Radio Frequency Identification - Innovation vs. Datenschutz?

Bernd Holznagel / Mareike Bonnekoh*

Radio Frequency Identification (RFID) - der Name steht für eine zukunftsträchtige Technologie und bezeichnet Verfahren zur automatischen und verbindungslosen Identifizierung von Objekten über Funk. Während der Handel sich langfristig Einsparungen in Milliardenhöhe erhofft, herrscht auf Seiten der Verbraucher zum Teil großes Misstrauen gegenüber der neuen Transpondertechnologie, denn sie befürchten Eingriffe in ihre Privatsphäre. Dieser Beitrag geht der Frage nach, ob diese Ängste berechtigt sind. Nach einer technischen Einführung (dazu I.) werden die unterschiedlichen Anwendungsbereiche für RFID dargestellt (dazu II.). Zentrale Fragen ergeben sich im Bereich des Datenschutzrechts, die am Beispiel des Einsatzes von RFID-Systemen im Endkundenbereich diskutiert werden (III.). Im Anschluss werden Aspekte der Datensicherheit beleuchtet (IV.).

I. Der technische Hintergrund der Funkerkennung

Jedes Radio Frequency Identification (RFID)-System besteht aus zwei technologischen Komponenten, einem Transponder („Tag") und einem Lesegerät („Reader"). Der Transponder beinhaltet einen elektronischen Mikrochip und eine Antenne zum Senden und Empfangen von Funkwellen.[1] Das Lesegerät setzt sich aus einem Sender, einem Empfänger und einer Antenne zusammen. Außerdem sind die meisten Lesegeräte mit einer Schnittstelle ausgestattet, um die ausgelesenen Daten an ein anderes System weiterleiten und dort verarbeiten zu können. Der Reader sendet in einer festgelegten Frequenz Funksignale aus, die vom Transponder erfasst werden. Das Tag sendet dann seine gespeicherten Daten an das Lesegerät, wo sie erfasst und gespeichert werden. Man unterscheidet aktive und passive RFID-Tags. Aktive Tags sind batteriebetrieben und können sowohl ausgelesen als auch beschrieben werden.[2] Die aktiven Transponder befinden sich im Ruhezustand und senden keinerlei Informationen aus, sofern nicht von einem Lesegerät ein Aktivierungssignal empfangen wird. Sie besitzen im Verhältnis zu passiven Transpondern eine höhere Sendereichweite, haben aber eine geringere Lebensdauer und sind deutlich teurer. Passive Tags kommen hingegen ohne interne Energiequelle aus. Sie werden bei Lesevorgängen über Funkwellen durch die Lesegeräte mit Energie versorgt. Die Menge der gespeicherten Daten ist bei passiven Funkchips wesentlich geringer als bei aktiven Transpondern.

RFID-Systeme können verschiedene Frequenzbänder nutzen.[3] Im Niedrigfrequenzbereich (125-134 kHz) und im Hochfrequenzbereich (13,56 MHz) eignen Transponder sich für Zugangskontrollen, Wegfahrsperren und Lagerverwaltung. Die Herstellungskosten sind hier am geringsten. Genutzt werden kann auch das Ultrahochfrequenzband (868 bzw. 915 MHz) und der Mikrowellenbereich (2,45 GHz).[4] Bei der Nutzung niedriger Frequenzbereiche besitzen Tags ohne Batterie lediglich eine Reichweite von wenigen Zentimetern. Auf hohen Frequenzbändern können aktive Transponder aus einer Entfernung von mehreren Metern ausgelesen werden. Die International Organization for Standardization (ISO) hat für den Bereich der Transpondertechnologie mehrere Normen verabschiedet.[5] Die ISO-Standards legen Frequenzen,

Übertragungsgeschwindigkeiten, Protokolle und Kodierungen fest. Im Bereich der Zugangskontrolle und der sog. Smart Labels[6] ist beispielsweise die Norm ISO 14443 anzutreffen.

II. Einsatzgebiete für die Transpondertechnologie

Der Einsatz von RFID-Systemen eignet sich grundsätzlich überall dort, wo automatisch gekennzeichnet, erkannt, registriert, gelagert, überwacht oder transportiert werden muss.

1. Handel

Der Einsatz der Transpondertechnologie bietet sich insbesondere im Handel an.[7] Eines der wichtigsten Anwendungsgebiete von RFID-Systemen betrifft das „Supply Chain Management".[8] Einer Studie zufolge ergeben sich für den Handel insbesondere zwei Vorteile: Zum einen können die Bestände und damit die Lager- und Kapitalbindungskosten reduziert werden, zum anderen können Personalkosten eingespart werden.[9]

Aber auch im Endkundenbereich bieten sich für RFID viele Anwendungsfelder. Im Bereich Lagermanagement dient die RFID-Technologie dem Warenflusssystem, das identifiziert, welche Produkte sich im Lager befinden und welche in den Markt verräumt wurden. Mit Hilfe der Transponder entstehen aber auch „intelligente" Regale, die melden, wann ein mit einem RFID-Chip versehenes Produkt das Regal verlässt und wann neue Ware nachgeräumt werden muss. Auch den Kunden selbst erwarten einige Neuerungen. Auf den Tags können zusätzliche Informationen abgespeichert werden, die der Kunde durch ein Lesegerät am Einkaufswagen zur Kenntnis nehmen kann.[10] Dadurch erhält der Verbraucher weitere Produktinformationen und Empfehlungen zu anderen Waren, die zu dem gesuchten Produkt passen. Auch die Preise können elektronisch im Einkaufswagen erfasst werden, wodurch die bisherige manuelle Barcode-Erfassung entfällt.

RFID-Chips können auch i.V.m. Kundenkarten[11] verarbeitet werden und dienen hierbei ähnlich wie ein Magnetstreifen oder Barcode als Datenträger. Es können persönliche Daten auf dem Chip gespeichert werden oder auch nur die Kundennummer, die dann in einer Datenbank mit den dort gespeicherten Kundendaten verbunden wird.

2. Zugangskontrolle

Transponder werden auch im Bereich der Zugangskontrolle eingesetzt. Sie können als Ausweis für den Zutritt von Gebäuden oder Räumen verwendet werden. Auch Skipässe und Clubmitgliedskarten arbeiten mit der RFID-Technologie. Eine besondere Idee hatte der Baja Beach Club, ein Nachtclub in Barcelona: Besucher des Clubs können sich hier einen Mikrochip unter die Haut spritzen lassen und dann ihre Getränke über ein Kundenkonto bargeld- und kartenlos bezahlen.[12] Populäres Beispiel für den RFID-Einsatz sind auch die Tickets für die Fußball-WM 2006.[13]

3. Weitere Anwendungsbereiche

Auch Ausweise werden in Zukunft mit RFID-Tags ausgestattet. Ein aktuelles Beispiel hierfür ist die auf europäischen Vorgaben beruhende Einführung der neuen „ePässe".[14] Ab dem 1.11.2005 begann die Ausgabe der neuen biometriegestützten Reisepässe, die einen Mikrochip enthalten, auf dem zunächst ein digitales Foto gespeichert wird. Ab März 2007 werden dann zusätzlich in den neuen Pässen zwei Fingerabdrücke gespeichert.[15] Die neuen Pässe sollen die Fälschungssicherheit der Ausweisdokumente erhöhen und dadurch die organisierte Kriminalität

und den internationalen Terrorismus bekämpfen.

Seit mehreren Jahren haben sich RFID-Systeme bereits im Bereich der Wegfahrsperren von Kraftfahrzeugen bewährt.[16] Aber auch im Einzelhandel werden schon seit langem RFID-Lösungen zur Diebstahlsicherung eingesetzt. Diese 1-Bit-Systeme[17] werden in Sicherungsetiketten eingearbeitet und signalisieren dem jeweiligen Erfassungsgerät am Ausgang, ob ein Transponder vorhanden ist oder nicht. Daher müssen sie an der Kasse deaktiviert bzw. auf „null" gesetzt werden. Eine weitere praxisrelevante Anwendung der Transpondertechnologie ist die der Tierkennzeichnung.

Holznagel, Bonnekoh: Radio Frequency Identification - Innovation vs. Datenschutz? (MMR 2006, 17) 19

In der Nutztierhaltung werden mit Identifikationsdaten ausgestattete Transponder am Tier angebracht oder in das Tier injiziert. Die Vorteile liegen hier in der schnellen, automatisierten und elektronischen Identifizierung von Tieren, in der eindeutigen Kennzeichnung sowie in der lückenlosen Verfolgbarkeit der Tiere von der Geburt bis zum Verkauf des Fleischs. In einigen öffentlichen Verkehrsnetzen, wie z.B. in London, Helsinki und Peking, wird die RFID-Technologie ebenfalls bereits eingesetzt. Der Kunde bezahlt einfach durch Vorhalten seines aufladbaren Fahrscheins, was zu einer schnelleren Kundenabfertigung und Kostenersparnissen führt. Weitere Vorteile liegen in der automatischen Tarifberechnung, der einfachen Umstellung von Tarifen und in der Prävention von Schwarzfahrten.[18] Im Bereich der Luftfahrt kann die Transpondertechnologie bei Wartungsarbeiten und bei der Gepäckabfertigung eingesetzt werden.[19] Auch in der Arzneimittelindustrie und in Krankenhäusern finden RFID-Systeme Anwendung, um Medikamente leichter zu lokalisieren, Fälschungen und Verluste zu vermeiden bzw. festzustellen oder um die Identität eines Patienten und seine Behandlung feststellen und Verwechslungen vermeiden zu können.[20]

III. RFID und Datenschutz

In jüngster Zeit ist vermehrt über die datenschutzrechtlichen Auswirkungen des Einsatzes von RFID-Systemen diskutiert worden. Es stellt sich die Frage, ob das geltende Datenschutzrecht dazu in der Lage ist, die Belange der Betroffenen zu wahren, ohne Innovationspotenziale einzuschränken. Vorab kann festgestellt werden, dass nicht alle Verwendungsmöglichkeiten der gleichen juristischen Bewertung zugeführt werden können; es bedarf vielmehr einer differenzierten Betrachtung. Im Bereich geschlossener Logistikketten orientiert sich der Einsatz der Transpondertechnologie primär an reinen Kosten-Nutzen-Erwägungen. Auf Endverbraucherebene können sich hingegen durchaus Auswirkungen auf den Persönlichkeits- und Datenschutz ergeben. Die folgende datenschutzrechtliche Beurteilung beschränkt sich daher auf solche Bereiche, in denen Verbraucher mit RFID-Systemen in Berührung kommen.

1. Grundsätzliches

Das Bundesdatenschutzgesetz (BDSG) stellt den Grundbau des Datenschutzrechts dar und schützt den Einzelnen vor der Beeinträchtigung von Persönlichkeitsrechten, die durch den Umgang anderer mit seinen personenbezogenen Daten entstehen kann.[21] Personenbezogene Daten sind gem. § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person" („Betroffener"). Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nach dem in § 4 Abs. 1 BDSG niedergelegten Grundsatz des „Verbots mit Erlaubnisvorbehalt"[22] nur dann zulässig, wenn der

Betroffene eingewilligt hat oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Als Erlaubnistatbestände für das Erheben, Speichern, Übermitteln, Verändern und Nutzen personenbezogener Daten für eigene Zwecke kommen insbesondere die Erlaubnistatbestände des § 28 Abs. 1 Satz 1 Nr. 1 und Nr. 2 BDSG in Betracht. Danach ist der Datenumgang zulässig, wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient (Nr. 1) oder soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Nr. 2).

2. RFID im Endkundenbereich

a) RFID i.V.m. einer Kundenkarte

Kundenkarten werden i.R.e. Kundenbindungssystems durch die Unternehmen an die Verbraucher ausgegeben. Grundlage der Teilnahme an einem Kundenbindungssystem ist ein entsprechender Vertrag des Kunden mit dem Unternehmen.[23] In dem Vertrag verpflichtet sich das Unternehmen, gegenüber dem Kunden Rabatte zu gewähren oder bestimmte Serviceleistungen zu erbringen. Verbraucherschützer befürchten, dass Unternehmen in Zukunft mit RFID-Chips ausgestattete Kundenkarten ausgeben und zusätzliche Lesegeräte im Geschäft aufstellen, die z.B. Einkaufsbeginn und Einkaufsende erfassen könnten sowie Bereiche, die der Kunde bevorzugt aufsucht. So könnten theoretisch das Einkaufsverhalten der Verbraucher ausgeforscht und umfassende Bewegungsprofile erstellt werden.[24]

Der Unterschied bei der einzelnen Nutzung besteht im Vergleich zur bisherigen Kundenkarte darin, dass für die Nutzung kein konkreter Mitwirkungsakt des Kunden erforderlich ist. Bei der herkömmlichen Kundenkarte liegt die letztendliche Entscheidung der Nutzung beim Kunden, denn er kann an der Kasse entscheiden, ob er die Kundenkarte einsetzen möchte oder nicht. Die RFID-Technologie ermöglicht aber ein kontaktloses Auslesen der gespeicherten Daten, ohne dass der Kunde die Karte im Einzelfall vorlegen muss.

Einwilligung

Wird RFID i.V.m. einer Kundenkarte eingesetzt, auf der personenbezogene Daten gespeichert sind, so ist hierfür die Einwilligung, d. h. die vorherige Einverständniserklärung[25] des Kunden gem. § 4 Abs. 1 BDSG erforderlich.[26] Diese muss gem. § 4a Abs. 1 Satz 1 BDSG auf der freien

Entscheidung des Betroffenen beruhen und grundsätzlich schriftlich erfolgen (Satz 3).[27] In der Praxis wird die Einwilligung regelmäßig bei Unterzeichnung des Kundenkartenantrags erklärt werden. Die Einwilligungserklärung ist im Antrag besonders hervorzuheben.[28] Außerdem bedarf es gem. § 4a Abs. 1 Satz 2 BDSG eines Hinweises auf den Zweck der Speicherung.

Ausnahmetatbestand nach § 28 BDSG?

Eine Einwilligung wäre dann nicht erforderlich, wenn ein Ausnahmetatbestand nach § 28 BDSG vorläge. Für mit Funkchips ausgestattete Kundenkarten gelten prinzipiell die gleichen Grundsätze wie für herkömmliche Kundenkarten.[29] Bzgl. der Frage, ob eine Privilegierung nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG vorliegt, ist daher nach den jeweils betroffenen Daten und dem mit

der Erhebung verfolgten Zweck zu differenzieren.

Zweck: Abwicklung des Bonusprogramms

Werden Kundendaten zum Zweck der Abwicklung des Bonusprogramms[30] verwendet, so ist die Erhebung sog. Stammdaten[31] gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Es muss aber ein unmittelbarer sachlicher Zusammenhang zwischen der beabsichtigten Verwendung und dem konkreten Vertragszweck vorliegen.[32] Zur Identifizierung und Kontaktierung des Kunden ist die Kenntnis des Namens und der Anschrift erforderlich. Darüber hinaus sind keine weiteren Daten notwendig, sodass Daten wie Geburtstag und Telefonnummer nur mit entsprechender Einwilligung erhoben werden können.[33] In vielen Fällen werden durch die Unternehmen aber noch weitere Daten (sog. Programmdaten) erhoben. Bei jedem Einsatz der Kundenkarte werden die Kennung des Kunden, Ort und Zeit des Karteneinsatzes und der getätigte Umsatz gespeichert. Dies ist gem. § 28 Abs. 1 Satz 1 Nr. 1 BDSG nur zulässig, soweit es für die Rabattgewährung oder eine sonstige Serviceleistung erforderlich ist.

Zweck: Werbung und Marktforschung

Werden die bereits zulässigerweise zur Abwicklung des Bonusprogramms erhobenen Daten zu Werbungs- und Marktforschungszwecken benutzt, so liegt eine Zweckänderung vor. Diese ist gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG zulässig, wenn die Datenerhebung zur Wahrung berechtigter Interessen des Unternehmens erforderlich ist. Die Durchführung von Werbemaßnahmen und Marktanalysen wird von der h.M. als berechtigtes Interesse eines Unternehmens bewertet.[34] Die Datenerhebung ist jedoch dann nicht zulässig, wenn schutzwürdige Interessen des Betroffenen überwiegen. Es ist also eine Interessenabwägung vorzunehmen. Das Gesetz lehnt den Begriff der „schutzwürdigen Interessen" entsprechend seinem Schutzziel nach § 1 BDSG an Begriffe wie „Privat-, Intim-, oder Vertraulichkeitssphäre" an, die gleichzeitig Synonyme für das auf Art. 1, 2 GG beruhende „Recht auf informationelle Selbstbestimmung" darstellen.[35] Für die Stammdaten wie Name und Anschrift lässt sich feststellen, dass kein schutzwürdiges Interesse des Betroffenen der Verwendung der Daten entgegensteht. Der Kunde wird in der Regel davon ausgehen müssen, dass diese Daten zu Werbezwecken verwendet werden.[36] In Kombination mit einem RFID-Chip können aber auch weitere Informationen erlangt werden. Würden an Ein- und Ausgang Reader aufgestellt, so könnte festgehalten werden, wann ein bestimmter Kunde das jeweilige Geschäft betritt und wann er es verlässt. Die Erhebung dieser Daten würde der Bestimmung der Verweildauer des Kunden im Geschäft dienen, was keine Ausnahme von der Einwilligungspflicht gem. § 28 Abs. 1 Satz 1 Nr. 2 BDSG begründen würde, da ein schutzwürdiges Interesse des Unternehmens an dieser Information nicht ersichtlich ist.[37] Informationen über das Kaufverhalten eines Verbrauchers könnte das Unternehmen durch Lesegeräte erlangen, die in bestimmten Abteilungen platziert werden und so registrieren können, welche Bereiche des Geschäfts Kunde X bevorzugt aufsucht. Das Erstellen solcher umfassenden Bewegungsprofile begegnet durchgreifenden datenschutzrechtlichen Bedenken, da es sich hierbei um einen sehr intensiven Eingriff in die Privatsphäre des Kunden handelt.[38] An der Erlangung derartiger Daten besteht wiederum kein schützenswertes Interesse des Unternehmers, sodass zur Erhebung dieser Informationen ebenfalls die Einwilligung des Kunden erforderlich ist.

Zweck: Wirtschaftliches Interesse

Als weiterer Zweck der Datenerhebung kommen wirtschaftliche Interessen des Unternehmens in Betracht. Werden Lesegeräte an den Produktregalen angebracht, so könnte dadurch jede Warenentnahme registriert werden. Der Unternehmer wäre so jederzeit über den aktuellen Warenbestand in den Verkaufsregalen informiert und hätte die Möglichkeit, rechtzeitig Ware

nachzuräumen. Wird lediglich die Information der Produktentnahme erfasst, ohne dass ein Bezug zum jeweiligen Kunden hergestellt wird, so bestehen hier keinerlei datenschutzrechtliche Bedenken. Anders stellt sich die Sachlage jedoch dar, wenn über die Kundenkarte die Information mit persönlichen Daten verknüpft wird.[39] Bei der Beurteilung der Frage, ob ein berechtigtes Interesse an der Datenerhebung i.S.v. § 28 Abs.[nbsp] 1 Satz 1 Nr. 2 BDSG besteht, sind zwar auch rein wirtschaftliche Interessen des Unternehmers zu berücksichtigen.[40] Es ist jedoch eine Interessenabwägung vorzunehmen, die sich am konkreten Verarbeitungsprozess orientieren muss.[41] Zweifelsohne hat der betreffende Unternehmer ein wirtschaftliches Interesse an einem stets aktualisierten Warenbestand in seinen Verkaufsräumen. Um den

Produktbestand in den Regalen zu überprüfen, ist die Erhebung personenbezogener Daten des Kunden jedoch nicht erforderlich. Ein Ausnahmetatbestand vom Einwilligungsvorbehalt liegt daher nicht vor.[42]

Unterrichtungspflicht nach § 6c Abs. 1 BDSG

Gem. § 6c Abs. 1 BDSG bestehen für den Unternehmer bei der Verwendung von mobilen personenbezogenen Speicher- und Verarbeitungsmedien besondere Unterrichtungspflichten.[43] Unter solchen Medien sind Datenträger zu verstehen, auf denen personenbezogene Daten über die Speicherung hinaus durch die ausgebende oder eine andere Stelle automatisiert verarbeitet werden können und bei denen der Betroffene diese Verarbeitung nur durch den Gebrauch des Mediums beeinflussen kann.[44] Typischer Anwendungsfall sind sog. „Chipkarten",[45] also z.B. ec-Karten, Krankenversicherungskarten, SIM-Karten für die Nutzung von Mobilfunkdiensten, elektronische Tickets und auch zahlreiche Varianten der Kundenkarte.[46] Ist also eine Kundenkarte mit einem RFID-Chip ausgestattet, auf dem personenbezogene Daten gespeichert sind, so ist der Anwendungsbereich des § 6c Abs. 1 BDSG betroffen.[47] In diesem Fall muss der Unternehmer dem Kunden seine Identität und Anschrift mitteilen (Nr. 1) und ihn über die Funktionsweise des Mediums aufklären, wobei hier keine detaillierte technische Beschreibung erfolgen soll, sondern für den Laien verständliche Informationen zu erteilen sind.[48] Außerdem muss der Betroffene wissen, wie er seine Rechte auf Auskunft und Korrektur nach den §§ 19, 20, 34 und 35 BDSG im Hinblick auf die Besonderheiten des Mediums ausüben kann (Nr. 3).

b) „Getagte" Produkte

Kauft ein Kunde ein Produkt, das mit einem RFID-Tag versehen wurde, ohne dass eine Verknüpfung mit personenbezogenen Daten hergestellt wird, so stellt dies keine Erhebung bzw. Verarbeitung personenbezogener Daten dar. Probleme entstehen erst dann, wenn der Kunde in ein anderes Geschäft geht und dort die Tags ausgelesen werden. Es besteht nämlich keine Löschungspflicht des Unternehmers, der den Chip ursprünglich verwendet hat. Dieser ist nicht als verantwortliche Stelle i.S.d. § 3 Abs. 7 BDSG anzusehen, da er keine personenbezogenen Daten erhebt, nutzt oder verarbeitet.[49] Möchte ein Dritter die Tags auslesen und mit personenbezogenen Daten seines Kunden in Verbindung bringen, liegt eine einwilligungspflichtige Datenerhebung vor (§ 4 Abs. 1 BDSG). Daten- und Verbraucherschützer befürchten aber, dass diese erforderliche Einwilligung gerade nicht eingeholt wird und Tags unbefugt ausgelesen werden.[50] Deshalb wird eine Hinweispflicht für Unternehmen, die

RFID-Chips an ihren Produkten anbringen, gefordert und eine Deaktivierungsmöglichkeit für Kunden, die die auf dem Tag gespeicherten Informationen nach dem Produktkauf löschen wollen.[51]

Eine Unterrichtungspflicht nach § 6c Abs. 1 BDSG besteht nicht, da auf den Tags keine personenbezogenen Daten gespeichert sind. Außerdem sind nur solche Chips als mobile personenbezogene Speichermedien i.S.v. § 6c BDSG zu qualifizieren, auf denen über die Speicherung hinaus Daten automatisiert verarbeitet werden können.[52] Werden RFID-Tags im Einzelhandel eingesetzt, so handelt es sich dabei aber in der Regel um passive Tags, d.h. um solche, die keine Daten verarbeiten. Solche „dummen" Speichermedien sind von der Regelung nicht erfasst.[53] Ein Medium, das lediglich ein automatisiertes Auslesen von Informationen ermöglicht, erfüllt nicht die Voraussetzungen von § 3 Abs. 10 Nr. 2 BDSG.[54]

c) Exkurs: Die Fußball-WM als Überwachungs-Großprojekt?

Datenschutzrechtlich kritisiert wurde auch die Vergabe der Fußball-WM-Tickets. Da den rund 40 Mio. erwarteten Kaufinteressenten lediglich eine Mio. Karten im freien Verkauf zur Verfügung stehen, wurden die Tickets verlost. Das *Organisationskomitee Deutschland FIFA Fußball-Weltmeisterschaft Deutschland 2006* (kurz: *OK*) setzt auf die Personalisierung der WM-Tickets: In den Antragsformularen müssen die Interessenten Namen, Anschrift, Geburtsdatum, Nationalität und Personalausweisnummer angeben. Die Erhebung dieser Daten soll der Gewährleistung der Sicherheit und der Verhinderung des Schwarzhandels dienen.[55] Die Daten der Berechtigten werden in einer *DFB*-Datenbank gespeichert. Durch einen Abgleich mit Gewalttäter- und Hooligan-Dateien sollen gewaltbereite Personen von vornherein vom Ticketverkauf ausgeschlossen werden. Die Tickets selbst werden dann mit einem RFID-Chip ausgestattet, der eine eindeutige Zuordnung zu der jeweiligen berechtigten Person ermöglicht. Durch die Verwendung von RFID-Chips sollen die Tickets fälschungssicher gemacht werden. Die Zugangskontrolle erfolgt durch am Eingang positionierte Drehsperren, die über ein RFID-Lesegerät verfügen. Zusätzliche Ausweiskontrollen sollen stichprobenartig durchgeführt werden.

Es erscheint fraglich, ob die gewählte Vorgehensweise mit dem gem. § 3a BDSG geltenden Grundsatz der Datenvermeidung und -sparsamkeit vereinbar ist.[56] Danach haben sich Gestaltung und Auswahl von DV-Systemen an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben. Auf dem RFID-Chip selbst werden zwar keine personenbezogenen Daten, sondern Kennnummern gespeichert.[57] Zu beachten ist aber, dass die auf dem Chip gespeicherte Nummer durch ein Abrufen in der *DFB*-Datenbank einen Bezug zu den darin gespeicherten

personenbezogenen Daten herstellen kann. Dennoch liegt die datenschutzrechtliche Brisanz des WM-Ticket-Verkaufs wohl weniger speziell in der Verwendung von RFID-Systemen als vielmehr in der Art und Weise, wie der Verkauf im Vorfeld ausgestaltet wurde. Die Fülle der im Bestellformular verlangten Daten erscheint auch angesichts der verfolgten Zwecke nicht erforderlich. Auf Grund massiver Kritik von Verbraucher- und Datenschützern räumte der *DFB* den Verbrauchern einen Einwilligungsvorbehalt für die Verwendung der Daten zu Werbezwecken ein. Zunächst war lediglich ein Widerspruchsrecht vorgesehen.[58] Die Einwilligungserklärung wurde

jedoch zunächst so gefasst, dass der Besteller gleichzeitig in die Weitergabe seiner Daten für Werbezwecke einwilligt. Dieser Passus wurde mittlerweile aus dem Formular gestrichen.[59] Auch eine Klausel, wonach der Käufer der Verwendung seines Bilds bei Aufnahmen im Stadion „unwiderruflich" und „für alle gegenwärtigen und zukünftigen Medien" zustimmen sollte, ist mittlerweile abgeändert worden. Es darf also nicht verwundern, dass Verbraucher misstrauisch gegenüber neuen Technologien sind, wenn dabei personbezogene Daten verarbeitet werden. Die Vorgehensweise i.R.d. WM-Ticket-Verkaufs zeigt, dass Unternehmen mit Daten ihrer Kunden teilweise unachtsam umgehen.

IV. Aspekte der Datensicherheit

Es stellt sich die Frage, welchen technischen Sicherheitsrisiken die RFID-Technologie ausgesetzt ist. Bei der Speicherung von Daten auf einem Tag kann sich in mehrfacher Hinsicht eine spezifische Bedrohungslage ergeben.[60]

1. Angriffsmöglichkeiten

Eine der spezifischen Bedrohungslagen für RFID-Systeme besteht im Abhören der Kommunikation zwischen Transponder und Lesegerät. Dabei wird die Kommunikation über die Luftschnittstelle durch Auffangen und Dekodieren der Funksignale abgehört.[61] Die Kommunikation handelsüblicher Tags läuft größtenteils im 125 kHz- oder im 13,56 MHz-Bereich ab. Wird nun eine im ISO-Standard 14443 definierte Funkschnittstelle verwendet, so liegt diese im Kurzwellenband und kann mit handelsüblichen Breitband- oder Weltempfängern empfangen werden.[62]

Eine weitere Angriffsart besteht in der Fälschung des Inhalts oder der Identität eines Transponders.[63] Die Fälschung kann in mehrerer Hinsicht erfolgen: Im ersten Fall werden die auf dem Tag gespeicherten Daten durch einen unautorisierten Schreibzugriff verändert. Die Seriennummer bleibt dabei unverändert, sodass das Lesegerät die Identität des Transponders weiterhin korrekt erkennt. Im zweiten Fall bringt sich der Angreifer dagegen in den Besitz der Seriennummer und eventuell darüber hinausgehender Sicherheitsinformationen eines Tags und missbraucht diese zur Vortäuschung der entsprechenden Identität. Drittens könnte ein Tag physisch vom Trägerobjekt getrennt und mit einem anderen Objekt verbunden werden. Dies entspricht von der strafrechtlichen Einordnung her dem „Umkleben" von Preisschildern auf Waren.[64] Schließlich ist es möglich, dass ein Angreifer die Identität eines autorisierten Lesegeräts vortäuscht, um die Daten eines Tags mit seinem eigenen Lesegerät auslesen zu können.

Die Sicherheit von RFID-Systemen kann auch durch das Stören des Datenaustauschs beeinträchtigt werden. Die Störung des Datenaustauschs ist passiv durch Abschirmen oder aktiv, z.B. durch Benutzen eines Störsenders möglich. Schließlich können sich Angriffe auf das Backend[65] von RFID-Systemen beziehen. Auch hier besteht das Risiko des Abhörens. Ist das Backend mit dem Internet verbunden, so ergeben sich zusätzliche Gefahren durch Hacking und durch das Einbringen von Software-Anomalien wie Viren und Würmer. Allerdings handelt es sich hierbei nicht um RFID-spezifische, sondern um allgemeine IT-Sicherheitsrisiken, die mit den üblichen IT-Sicherheitsverfahren abgewehrt werden können.

2. Sicherheitsmaßnahmen

Ausgehend von den Angriffsarten bieten sich folgende Sicherheitsmaßnahmen an:

a) Authentifizierung

Um das Abhören der Kommunikation zu verhindern, können Authentifizierungsmechanismen in RFID-Systeme implementiert werden. Zur Überprüfung der Identität eines Lesegeräts kann z.B. ein Passwortschutz eingerichtet werden. Dabei identifiziert sich das Lesegerät gegenüber dem Tag durch Übertragung eines Passworts, das der Transponder mit dem gespeicherten Passwort vergleicht, und gestattet den Zugriff auf die gespeicherten Daten nur, wenn beide miteinander übereinstimmen.[66]

b) Verschlüsselung

Eine höhere Sicherheit gegen das Auslesen von Daten wird durch eine Verschlüsselung der Daten mittels des Hash-Lock-Verfahrens erreicht.[67] Vor dem erstmaligen Beschreiben eines Tags wird mithilfe einer Hash-Funktion aus einem Schlüssel eine sog. Meta-ID als Pseudonym für das Tag erzeugt und im Tag gespeichert, wodurch das Tag gesperrt wird („locked"). Auf die Signale eines Lesegeräts reagiert es dann nur noch mit dem Senden der Meta-ID. Erst wenn das Lesegerät in einer Backend-Datenbank den zur Meta-ID gehörenden Schlüssel abgerufen und zum Tag übertragen hat, wird dieses entsperrt, falls das Ergebnis der auf den Schlüssel angewandten Hash-Funktion mit der Meta-ID identisch ist.[68]

c) Verhinderung des Auslesens durch Blocker-Tags

Das unautorisierte Auslesen von auf Transpondern gespeicherten Daten kann durch den Einsatz sog. Blocker-Tags erreicht werden. Ein Blocker-Tag ist ein Transponder, der

sämtliche Anfragen eines Lesegeräts positiv beantwortet und dieses dadurch derart verwirrt, dass das eindeutige Identifizieren eines bestimmten Tags unmöglich gemacht wird.[69] Ein Kunde könnte ein solches Blocker-Tag in seinem Einkaufsbeutel mit sich führen und so verhindern, dass die von ihm gekauften Produkte von Dritten erkannt werden können. Unerwünschter Nebeneffekt kann jedoch die ungewollte Störung anderer RFID-Anwendungen in der Umgebung sein. Außerdem wird die Verlässlichkeit von Blocker-Tags als eher gering eingeschätzt.

d) Deaktivierung durch „Kill"-Befehl

Um auf Konsumgütern angebrachte Tags zu deaktivieren, kann durch einen sog. Kill-Befehl die Seriennummer derart anonymisiert werden, dass diese nicht mehr ausgelesen werden kann. Dieses Vorgehen birgt jedoch einige Nachteile in sich. Zum einen ist derzeit technisch nur die Deaktivierung eines einzelnen Transponders möglich, sodass jedes gekaufte Produkt einzeln behandelt werden muss. Ob die Kunden einen solchen Aufwand auf sich nehmen wollen, erscheint zweifelhaft.[70] Unpraktikabel ist der Einsatz des Kill-Befehls auch vor dem Hintergrund, dass der Kunde den Vorgang der Deaktivierung nicht überprüfen kann. Ihm müsste daher außerdem ein Lesegerät zur Verfügung gestellt werden, mit dem er das jeweilige Tag selbst auslesen und so die Deaktivierung kontrollieren kann. Schließlich führt die Deaktivierung dazu, dass auch positive Nutzungsmöglichkeiten, etwa die Verwendung von Daten bei Umtausch, Reparatur, Weiterverkauf oder Recycling, verloren gehen.

V. Ausblick

Die neue Art des kontaktlosen Datentransfers durch RFID-Systeme bringt neue

Herausforderungen für die Sicherheit der Datenübertragung und den Datenschutz mit sich. Für die Zukunft zeichnet sich eine flächendeckende Verbreitung der neuen Technologie ab, sodass eine klare rechtliche Einordnung unerlässlich ist. Dabei lässt sich feststellen, dass sämtliche Varianten der Transpondertechnologie durch das geltende Datenschutzrecht erfasst werden. Innerhalb des BDSG sind keine Gesetzeslücken ersichtlich. Die Transpondertechnologie kann letztlich aber nur dann Erfolg haben, wenn sie auch von den Verbrauchern angenommen wird. Bei den Konsumenten ist jedoch eine große Verunsicherung zu beobachten. Die Studie einer Unternehmensberatung ergab, dass 55% der Befragten denken, dass RFID-Tags an gekauften Produkten der Überwachung ihres Konsumverhaltens dienen könnten.[71] Auch Aspekte der Datensicherheit spielen bei den Verbraucherängsten eine große Rolle. So glauben 59% der Verbraucher, dass die über die Funkchips gewonnenen Daten von Dritten missbraucht werden könnten. Die große Mehrheit der Befragten begrüßt den Einsatz der Technik jedoch, wenn es z.B. darum geht, den Diebstahl von Fahrzeugen zu verhindern, gestohlene Waren schneller wieder aufzufinden oder Sicherheitsmaßnahmen für verschreibungspflichtige Medikamente zu verbessern. Die Akzeptanz kann nur durch größtmögliche Transparenz und Konsumentenaufklärung beim Einsatz von RFID-Chips gesteigert werden. Deshalb sollten Produkte, die mit Tags versehen sind, entsprechend gekennzeichnet werden, auch wenn darauf keine personenbezogenen Daten gespeichert sind. Außerdem sollten Kunden die Möglichkeit haben, Transponder nach dem Einkauf zu deaktivieren. Schließlich sind ausreichende Sicherheitsmaßnahmen zu ergreifen, damit die Verbraucher keine Zugriffe Dritter befürchten müssen. Sollten die Unternehmen diesen Anforderungen Rechnung tragen, so könnten RFID-Systeme schon bald in nahezu allen Alltagsbereichen den herkömmlichen Barcode ersetzen.

---

* Professor Dr. Bernd Holznagel ist Direktor der öffentlich-rechtlichen Abt. des Instituts für Informations-, Telekommunikatons- und Medienrecht (ITM), Universität Münster. Mareike Bonnekoh ist wissenschaftliche Mitarbeiterin am ITM.

1 *Finkenzeller*, RFID-Handbuch, Grundlagen und Praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten, 3. Aufl. 2003, S. 6 f. Zur technischen Funktionsweise von RFID vgl. auch die Beiträge aus *Eberspächer*/*von Reden* (Hrsg.), Umhegt oder abhängig?, 2006.

2 *Wikipedia*, Freie Enzyklopädie, Stichwort: Radio Frequency Identification, abrufbar unter: http://de.wikipedia.org/wiki/Rfid [Stand: 29.11.2005].

3 Zu den einzelnen Frequenzbereichen wird auf die umfassenden Ausführungen der Studie des *Bundesamtes für Sicherheit in der Informationstechnik* (*BSI*): Risiken und Chancen des Einsatzes von RFID-Systemen, 2004, S. 28 ff. verwiesen.

4 Dieser Frequenzbereich wird z.B. für Straßenmaut-Systeme wie Toll Collect genutzt.

5 Dazu zählen insb. die Normen ISO 10536 (Close Coupling), ISO 14443 (Proximity Coupling), ISO 15693 (Vicinity Coupling) und ISO 18092 (Near Field Communication).

6 Unter Smart Labels versteht man die auf Produkten und Kundenkarten angebrachten Miniatur-Transponder.

7 So wird RFID z.B. im METRO Future Store auf seine Praxistauglichkeit getestet. Die METRO Group Future Store Initiative ist eine Kooperation der *METRO Group* mit *SAP*, *Intel*, *IBM* und *T-Systems* sowie weiteren Partnerunternehmen und bildet das Pilotprojekt für Supermärkte mit einem Bündel von technologischen Neuerungen, insb. dem Einsatz der RFID-Technologie. Weitere Informationen hierzu unter: http://www.future-store.org [Stand: 29.11.2005].

8 Mit Supply Chain ist ein Netzwerk verschiedener Unternehmen gemeint, die ihre Arbeitsabläufe so aufeinander abstimmen, dass die Steuerung und Überwachung der Lieferkette eines Produkts vom Hersteller bis zum Endkunden optimiert wird.

9 *A. T. Kearny*, RFID spart dem deutschen Einzelhandel sechs Milliarden Euro pro Jahr. Nutzen für Händler - Kosten für Hersteller, PM v. 8.3.2004, abrufbar über die Homepage der Unternehmensberatung: http:// www.atkearny.de [Stand: 29.11.2005].

10 *Roßnagel*/*Müller*, CR 2004, 625, 626 f.

11 Auf der im METRO Future Store verwendeten Kundenkarte, sog. „Future Card", war zunächst die jeweilige Kundennummer gespeichert, die dann über eine Datenbank mit den jeweiligen Kundendaten verknüpft werden konnte. Seit Anfang letzten Jahres werden Kundenkarten mit integriertem RFID-Chip im Rahmen dieses Projekts jedoch nicht mehr eingesetzt.

12 Börse unter der Haut, Der Spiegel 23/2004, S. 156.

13 Zur rechtlichen Bewertung sogleich unter III.2.c).

14 ePass steht für „elektronischer Pass". Die Einführung des ePasses geschieht auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates v. 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten, ABl. EG Nr. L 385 v. 29.12.2004, S. 1.

15 Vgl. hierzu die ausführlichen Informationen des *BMI*, abrufbar unter: http://www.bmi.bund.de (Thema: Informationsgesellschaft) [Stand: 29.11. 2005].

16 *BSI*-Studie (o. Fußn. 3), S. 81.

17 Diese Sicherungsetiketten werden auch als EAS-Systeme bezeichnet (Electronic Article Surveillance).

18 *Finkenzeller* (o. Fußn. 1), S. 358.

19 Vgl. http://www.heise.de/newsticker/meldung/56099 [Stand: 29.11. 2005].

20 Die amerikanische Gesundheitsbehörde hat sogar eine Genehmigung für den Einsatz von RFID-Transpondern im menschlichen Körper erteilt: Der sog. „VeriChip" wird unter die Haut

injiziert oder eingepflanzt und soll Ärzten bei Notfällen Auskunft über die Krankengeschichte des Patienten geben, *Department of Health and Human Services, Food and Drug Administration*, 21 CFR Part 880, Docket No. 2004N-0477, veröffentlicht im Federal Register/Vol. 69, No. 237/10. December 2004/Rules and Regulations.

21 Vgl. § 1 Abs. 1 BDSG.

22 *Gola*/*Schomerus*, BDSG, Bundesdatenschutzgesetz, Komm., 8. Aufl. 2005, § 4 Rdnr. 3; *Globig*, in: Roßnagel, Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, 2003, 4.7 Rdnr. 6; *Sokol*, in: Simitis, Komm. zum Bundesdatenschutzgesetz, 5. Aufl. 2003, § 4 Rdnr. 3.

23 In der Regel beantragt der Kunde die Teilnahme durch Ausfüllen eines Formulars des Unternehmens. Durch die Annahme des Antrags kommt der Vertrag dann zu Stande. Vgl. hierzu das Gutachten des *Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein* (*ULD*), Kundenbindungssysteme und Datenschutz, 2003, S. 69; abrufbar unter: http://www.datenschutzzentrum.de/wirtschaft/kundenbindungssysteme.pdf [Stand: 29.11.2005].

24 *Roßnagel*/*Müller*, CR 2004, 625, 628. Zu den datenschutzrechtlichen Bedenken vgl. auch *Tangens*, RFID in der Kritik, in: Eberspächer/von Reden (o. Fußn. 1), S. 93 ff.

25 *Gola*/*Schomerus*, BDSG (o. Fußn. 22), § 4 Rdnr. 15.

26 *Gräfin von Westerholt*/*Döring*, CR 2004, 710, 712.

27 Eine Einwilligungserklärung, die der Schriftform nicht genügt, ist in entsprechender Anwendung der §§ 125, 126 BGB unwirksam und führt zur Unzulässigkeit der darauf beruhenden Datenverarbeitung, vgl. *Gola*/*Schomerus*, BDSG (o. Fußn. 22), § 4a Rdnr. 13.

28 Vgl. § 4a Abs. 1 Satz 4 BDSG.

29 Zur datenschutzrechtlichen Bewertung von Kundenbindungssystemen vgl. das Gutachten des *ULD* (o. Fußn. 23).

30 Unter Bonusprogramm sind die Rabattaktionen oder sonstigen Serviceleistungen zu verstehen, die den Verbrauchern vom Unternehmen i. R. d. Kundenbindungssystems gewährt werden.

31 Hierbei handelt es sich in der Regel um den vollständigen Namen, die Anschrift und in einigen Fällen auch um weitere Angaben wie das Geburtsdatum, die Telefonnummer und die E-Mail-Adresse.

32 *Simitis*, in: Simitis (o. Fußn. 22), § 28 Rdnr. 79; *Bergmann*/*Möhrle*/*Herb*, Datenschutzrecht, Komm., 2005, Bd. 1, § 28 Rdnr. 26.

33 Gutachten des *ULD* (o. Fußn. 23) S. 70 f.

34 *Simitis* (o. Fußn. 32), § 28 Rdnr. 137; *Schaffland*/*Wiltfang*, BDSG, Komm., 2005, § 28 Rdnr. 85.

35 *Gola*/*Schomerus* (o. Fußn. 22), § 28 Rdnr. 35.

36 Gutachten des *ULD* (o. Fußn. 23) S. 72.

37 Auch eine Ausnahme nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG läge nicht vor, da die erhobenen Daten weder der Abwicklung des potenziellen Kaufvertrags noch der Abwicklung des Bonus-/Serviceprogramms dienen würden.

38 Das Erstellen von Persönlichkeitsprofilen, d.h. die langfristige Speicherung von Daten aus unterschiedlichen Lebensbereichen ist unzulässig, da es gegen das Menschenbild des GG verstößt und somit verfassungswidrig ist; vgl. *BVerfG* NJW 1969, 1707; *BVerfG* NJW 1984, 424; allg. zu dieser Thematik: *Weichert*, in: Kilian/Heussen, Computerrechts-Handbuch, 2005, Teil 13, Nr. 130, Rdnr. 35 f.

39 *Gräfin von Westerholt*/*Döring*, CR 2004, 710, 712.

40 *Simitis* (o. Fn. 32), § 28 Rdnr. 139.

41 *Schaffland*/*Wiltfang* (o. Fußn. 34), § 28 Rdnr. 89.

42 Ebenso *Gräfin von Westerholt*/*Döring*, CR 2004, 710, 712.

43 Diese 2001 in das BDSG aufgenommene Informationspflicht soll einen weiteren Schritt des neuen BDSG zu mehr Transparenz für den Betroffenen bewirken, vgl. *Gola*/*Schomerus* (o. Fußn. 22), § 6c Rdnr. 6.

44 So die gesetzliche Legaldefinition, vgl. § 3 Abs. 10 BDSG.

45 S. hierzu ausf. *Weichert*, in: Roßnagel (o. Fußn. 22), S. 1948 ff.; *ders.*, DuD 1997, 266 ff.

46 *Bizer*, in: Simitis (o. Fußn. 22), § 6c Rdnr. 6 f.

47 So auch *Gräfin von Westerholt*/*Döring*, CR 2004, 710, 714.

48 *Gola*/*Schomerus* (o. Fußn. 22), § 6c Rdnr. 6.

49 *Gräfin von Westerholt*/*Döring*, CR 2004, 710, 715.

50 Dies ist jedoch eher als ein Problem der Datensicherheit einzustufen, dazu unter IV.

51 Arbeitspapier der *Artikel-29-Datenschutzgruppe* „Datenschutzfragen im Zusammenhang mit der RFID-Technik", 10107/05/DE, WP 105 v. 19.1.2005, abrufbar unter: www.europa.eu.int/comm/privacy [Stand: 29.11.2005]; Entschließung der *Internationalen*

Konferenz der Beauftragen für den Datenschutz und den Schutz der Privatsphäre „Entschließung zu Radio-Frequency Identification" v. 20.11. 2003, abrufbar unter: http://www.datenschutz-berlin.de/doc/de/konf/67/radio-frequency.htm [Stand: 29.11.2005]; vgl. auch das Positionspapier des *FoeBuD e.V.* über den Gebrauch von RFID auf und in Konsumgütern, http://www.foebud.org/rfid/positionspapier [Stand: 29.11.2005].

52 § 3 Abs. 10 BDSG.

53 So die Gesetzesbegründung, BT-Drs. 14/5793, S. 60.

54 *Bizer* (o. Fußn. 46) § 3 Rdnr. 277.

55 So die Erläuterungen zum Datenschutz auf der *FIFA*-Homepage, abrufbar unter: http://fifaworldcup.yahoo.com [Stand: 29.11.2005].

56 *Weichert* sieht in der Personalisierung der WM-Tickets ein Großprojekt zur Förderung der RFID-Technologie im Konsumentenbereich; *Weichert*, Die Fußball-WM als Überwachungs-Großprojekt, 2005, S. 1, abrufbar unter: http://www.datenschutzzentrum.de/allgemein/wmticket.htm [Stand: 29.11.2005].

57 Krit. dazu *Weichert* (o. Fußn. 56), S. 5, der die Darstellung des *DFB* in den Datenschutzbestimmungen als irreführend betrachtet.

58 *Schüler*, c't 4/2005, 38.

59 S. http://www.heise.de/newsticker/meldung/56548 [Stand: 29.11.2005].

60 Zu den unterschiedlichen Bedrohungslagen umfassend Kap. 7 der *BSI*-Studie (o. Fußn. 3), wobei hier die verschiedenen Angriffsarten auch nach den unterschiedlichen Bedrohungslagen der aktiven (Betreiber der RFID-Systeme) und der passiven Partei (insb. Kunden und Arbeitnehmer) differenziert werden.

61 *BSI*-Studie (o. Fußn. 3), S. 42.

62 *Finke*/*Kelter*, Radio Frequency Identification - Abhörmöglichkeiten der Kommunikation zwischen Lesegerät und Transponder am Beispiel eines ISO 14443-Systems, abrufbar unter: www.bsi.de [Stand: 29.11.2005]. Das dort beschriebene Experiment ergab, dass ein passives Abhören der Kommunikation von RFID-Systemen nach ISO 14443 bis zu mehreren Metern und damit weit über den spezifischen Arbeitsbereich von 10-15 cm hinaus möglich ist.

63 *BSI*-Studie (o. Fußn. 3), S. 42.

64 Zur strafrechtlichen Bewertung des Umklebens von Preisetiketten vgl. z.B. *Tröndle*, in: Leipziger Komm., § 267 Rdnr. 147 f.

65 Unter Backend versteht man die Datenbestände, mit denen die vom Lesegerät erfassten

Daten über weitere Kommunikationskanäle verknüpft werden.

66 *BSI*-Studie (o. Fußn. 3), S. 48.

67 Hierzu *BSI*-Studie (Fußn. 3), S. 48 f.; zu den technischen Grundlagen s.a. *Holznagel*, Recht der IT-Sicherheit, 2003, S. 50 ff.

68 *Weis*, Security and Privacy in Radio-Frequency Identification Devices, 2003, S. 38 f.; *Weis*/*Sarma*/*Rivest*/*Engels*, Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems, 2003, S. 7.

69 *BSI*-Studie (o. Fußn. 3), S. 53 f.

70 So auch *Langheinrich*, Die Privatsphäre im Ubiquitous Computing - Datenschutzaspekte der RFID-Technologie, 2004, S. 14.

71 So die im März 2005 veröffentliche Studie von *Capgemini*. Befragt wurden 2.000 Personen im Alter über 18 Jahren aus Deutschland, Frankreich, Großbritannien und den Niederlanden. Die Studie ist abrufbar unter: http://www.de.capgemini.com/servlet/PB/show/1567889/Capgemini_European_RFID_report.pdf [Stand: 29.11.2005].