lokalen Datenhaltung“ soll am Beispiel eines Readers für EPC Kennungen verdeutlicht werden. Der Reader besteht aus einem kleinen Display, das Produktbezeichnung, Gewicht und Preis anzeigen soll. Der Reader soll an den Regalen angebracht werden und das klassische auf Papier geduckte Preisschildchen ersetzen. Aus Sicht des Unternehmens müssen dann nur noch die Produkte in das Regalfach gelegt werden und das elektronische Preisschildchen passt sich automatisch dem Produkt an.
Aus technischer Sicht könnte die Technik des Preisschildchens so beschaffen sein, dass die EPC Kennung an die zentrale Datenbank übertragen und dort verarbeitet wird. Anschließend erfolgt eine Übertragung der ermittelten Produktdaten an das Preisschildchen. Alternativ könnte das Geräte wie folgt beschaffen sein:
Das Gerät ist neben den für RFID notwendigen Komponenten mit einer internen „Übersetzungstabelle“ für EPC Kennungen in die „normale Sprache“[86] und einem Display zur Anzeige ausgestattet. Die Ermittlung der Produktdaten erfolgt durch Abgleich mit den erhobenen EPC Kennungen. Ein Abgleich mit externen Datenverarbeitungsanlagen ist nicht notwendig. Die beiden Zusatzkomponenten sind zum bloßen Erheben von Daten mit RFID nicht notwendig (es erfolgt eine Verarbeitung die nicht zum „Aufnehmen“ der Daten gehört), sollen aber trotzdem als Bestandteil des „RFID-Systems“ verstanden werden, da die erhobenen Daten nicht an nachgelagerte Datenverarbeitungsanlagen übertragen werden. Aus Sicht des Betroffenen wird dieser Aspekt erst dann interessant, wenn ein Personenbezug hergestellt werden könnte. Würde in einer Datenverarbeitungsanlage der „Abgang“ des Produktes bzw. der EPC Kennung gespeichert, so wäre spätestens an der Kasse ein Personenbezug herstellbar (Profilbildung). Durch eine strikte Datenhaltung im (geschlossenen) RFID-System „Preisschildchen-Produkt“ kann dem also vorgebeugt werden und trotzdem der Zweck des Anwenders (automatische Preisauszeichnung) erfüllt werden.

2. Unschärfe

Weiterhin wird vorgeschlagen, folgenden Absatz in das BDSG einzufügen:

[86] Z.B. „123456789“ wird übersetzt nach „Coladose XY“

Bundesdatenschutzgesetz § 3b: Kontrollierbarkeit und Datenunschärfe bei RFID-Systemen
(1) Werden personenbeziehbare Daten in RFID-Systemen gespeichert, so ist dafür Sorge zu tragen, dass eine Kontrollierbarkeit der Einhaltung der Grundsätze von § 3a BDSG mit angemessenen Mitteln möglich ist. (Transparenz)
(2) Ist eine Kontrollierbarkeit nach Abs. 1 nicht möglich, so muss ein RFID-System eingesetzt werden, dass einen Schutz der personenbeziehbaren Daten erzwingt. (Impliziter Schutz)
(3) Bei der Übertragung personenbeziehbarer Daten aus dem RFID-System hinaus ist zusätzlich zu den anderen gesetzlichen Regelungen dafür Sorge zu tragen, dass eine Personenbeziehbarkeit der Daten so weit wie möglich verhindert wird. (Unschärfe)

a) Kontrollierbarkeit (§ 3b Abs. 1)

In § 3b BDSG Abs. 1 wird eine Kontrollmöglichkeit der Grundsätze Datenvermeidung und Datensparsamkeit verankert. Es soll mit angemessenen Mitteln ermöglicht werden, eine Einhaltung dieser Grundsätze beim Einsatz von RFID-Systemen durch Kontrollen sicherzustellen. Dies impliziert zwei Dinge: Erstens muss der Betroffene überhaupt Kenntnis über den Einsatz von RFID erlangen können, woraus im allgemeinen eine Kennzeichnungs- oder Hinweispflicht abgeleitet werden kann. Zweitens muss dem Betroffenen die Möglichkeit gegeben werden, die im RFID-Tag gespeicherten Daten einsehen zu können.

aa) Beispiel

Ein Supermarkt erhebt mit einem universellen RFID-Reader an der Kasse die Daten, die notwendig sind, um den Gesamtpreis des Warenbündels eines Kunden zu ermitteln. Der Kunde zahlt mittels Kreditkarte. Es stellt sich die Frage, welche Daten der Supermarkt über den Kauf speichert und insbesondere ob die Information über den Kauf (genaue Artikel, Einkaufszeit und- datum, etc.) weiter als nötig gespeichert werden (Datensparsamkeit). Einzig der Gesamtpreis des Warenkorbes ist zur Abrechnung (Zweck) notwendig. Eine Rechtfertigung zur Speicherung anderer Details ist nicht ersichtlich. Selbst wenn der Supermarkt garantiert, dass eine solche Speicherung nicht stattfindet, muss der eine Möglichkeit bieten, dies für den Betroffenen transparent zu machen. Dies mag drastisch wirken, da es Kosten für die Bereitstellung der Gerätschaften mit sich bringt. Zieht man jedoch in Betracht, dass diese Pflicht durch einen impliziten (technischen) Schutz der personenbeziehbaren Daten im RFID-System aufgehoben werden kann, so wird deutlich, dass es sich nur um eine Not- oder Übergangslösung handeln soll, bis ein System mit implizitem Schutz zum Einsatz kommt: Im Beispiel könnte der Supermarkt z.B. über ein Display den Auslesevorgang transparent machen („Ihr Warenkorb bestehend aus einer Cola-Dose hat einen Preis von x Euro. Möchten Sie diesen Preis an die Kasse übermitteln?“).

bb) „RFID-Datenschutz-Gütesiegel“

An dieser Stelle bietet es sich ebenfalls an, ein „RFID-Datenschutz-Gütesiegel“ vorzuschlagen:
Ein unabhängiges Institut prüft, ob die Technik des Supermarktes so ausgelegt ist, dass sie konform zum Gesetz ist. Diese Prüfung betrifft die gesamte Datenverarbeitung des Unternehmens, die die Möglichkeit zur Verarbeitung personenbeziehbarer Daten bietet. Es wird dahingehend geprüft, ob die Technik, den Umgang mit den Daten nur im Rahmen der Regelungen des BDSG zulässt. Eine Abgrenzung kann über die Schnittstellen in der Software erfolgen. Diese sollten so beschaffen sein, dass sie eine Zweckentfremdung ad-hoc nicht zulassen[87] und keinem Mitarbeiter eine freie Verwendung der Daten ermöglichen. Ein sicherer Schutz vor einem Missbrauch der Daten kann so nicht gewährleistet werden, da Software i.d.R. konfigurierbar ist. Jedoch wäre ein Missbrauch der personenbezogenen dann kein „Kavaliersdelikt“ mehr, sondern würde aktive Maßnahmen zur Umstellung der Technik mit sich bringen.
Digital signierte Software-Schnittstellen könnten diese Schutzmaßnahme noch weiter verstärken. Die Zertifizierung sollte als kontinuierlicher Prozess verstanden werden, um die Qualität des Gütesiegels nach eventuellen Änderungen in der IT-Landschaft des RFID-Anwenders aufrecht zu erhalten. .
Beide Verfahren werden hier nur angerissen, um die möglichen Folgen und damit den Sinn des vorgeschlagenen Absatzes zu zeigen.

b) Impliziter Schutz statt Kontrollierbarkeit (§3b Abs. 2 Satz 1 BDSG)

Das eingesetzte RFID-System kann derart beschaffen sein, dass personenbezogene Daten durch die technische Beschaffenheit des Systems geschützt werden.
Im einfachsten Fall ist liegt ein solcher impliziter Schutz vor, wenn die erhobenen Daten das RFID-System bei Verarbeitung nicht verlassen. Diese Regelung soll den Anwendern der RFID Technik eine Möglichkeit einräumen, die erhobenen Daten im RFID-System automatisiert zu verarbeiten und gleichzeitig vor einer einer zentralen Speicherung und einer möglichen Korrelation der Daten mit anderen Datenbeständen vorbeugen.
Angemerkt sei, dass die Übertragung von betriebsnotwendigen Daten und Programmen kein datenschutzrechtliches Problem darstellt. Hierbei findet zwar eine Übertragung von Daten statt, die aus dem Wirkungsbereich der RFID

[87] Dem Mitarbeiter darf also beispielsweise kein Programm zur Verfügung stehen, das die Funktion bietet: „Erstelle eine Liste aller Kunden, die zwischen 12 und 13 Uhr Bananen gekauft hat“

Technik herausführt[88]. Jedoch wurden die übertragenen Daten nicht mittels RFID erhoben (Und sie lassen auch keinen Rückschluss auf die erhobenen Daten zu). Deshalb gehören auch diese Komponenten zum RFID-System nach §3 Abs. 12 BDSG.

Im ersten Beispiel ist die Aktualisierung der EPC-Übersetzungstabelle ein solcher Fall von betriebsnotwendigen Daten. Ebenso haben die meisten elektronischen Geräte heutzutage Diagnoseschnittstellen oder die Möglichkeit zur Aktualisierung ihrer Betriebssystem-Software („Firmware Upgrade“). Auch hierbei werden keine personenbezogenen Daten übertragen.

Eine technisch sehr feingranulare Lösung für den impliziten Schutz wird in der Arbeit „Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols“[89] vorgestellt. Dort wird ein bestehender RFID Standard um verschiedene Datenschutz-Funktionen erweitert, die sich am Grundsatz der Zweckbindung orientieren. Unter anderem besteht dabei die technische Möglichkeit, eine Datenerhebung als „Local Identification“[90] zu deklarieren. Vereinfacht gesagt, würde eine Anfrage des Kassensystems nach „Local Identification“ eine Datenübertragung der RFID-Transponder auslösen, eine Anfrage nach einem Auslesevorgang zu einem anderen Zweck, beispielsweise „Item Tracking“[91], hingegen nicht.

Es bleibt abzuwarten, in wie weit dieser oder vergleichbare Vorschläge als Standard akzeptiert werden. Es sind folgende Kontraindikationen gegeben:

1. Der bereits verabschiedete Standard müsste geändert werden
2. Eine Änderung am Standard zieht Änderungen an der Hardware nach sich
3. Ein vergleichbares System für den Datenschutz beim Surfen im Internet hat sich bisher nicht etablieren können: P3P[92]
4. Auch diese Lösung schützt nicht gegen böswilligen Missbrauch, etwa gegen den Einsatz modifizierter Reader

Aus der Perspektive des Datenschutzes bleibt zu hoffen, dass die vorgeschlagene Gesetzesänderung Herstellern und Anwendern ausreichend Motivation gibt, einen solchen Standard zu etablieren.

3. Gebot zur „Unschärfe“ (§ 3b Abs. 3 BDSG)

Werden Daten mittels RFID erhoben, besteht durch Verknüpfung mit anderen Daten die Gefahr, nicht-personenbezogene Daten einzelnen Personen zuordnen

[88] Die Übersetzungstabelle wird zwar nur „hineinübetragen“, jedoch liefert das Gerät zumindest Prüfsummen und Quittungsmeldungen zurück.
[89] Floerkemeier, Schneider und Langheinrich: Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols. Internet: ...
[90] „Räumlich begrenzte Identifikation“
[91] „Verfolgung eines Gegenstands“
[92] W3C: Platform for Privacy Preferences (P3P) Project. Internet: http://www.w3.org/P3P/. Stand 31.8.2004

zu können (Personenbeziehbarkeit). Die Speicherung solcher Daten soll in Formaten erfolgen, die eine eineindeutige Identifizierung des Betroffenen auch unter Verwendung von Zusatzwissen nicht ermöglicht.
Ein Beispiel: Bei der Entnahme eines Produktes P aus dem Warenregal eines Supermarktes wird der Abgang der Ware mittels RFID Reader automatisch erhoben. Hierbei werden EPC Kennung, Uhrzeit, etc. gespeichert.
Verknüpft man diese Daten mit den Daten aus dem obigen Kassen-Beispiel, lässt sich hieraus Kenntnis über die exakte Aufenthaltszeit des Kunden am Regal bestimmen (Über die zeitliche Abfolge lässt sich auf diesem Wege ein Bewegungsprofil des Kunden durch den Supermarkt erstellen).
Das Speicherformat sollte so beschaffen sein, dass eine eineindeutige Zuordnung zwischen EPC Kennung und Uhrzeit nicht möglich ist. Die Erstellung eines Bewegungsprofils ist für den Supermarkt so nicht mehr möglich.
Jedoch erfordert das Identifizieren solcher Daten in der Praxis viel Fachkenntnis und zieht hohen Aufwand nach sich. Einfach ausgedrückt, würden die im Beispiel zwei getrennte Listen geführt: Eine mit den entnommenen Produkten, eine weitere mit den Entnahmezeitpunkten. Sie Sortierung der Listen erfolgt beispielsweise jeweils alphabetisch. Eine Verknüpfungstabelle wird nicht geführt. Werden diese Listen nun mit beispielsweise jeweils 100 Elementen übertragen, so ist eine zumindest eine exakte Zuordnung zwischen Zeitpunkt und Produkt möglich, jedoch eine Zuordnung zu einem Zeitraum (nämlich zwischen dem ersten und dem letzten Zeitpunkt in der Liste). Aus diesem Grunde wird hier auch von „Unschärfe“ gesprochen und nicht von Anonymisierung. Das Gebot zur Unschärfe sollte bei RFID zusätzlich zur Datensparsamkeit und Datenvemeidung angewendet werden.

II. Andere Gesetze

Es bleibt zu erwähnen, dass sicherlich entsprechende Änderungen in einigen Spezialgesetzen notwendig werden, da diese die Regelungen des BDSG häufig verdrängen ("lex specialis derogat legi generali"). Als Beispiel sei hier auf das oben herangeführte BGSG verwiesen. Ebenso bietet das UWG im nicht-öffentlichen Umfeld eine gute Möglichkeit den Betroffenen insbesondere vor Belästigungen zu schützen.