Effizienzsteigerungspotentiale durch den Einsatz von RFID-Systemen im Gesundheitswesen und in der Pharmazeutischen Industrie

Heinrich Hanika

1 Ausgangssituation

Mit dem Begriff „Revolution“ sollte man zurückhaltend und behutsam umgehen. Bei der Entwicklung des Technik-Zukunftsbildes „Pervasive Computing“ bzw. „Ubiquitous Computing“ ist es allerdings angemessen, von einer revolutionären Technikperspektive zu sprechen.

Das Technikleitbild „Pervasive Computing“ bezeichnet eine neue Entwicklung in der Informations- und Kommunikationstechnologie. „Pervasive“ steht für „(alles) durchdringend“, „ubiquitous“ für „allgegenwärtig“. Im Zuge dieser Entwicklung werden zukünftig auch immer mehr Alltagsgegenstände mit Mikroelektronik ausgestattet sein. Die so entstehenden „intelligenten“ Objekte, auch „Smart Objects“ genannt, werden nahezu alle Bereiche des täglichen Lebens beeinflussen. Computer werden ihre Dienste zunehmend unsichtbar im Hintergrund ausführen.

Einen wesentlichen Entwicklungsstrang im Rahmen des Pervasive Computing bilden digitale automatische Identifikationssysteme (Auto-ID-Systeme), die traditionelle Lösungen wie Barcode oder Optical Character Recognition (OCR) zukünftig ersetzen sollen. Aufgabe und Ziel der Auto-ID-Tenologie ist grundsätzlich die Bereitstellung von Informationen zu Objekten (Personen, Tieren, Gütern oder Waren). RFID-Systeme (Radio-Frequency-Identification) erweitern die Funktionalitäten und Einsatzmöglichkeiten traditioneller Auto-ID-Systeme und bieten hohe Effizienzsteigerungspotentiale.[1]

Obwohl Radio Frequency Identification (RFID) bereits vor etwa 60 Jahren zum ersten Mal eingesetzt wurde, ist die Technologie erst in den letzten Jahren stärker in den Focus der Öffentlichkeit gerückt. Insbesondere die informations- und telekommunikationstechnologische Entwicklung sowie die zunehmende Standardisierung haben sichtlich zur Verbreiterung innovativer Einsatzszenarien der Funktechnologie beigetragen.[2]

Während Logistiker und Produktionsunternehmen bereits seit vielen Jahren RFID-Einsätze erproben und bereits von fundierten Erfahrungen profitieren, hat das Gesundheitswesen die Funktechnologie nunmehr für sich entdeckt. Marktforscher sagen dem Segment dennoch ein stolzes Wachstum voraus. So prognostiziert z. B. die Studie „RFID in Healthcare 2006–2016“ von IDTechEx dem Markt bis 2016 ein Volumen von 2,1 Mrd. US-Dollar. Hauptmotoren für das Wachstum seien Medikamentenkontrollen sowie die Echtzeitüberwachung von Mitarbeitern, Patienten und Material.[3]

Aktuell sind auch im Gesundheitswesen und in der pharmazeutischen Industrie strukturelle Veränderungen zu beobachten, die den Einsatz der elektronischen Identifikation befördern. Hierzu zählt beispielsweise die Kennzeichnung medizinischer Produkte wie Blutplasma oder Proben.

Die RFID-Technologie soll in diesem Anwendungssegment dazu beitragen, die Kosten zu senken und Personal einzusparen sowie gleichzeitig die Qualitätsstandards zu wahren und Serviceleistungen zu verbessern.

Zu den betriebswirtschaftlichen Vorteilen der elektronischen Identifikation im Gesundheitswesen zählt zum einen die Zeitersparnis: Transponder in den Kitteltaschen von Ärzten und Pflegepersonal können die Benutzer automatisch und somit Zeit sparend authentifizieren.

Zum anderen kommen Kostensenkungspotenziale hinzu. Die Inventarisierung von Geräten und Materialien kann über die Ausstattung mit Transpondern zuverlässig und Zeit sparend erfolgen. Die direkte Folge ist eine Reduktion der im Bestellwesen und bei der Geräteüberwachung anfallenden Kosten.

Darüber hinaus werden Kennzeichnungssysteme zur Gewährleistung der Qualität von medizinischen Produkten erprobt. So zeichnen beispielsweise an Blutbeuteln angebrachte aktive Transponder eventuelle Temperaturabweichungen auf und beugen einer Schädigung des Patienten durch die Verabreichung verfallener Blutprodukte vor.[4]

Radio Frequency Identification (RFID) findet bereits seit 20 Jahren alltägliche Anwendung, so etwa bei der Mauterhebung, in Wegfahrsperren, Diebstahlsicherungen in Kaufhäusern oder Zugangskontrollen an Skiliften. Sie erfährt aktuell einen großen Schub durch neue praxisnahe Entwicklungen, die weitere Anwendungsfelder im Bereich der AutoID-Technik (Automatische Identifikationstechnik) erschließen. Vor allem durch den kontinuierlichen informationstechnologischen Fortschritt werden Anwendungen nunmehr auch im Gesundheitswesen und in der pharmazeutischen Industrie geschaffen, die vor wenigen Jahren noch nicht denkbar waren. Die fortschreitende Standardisierung eröffnet weitere Einsatzmöglichkeiten.

In den vergangenen Jahren ist die Erkenntnis gewachsen, dass die Bewertung technischer Entwicklungen vorausschauend und problemorientiert erfolgen sollte, um Hinweise für eine zukunftsfähige Technikgestaltung zu gewinnen. Hierzu zählt auch die interdisziplinäre Abschätzung der Chancen und Risiken des Einsatzes von RFID mit fokussiertem Blick auf die Bereiche IT-Sicherheit und Datenschutz. Nur so können echte oder vermeintliche Sicherheitsprobleme als zentrale Barriere der wirtschaftlichen Nutzung der RFID-

Autor: Heinrich Hanika
Titel: Effizienzsteigerungspotentiale durch den Einsatz von RFID-Systemen im Gesundheitswesen und in der Pharmazeutischen Industrie
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Bad Nauheim, Ausgabe 2009
Seite: 281-289

Technologie frühzeitig erkannt und so weit als möglich auch vermieden werden.[5]

2 Grundlagen der RFID-Technologie

RFID stellt die Abkürzung für „Radiofrequenz-Identifikation“ dar und bezeichnet Verfahren zur automatischen und kontaktlosen Identifizierung von Objekten per Funk. RFID-Systeme können sich zu einer Schlüsseltechnologie der Zukunft gerade auch im Gesundheitswesen entwickeln und werden schon heute in vielen Bereichen, insbesondere im Logistikbereich und der Lagerbewirtschaftung, erfolgreich eingesetzt. Die Datenübertragung erfolgt durch magnetische oder elektromagnetische Felder.[6] RFID-Systeme bestehen aus zwei technologischen Komponenten: einem Transponder[7] und einem Lesegerät. Die Vorteile der RFID-Technologien liegen in der Möglichkeit, kontaktlos und ohne optische Verbindung Daten zu übertragen, in der Leseschnelligkeit von weniger als 100 Millisekunden[8] und in der Langlebigkeit der Mikrochips. Außerdem sind RFID-Systeme nahezu wartungsfrei[9]

2.1 Technologische Komponenten von RFID-Systemen

Jedes RFID-System besteht aus zwei technologischen Komponenten, einem Transponder („Tag“) und einem Lesegerät („Reader“). Der Transponder beinhaltet einen elektronischen Mikrochip und eine Antenne zum Empfangen und Senden von Funkwellen.[10] Der Transponder wird in ein Trägerobjekt integriert, z. B. in eine Chipkarte oder ein Klebeetikett. Auf dem Tag werden Informationen, wie beispielsweise ein Nummerncode, gespeichert. Um diese gespeicherten Daten erfassen zu können sind spezifische Lesegeräte erforderlich. Der Reader setzt sich aus einem Sender, einem Empfänger und einer Antenne zusammen. Zudem 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. Dieser sendet dann seine gespeicherten Daten an das Lesegerät, wo sie erfasst und gespeichert werden.[11]

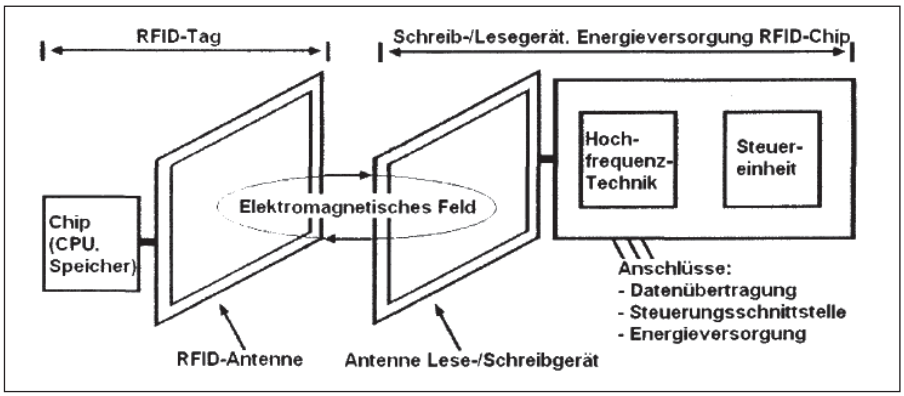

Abbildung 1: *Abbildung 1: Radiofrequenz-Identifikation (RFID) (Quelle: Schaar[12] vom 19.04.2007)*

Es gibt aktive und passive Transponder. Die aktiven Transponder besitzen mit Batterien eine eigene Energiequelle, mit der sie elektromagnetische Wellen auslösen. Sie bleiben solange im Ruhezustand, bis sie von einem Lesegerät durch ein Signal angesprochen werden. Passive Transponder besitzen keine eigene Energiequelle. Wenn sie in das Feld eines Lesegerätes gelangen, werden sie zum Auslesen der Daten vom Lesegerät über Funkwellen mit Energie versorgt (induktive Koppelung).

Mit aktiven Transpondern lassen sich Daten über größere Distanzen mit dem Lesegerät austauschen. Diesem Vorteil stehen allerdings Nachteile in der Anwendungspraxis gegenüber. Aktive Transponder haben durch den eigenen Energieträger nur eine begrenzte Lebensdauer, ein größeres Gewicht und einen höheren Preis. Da der Einsatz passiver Transponder nicht von der Lebensdauer der Batterien begrenzt wird, können sie dauerhaft eingesetzt werden. Darüber hinaus sind sie kostengünstiger, kleiner und leichter, haben jedoch eine geringere Reichweite. Immer dann, wenn die spezifischen Eigenschaften der passiven Transponder für den Anwendungszweck ausreichen, sind sie den aktiven vorzuziehen.[13]

Ein weiteres Unterscheidungsmerkmal sind die Speichereigenschaften. Auf Read-only-Transpondern werden bereits bei der Produktion die zur Objektidentifizierung erforderlichen Daten gespeichert. Die Daten können nicht mehr verändert oder gelöscht, sondern nur ausgelesen werden. Auf Read-write-Transponder gespeicherte Daten können bei Bedarf geändert, durch neue Informationen ersetzt oder gelöscht werden. Die aufwendigere Speichertechnologie bedingt zwar höhere Produktionskosten, dafür können sie flexibler eingesetzt werden.

Pulkerfassung ist immer dann relevant, wenn eine große Zahl von Transpondern gleichzeitig das Lesefeld durchläuft. Mit bestimmten Algorithmen werden die ID-Nummern der einzelnen Transponder ausgelesen, bis die Transponder einzeln angesprochen und eindeutig erfasst werden können. Sind Systeme nicht pulkfähig, überlagern sich die Transpondersignale und das Lesegerät ist nicht in der Lage, sie zu identifizieren.

RFID-Systeme werden mit unterschiedlichen Arbeitsfrequenzen angeboten. Diese Frequenzen bringen unterschiedliche technische Eigenschaften und somit unterschiedliche Fähigkeiten mit sich. Vor allem im Hinblick auf Reichweiten und die Störanfälligkeit gegenüber Flüssigkeiten und Metallen in der Arbeitsumgebung lassen sich Unterschiede ausmachen, so dass eine individuelle Materialprüfung bezogen auf die jeweilige Anwendung unerlässlich ist.

Die Tabelle liefert einen Überblick über verschiedene RFID-Systeme:[14]

3 Standardisierung

Eine wesentliche Voraussetzung für eine weite Verbreitung von RFID ist die Entwicklung und Anwendung einheitlicher und unternehmensübergreifender Standards. Man unterscheidet zwischen Technologie, Daten- und Anwendungsstandards.

Technologiestandards definieren grundlegende technische Eigenschaften wie Frequenzen, Übertragungsgeschwindigkeiten, Codierungen und Protokolle. Datenstan-

RFID-Systeme	Niederfrequenz	Hochfrequenz	Ultrahochfrequenz	Mikrowelle
Frequenz	125 kHz - 135 kHz	13,56 MHz	860 MHz - 960 MHz	2,45 GHz
Energieversorgung	passiv	passiv	aktiv oder passiv	aktiv oder passiv
Speicherkapazität	bis 2 kBit	bis 2 kBit	bis 256 kBit (aktiv)	bis 256 kBit (aktiv)
Reichweite	bis 1 m	bis 1,7 m	bis 6 m (passiv), bis 100 m (aktiv)	bis 6 m (passiv), bis 100 m (aktiv)
Pulkerfassung	ja, selten realisiert	ja	ja	ja
Störung durch Flüssigkeiten	nein	gering	stark	stark
Störung durch Metall	bedingt	Bei direkter Aufbringung keine Lesefähigkeit, mit Abstand bedingt	Bei direkter Aufbringung keine Lesefähigkeit, mit Abstand bedingt	Bei direkter Aufbringung keine Lesefähigkeit, mit Abstand bedingt

Tabelle 1: *Verschiedene RFID-Systeme*
(Quelle: Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, RFID Geschäftsprozesse mit Funktechnologie unterstützen, 2006, S. 8.)

dards sind unabhängig von der Technologie und dienen der Datenorganisation. In nachfolgender Tabelle 2 sind relevante Standards aufgelistet, und als Beispiel für die Bedeutung eines Datenstandards kann der im September 2004 beschlossene Standard ISO/IEC 15963 genannt werden. Mit ihm wird das Schema festgelegt, wie eindeutige ID-Nummern für Transponder realisiert werden können. Die Eindeutigkeit der Nummern ist nur erreichbar, wenn sie von allen teilnehmenden Unternehmen nach dem gleichen Schema vergeben werden. Anwendungsstandards schließlich dienen dazu, für einzelne Anwendungsfelder die am besten geeignete technische Lösung zu empfehlen.[15]

ISO/IEC 19762 Information Technology - Harmonized Vocabulary
ISO/IEC 7816-6 Registration of Electronic Manufacturers for RFID tags
ISO/IEC 15418 Automatic Identification - International Specification - EAN.UCC Applications Identifiers and ASC Data Identifiers
ISO/IEC 15434 Automatic Identification and Data Capture Techniques - International Specification - Syntax for high-capacity data carriers
ISO/IEC 15459 Automatic Identification and Data Capture Techniques - International Specification - unique identifier for item management
ISO/IEC 15961 Automatic identification - Radio-Frequency Identification for item management - Data protocol: application interface
ISO/IEC 15962 Automatic identification - Radio-Frequency Identification for item management - Data protocol: data encoding rules and logical memory functions
ISO/IEC 15963 Automatic identification - Radio-Frequency Identification for item management - Unique identification for RF tags
ISO/IEC 18000-2 Automatic identification - Radio-Frequency Identification for item management - Air interface protocol 135 kHz
ISO/IEC 18000-3 Automatic identification - Radio-Frequency Identification for item management - Air interface protocol 13,56 MHz
ISO/IEC 18000-4 Automatic identification - Radio-Frequency Identification for item management - Air interface protocol 2,4 GHz
ISO/IEC 18000-6 Automatic identification - Radio-Frequency Identification for item management - Air interface protocol 870-930 MHz (UHF)

Tabelle 2: *Auswahl relevanter Standards der RFID*
(Quelle: Eurodata Council)

Die technischen Normen sind bereits festgelegt, während die Anwendungsempfehlungen als ISO 17364 bis 17367 dargestellt werden. Dann werden auch die spezifischen Empfehlungen zum Einsatz von RFID auf den Ebenen Produkt, Verpackung, Transporteinheit, wiederverwendbarer Container und Frachtcontainer festgeschrieben. Die Barcode-Standards für Produktverpackungen und Transportkennzeichen fließen aus Gründen der Kompatibilität in die Entwicklung ein, so dass Interoperabilität zwischen Barcode und RFID besteht.[16]

4 Abgrenzung von RFID-Verfahren

Neben RFID gehören unter anderem Mobilfunk, W-LAN oder Bluetooth zu den digitalen Funkanlagen. RFID unterscheidet sich von diesen Verfahren durch die elektronische Identifizierung von Objekten und die Tatsache, dass die Transponder erst bei Aktivierung durch ein Lesegerät die gespeicherten Daten aussenden.

Die führende AutoID-Technik ist zurzeit noch der Barcode. Im Gegensatz zur Radiofrequenztechnologie, bei der Daten über einen Funkfrequenzkanal übertragen werden, basiert der Barcode auf einer optischen Verschlüsselung. Die Daten werden als Strichcode dargestellt und mit einem optischen Lesegerät erfasst.

Diese Technik dominiert momentan noch deutlich sowohl in der Konsumgüterbranche als auch in der Investitionsgüterindustrie gegenüber RFID.

RFID weist jedoch gegenüber anderen AutoID-Techniken eine Reihe von Vorteilen auf:[17]

Leistung	vor allem große Kapazität bei der Datenspeicherung
Effizienz	Pulklesung, hohe Geschwindigkeit, sichtkontaktloses Lesen
Sicherheit	Robustheit gegenüber Umwelteinflüssen, geringe Manipulationsmöglichkeiten
Zusatzfunktionen	Sensorik, Verschlüsselung, Artikelsicherung

Tabelle 3: *Vorteile*

5 Anwendungsfelder der RFID-Technologie im Gesundheitswesen und in der pharmazeutischen Industrie

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

Somit ergeben sich vielfältige Anwendungsfelder der RFID-Technologie im Gesundheitswesen und in der pharmazeutischen Industrie.

Die möglichen Anwendungsfelder der RFID-Technologie lassen sich in fünf Kategorien einteilen:[18]

5.1 Die Identifizierung und Authentifizierung (Wer?)

In Krankenhäusern können die Patienten mit einem Transponder, der z. B. in ein Armband, Brille, etc. (zum Teil schon Realität: Implantate im menschlichen Körper[19]) integriert ist, versehen werden, um die Identität und die Behandlung feststellen und Verwechslungen vermeiden zu können. Ein besonderer Anwendungsfall ist in diesem Zusammenhang auch die eindeutige Identifikation von Neugeborenen. So kann durch RFID beispielsweise das Vertauschen von Neugeborenen verhindert bzw. erschwert werden.

Das Klinikum Saarbrücken beispielsweise hat im April 2005 ein Pilotprojekt gestartet.[20] In der ersten Phase des Projektes erhielten 1.000 Patienten bei der Aufnahme ein Armband mit integriertem RFID-Chip, welcher die Patientennummer enthält.

Mittels Tableau-PCs und PDAs (Personal-Digital-Assistant) lesen Ärzte und Pflegepersonal die Nummer aus und können so die Patienten in Sekundenschnelle identifizieren. Über WLAN und PKI-Verschlüsselungen erhalten die Berechtigten Zugriff auf die Patienten-Datenbank einschließlich der zu verabreichenden Arzneimittel und deren Dosierung.

An Vorteilen werden genannt die sichere und schnellere Identifikation des Patienten, optimalerer Ressourceneinsatz, sichere und einfachere Zuteilung von Medikamenten, ansteigende Patientenzufriedenheit sowie die Möglichkeit der Selbst-Abfrage von Terminen und Werten am Info-Terminal (Blutdruckwerte, Gewicht, Behandlungs- oder Entlassungstermine).[21]

Durch die eindeutige Authentifizierung und Identifikation kann aber insbesondere auch der Zutritt zu sensiblen Bereichen gesichert werden, wie beispielsweise der Zutritt in den Apothekenbereich oder Säuglingsstation aber auch zu bestimmten IT-Anwendungen bis hin zu bestimmten Datensätzen.

Das Projekt des Klinikums Saarbrücken soll um die sichere Zuordnung des richtigen Blutbeutels zum richtigen Patienten ausgeweitet werden. Das Tracking des Beutels, automatisiertes Retourenmanagement, Erweiterung um Sensoren, welche z. B. die Lagertemperatur des Beutels überwachen, die Dokumentation des Weges des Blutbeutel sowie Kostensenkung durch optimalen Einsatz zeigen, dass RFID in Krankenhäusern zur Kontrolle von Blutkonserven sowie Medikamenten genutzt werden können.

5.2 Die Lokalisierung (Wo?)

Insbesondere bei Demenz-Patienten oder Hochrisiko-Patienten kann die Antwort auf die Frage „Wo befindet sich jemand?“ existentiell entscheidend werden.

Auch die Suche nach dem eigenen Personal kann durch die Anwendung der RFID- Technologie beispielsweise in Notfällen lebensrettend verkürzt werden.

Die amerikanische Gesundheitsbehörde hat bereits eine Genehmigung für den Einsatz von RFID-Transpondern im menschlichen Körper erteilt. Der sogenannte „VeriChip“ wird unter die Haut injiziert oder eingepflanzt und soll Ärzten bei Notfällen Auskunft über die Krankengeschichte des Patienten geben.[22]

Für viele Krankenhäuser steht weiterhin die Möglichkeit der Ortung von mobilem Equipment und Instrumenten im Vordergrund.

Im OP ermöglicht RFID ein sicheres Tracking für sämtliche OP-Instrumente und das Personal. Die gesamte medizinische Ausrüstung sowie der Ablauf des chirurgischen Eingriffs können durch den Einsatz von RFID-Transpondern identifiziert, erfasst und dokumentiert werden. Dies gewährleistet und erhöht nicht nur die Sicherheit der Patienten, sondern entlastet zudem das Klinikpersonal, das durchschnittlich etwa 40 Prozent seiner Arbeitszeit damit verbringt, die Vorgänge zu dokumentieren.[23]

5.3 Qualitätsmanagement (Wie?)

Durch Kennzeichnung der Patienten und Medikamente können die Fragen wie: „Richtiger Patient?, Richtiges Medikament?, Richtige Dosierung?“ beantwortet werden. Auch kann mit der RFID-Technologie dokumentiert werden, wer verordnet und verabreicht hat. Selbst das Verfallsdatum oder die Echtheit von Medikamenten kann verifiziert werden.

In der pharmazeutischen Industrie können RFID-Systeme verwendet werden, um Medikamente leichter zu lokalisieren und Fälschungen und Verluste zu vermeiden bzw. festzustellen. Die US-amerikanische Behörde Food and Drug Administration (FDA) empfiehlt den Einsatz von RFID-Transpondern, um Produktfälschungen zu verhindern.[24]

Immer mehr Pharmahersteller bestücken daher ihre Medikamente mit RFID-Transpondern, um sie vor Fälschungen und Missbrauch zu schützen. Auch der Weg von Blutkonserven lässt sich mit RFID lückenlos nachvollziehen. In Kombination mit Temperatursensoren sichert die Technologie darüber hinaus die Qualität der Spende.[25]

In Schweden wurde ein neues RFID-System für die Anbringung an pharmazeutischen Verpackungen entwickelt, das bereits bei einem Feldversuch im Einsatz ist. Der Chip, der über einen Speicher von 32 Kilobyte verfügt, kann laut dem Herstellerunternehmen Cypak umfassende Bestände verschlüsselter Daten sammeln, bearbeiten und austauschen.[26]

Auch einige Großlabors nutzen die RFID-Technologie bereits heute, um ihre umfassenden Bestände an Gewebe- oder Blutproben zu verwalten. Wenn Arzneimittel lückenlos mit RFID-Transpondern ausgestattet wären, ließen sich Missbrauch und Fehlanwendungen deutlich reduzieren. Patienten könnten gewarnt werden, wenn sie ein Medikament zu häufig oder zu selten einnehmen. Sehbehinderten, so ein Szenario von Sun Microsystems, könnte ein Ausgabegerät Hinweise geben: „Dies ist Aspirin. Nehmen Sie zwei pro Tag“.[27]

5.4 Logistik in den Kliniken

Das Tracking (Nachverfolgung) von Inventar wie Betten, Pumpen, Wäsche sind Beispiele der vielfältigen Anwendungsmöglichkeiten für einen sinnvollen Logistik-Einsatz.

Zukünftig wird auch die direkte Kennzeichnung von Verbrauchsmaterialen wie z. B. Tupfer oder die automatische Befüllung von Schränken oder ähnliches wirtschaftlich sinnvoll sein. So könnte festgestellt werden, dass die Blutkonserve immer optimal gelagert wurde. Die mögliche Reduzierung von Beständen wie z. B. die Anzahl der Infusions-Pumpen oder auch die Anzahl der Betten, wie es in den USA. bereits durch Projekte belegt wurde, ist ein Hauptnutzen des Einsatzes von RFID im Logistik-Umfeld.

5.5 Prozess- bzw. Workflow-Optimierung

Durch den Einsatz von RFID können Prozesse dokumentiert und überwacht werden, so dass Abläufe leichter analysiert und optimiert aber auch automatisiert werden können. Im Umfeld der RFID-Systeme kann eine automatische Verrechnung bzw. Kostenzuordnung eingerichtet werden.

Prozessoptimierung kann aber auch bedeuten, verschiedene Arbeitsschritte zu kombinieren und zu automatisieren, wie z. B. die Übermittlung von Vitalwerten und die Verbindung zur elektronischen Gesundheitsakte. Die Möglichkeiten sind vielfältig.

Der Einsatz der RFID-Technologie kann helfen, die Behandlung der Patienten zu verbessern und Verwaltungskosten zu reduzieren.

6 Verfassungs- und Datenschutzrecht[28]

„Moderner Datenschutz", so der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit „hat nicht das Ziel, innovative technologische Entwicklungen zu verhindern."[29] Jedoch müssen Hersteller, Anwender und Nutzer von RFID den Fragen des Datenschutzes und der Datensicherheit höchste Aufmerksamkeit entgegenbringen, um Fehlentwicklungen und Missbrauch wirksam zu verhindern.

Aufgrund der kontaktlosen Auslesbarkeit der RFID-Chips ist die Frage zu beantworten, ob die Technologie Einschränkungen für das verfassungsrechtlich verbürgte Recht der Bürger auf informationelle Selbstbestimmung mit sich bringt. In der öffentlichen Diskussion wird befürchtet, dass gesammelte Daten beliebig miteinander verknüpft werden, ohne dass der Bürger etwas davon erfährt. Das deutsche und das europäische Recht verfügen jedoch über gute Schutzvorkehrungen zur Wahrung der Privatsphäre im Recht des Datenschutzes, in der Datensicherheit von RFID-Systemen sowie zum Schutz der vertraulichen Kommunikation und damit des Fernmeldegeheimnisses.

Gegenwärtig existieren keine speziellen datenschutzrechtlichen Bestimmungen, die den Einsatz und den Umgang mit der Radiofrequenztechnologie zu Identifikationszwecken differenziert reglementieren.[30]

Sowohl das Bundesdatenschutzgesetz (BDSG)[31] als auch die Datenschutzgesetze der Länder konkretisieren jedoch die verfassungsrechtlichen Anforderungen an den Datenschutz.[32] Alleine das auf Art. 29 der Datenschutzrichtlinie der Europäischen Gemeinschaft (EG) basierende Arbeitspapier mit dem Titel „Datenschutzfragen im Zusammenhang mit der RFID-Technik" weist auf eine potentielle Gefahr für das Persönlichkeitsrecht beim Einsatz der RFID-Technik im Krankenhausbereich hin.[33] Eine detaillierte Betrachtung bestehender Datenschutzvorschriften ist deshalb nur im Hinblick auf den konkreten Einzelfall möglich und sinnvoll.

Dementsprechend stellt sich hier die Frage, inwieweit das geltende Datenschutzrecht angemessen ist, um die Belange der Betroffenen und Patienten in Bezug auf die Anwendung der Radiofrequenztechnologie zu Identifikationszwecken im Gesundheitswesen zu wahren.

Gemäß § 1 Abs. 1 des Bundesdatenschutzgesetzes (BDSG) soll der einzelne vor der Beeinträchtigung von Persönlichkeitsrechten geschützt werden, die durch den Umgang anderer mit seinen personenbezogenen Daten entstehen kann. Der Anwendungsbereich des Gesetzes wird somit durch den Begriff der „personenbezogenen Daten" bestimmt.

Ziel und Zweck des Datenschutzes ist nicht der Schutz von Daten, sondern der Schutz von Personen vor Missbrauch und unberechtigtem Zugriff auf personenbezogene Daten. Ein wichtiger Aspekt hierbei ist die informationelle Selbstbestimmung. Grundsätzlich darf jeder selbst über die Verbreitung persönlicher Daten entscheiden. „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer Person" (§ 3 BDSG). Daten werden zu personenbezogenen Daten durch Verknüpfung von z. B. Namen mit Geburtsdatum, Kfz-Kennzeichen, Kontonummer oder Gesundheitsdaten. RFID-Anwendungen, bei denen keine Personen betroffen sind (u. a. zur Tieridentifikation) werfen dahingehend keine datenschutzrechtlichen Probleme in Bezug auf personenbezogene Daten auf.[34]

Bei RFID-Anwendungen ist danach zu differenzieren, ob personenbezogene Daten betroffen sind. Grundsätzlich lassen sich hier drei verschiedene Fallgruppen unterscheiden.[35]

- Zum einen gibt es RFID-Anwendungen bei denen ausschließlich ein elektronischer Produktcode (EPC) auf den Tags gespeichert wird (Fallgruppe 1).
- In einer zweiten Fallgruppe werden diese Produktcodes mit Versicherten-/Patientdaten verknüpft, die in einer Datenbank gespeichert sind (Fallgruppe 2).
- In einer dritten Fallgruppe werden persönliche Daten direkt auf dem Tag gespeichert (Fallgruppe 3).

Als Fazit kann festgehalten werden, dass personenbezogene Daten auch bei der Verwendung der Transpondertechnologie durch die geltenden Bestimmungen des BDSG geschützt sind. Personenbezogene Daten sind tangiert und damit der Anwendungsbereich des BDSG eröffnet, wenn Angaben über persönliche oder sachliche Verhältnisse einer Person unmittelbar auf dem Tag gespeichert werden. Des Weiteren ist dies der Fall, wenn eine Verknüpfung über das Tag mit solchen Daten möglich ist, die in einer Datenbank gespeichert sind. Ist das BDSG anwendbar, so ist die Erhebung, Verarbeitung und Nutzung personenbezogner Daten nach § 4 Abs. 1 BDSG nur dann zulässig, wenn der Betroffene eingewilligt hat oder das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder anordnet. Auch die weiteren datenschutzrechtlichen Grundsätze wie das Prinzip der Erforderlichkeit, der Transparenz- und der Zweckbindungsgrundsatz sind zu beachten. Werden mobile Speichermedien eingesetzt, bestehen zusätzliche Unterrichtungspflichten des Verwenders. Bei einem elektronischen Produktcode, der auf einem RFID-Tag gespeichert ist, handelt es sich nicht um ein personenbezogenes Datum, so dass datenschutzrechtliche Vorschriften nicht anwendbar sind.[36]

7 Recht der Datensicherheit

Neben den Chancen, die die RFID-Technologie für die Gesellschaft und die Gesundheitswirtschaft eröffnet, entstehen auch neue Risiken. Der wirtschaftliche Erfolg wird davon abhängen, inwieweit es gelingt, die anfallenden Daten gegen Datenverlust und -missbrauch zu schützen.[37]

Die RFID-Technologie ist technischer Sicherheitsrisiken ausgesetzt. Bei der Speicherung von Daten auf einem Tag kann sich in mehrfacher Hinsicht eine spezifische Bedrohungslage ergeben.[38] Bedrohungen können sich für die Verfügbarkeit von Daten, deren Integrität, Vertraulichkeit und Authentizität einstellen.[39]

Eine der signifikanten 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.

Eine weitere Angriffsart besteht in der Fälschung des Inhalts oder der Identität eines Transponders.[40]

Die Sicherheit von RFID-Systemen kann auch durch das Stören des Datenaustauschs durch Denial-of-Service-Angriffe (DoS-Angriffe) beeinträchtigt werden. Der Datenaustausch kann zum einen aktiv, z. B. durch Benutzen eines Störsenders, behindert werden. Wenn dieser Störsender ein ausreichendes künstliches Umgebungsrauschen erzeugt, sind Tag und Reader nicht mehr in der Lage, dieses Signal durch ihr eigenes Nutzsignal zu überlagern.[41] Außerdem kann der Datentransfer durch den unautorisierten Gebrauch von Deaktivierungsbefehlen unterbrochen werden.

Eine weitere Gefahr besteht im Zerstören der RFID-Chips. Transponder können durch physische Gewalteinwirkung oder auch durch Mikrowellenstrahlung beschädigt oder zerstört werden.[42] Das gleiche Ergebnis kann auch durch die Verwendung von elektromagnetischen Feldern erreicht werden. Ein passives Tag bezieht seine Energie aus dem magnetischen Feld des Lesegeräts. Wird nun ein geeignetes Feld erzeugt, das hinreichend stark ist, so kann die Kopplungseinheit des Tags oder sogar das gesamte Tag zerstört werden.[43]

Schließlich können sich Angriffe auf das Backend 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. Dadurch kann die Identität eines Lesegeräts mit autorisiertem Zugang zum Backend gefälscht werden. Allerdings handelt es sich hierbei nicht um RFID-spezifische, sondern um allgemeine IT-Sicherheitsrisiken, die mit den üblichen IT-Sicherheitsverfahren abgewehrt werden können. Diese lassen sich leichter neuen Erfordernissen anpassen als Sicherheitsverfahren, die auf den Tags implementiert werden.

Ausgehend von den oben geschilderten Angriffsmöglichkeiten bieten sich folgende technische Sicherheitsmaßnahmen an:

- Authentifizierung
- Verschlüsselung
- Verhinderung des Auslesens durch Blocker-Tags
- Deaktivierung durch Kill-Befehl.[44]

Insbesondere im Bereich der Datenverarbeitung im Backend[45] sind gemäß § 9 BDSG i. V. m. Punkt 3 der Anlage zu § 9 S. 1 BDSG Maßnahmen für eine ausreichende Zugriffskontrolle zu veranlassen. Hier kommen insbesondere in Betracht:[46]

- Festlegen der Zugriffsbefugnisse der einzelnen Mitarbeiter
- Identifikation der Zugreifenden
- Protokollieren von Zugriffen und Missbrauchsversuchen
- Authentifizierung durch Passwortschutz
- Automatischen log-off nach einem bestimmten Zeitraum/nach Dienstschluss

Auch für die Weitergabekontrolle sind erforderliche Maßnahmen zum Schutz der personenbezogenen Daten zu treffen. Gemäß § 9 BDSG i.V.m. Punkt 4 der Anlage zu § 9 S. 1 BDSG müssen personenbezogene Daten, wenn sie im Rahmen von RFID-Systemen übertragen werden, grundsätzlich verschlüsselt werden. Weiterhin können Maßnahmen zur Authentifizierung von Tag und Reader nach den Grundsätzen des Verhältnismäßigkeitsgrundsatzes (Entwicklungskosten versus Risikoanalyse) getroffen werden.

Insgesamt lässt sich feststellen, dass die RFID-Technologie zwar neue Risiken für die Verfügbarkeit der Daten, deren Integrität, Vertraulichkeit und Authentizität in sich birgt. Allerdings kann diesen Gefahren durch technische Sicherheitsmaßnahmen begegnet werden. So können Authentifizierungsmechanismen eingesetzt werden wie z. B. ein Passwortschutz. Eine weltweit eindeutige Regelung zur Vergabe von Seriennummern kann zum Identitätsschutz von Transpondern beitragen. Darüber hinaus bieten sich Verschlüsselungsverfahren und Deaktivierungsmöglichkeiten an. Insbesondere für den Bereich der personenbezogenen Daten bestehen umfangreiche rechtliche Verpflichtungen zur Datensicherung.[47]

7.1 Strafrechtlicher Schutz

Die Sicherheit und Integrität von RFID-Systemen ist auch strafrechtlich geschützt. An Straftatbeständen sind zu nennen:

- Datenveränderung gemäß § 303 a StGB
- Computersabotage gemäß § 303 b StGB
- Fälschung beweiserheblicher Daten gemäß § 269 StGB
- Verändern beweiserheblicher Daten gemäß § 274 Abs. 1 Nr. 2 StGB
- Computerbetrug gemäß § 263 a StGB

Der strafrechtliche Schutz ist gut ausgeprägt, so dass eine zusätzliche gesetzliche Regelung für die RFID-Technologie nicht erforderlich erscheint.

7.2 Schutz der vertraulichen Kommunikation

Des Weiteren wird die Integrität, Vertraulichkeit und Authentizität von RFID-Systemen auch durch das Fernmeldegeheimnis geschützt. Vom Abhörverbot des § 89 TKG ist nur das beabsichtigte Auslesen von Transpondern betroffen. Zusätzlich wird die Vertraulichkeit durch die Straftatbestände der §§ 148 Abs. 1 Nr. 1 TKG und § 202 a StGB abgesichert.[48]

7.3 Datenschutzanforderungen

Die informationelle Selbstbestimmung zu respektieren, bedeutet den Verzicht auf vermeidbare Verarbeitungen personenbeziehbarer Daten, die Herstellung von Transparenz durch Informationen sowie die Schaffung von Handlungsoptionen für die Betroffenen. Daher sollten sich Einrichtungen und Unternehmen, die mit RFID arbeiten wollen und dabei auf die Personenbeziehbarkeit der Daten nicht verzichten können, Datenschutzpolitisch mindestens an folgenden nicht in jedem Einzelfall abschließenden 11-Punkte- Katalog orientieren:[49]

1 Alternativenprüfung, d. h.: Kann das angestrebte Ziel auch ohne Verarbeitung personenbeziehbarer Daten erreicht werden? Gibt es ganz andere Möglichkeiten, das Ziel zu erreichen?
2 Technikfolgenabschätzung /Vorabkontrolle.
3 Zweckbindung: Eindeutige Festlegung des die Datenverarbeitung rechtfertigenden Zwecks (keine spätere Änderung oder Erweiterung mehr).
4 Datensparsamkeit/Erforderlichkeitsgrundsatz, d. h. die Menge personenbeziehbarer Daten darf nur so gering wie möglich sein; das zulässige Ausmaß der

Verarbeitung hat sich auf den unabdingbar nötigen Umfang zu beschränken.
5 Datenspeicherung nur für die Dauer, die zur Zweckerreichung erforderlich ist.
6 Datensicherheitsfragen: Sicherheitskonzept, u. a. sichere Verschlüsselung der Daten, wirksamen Authentisierung der beteiligten Geräte, Systemgestaltung, die keine unbemerkte oder ungewollte Profilerstellung ermöglicht.
7 Betroffene Personen sind umfassend zu informieren über z. B. den Einsatz und die Funktionsweise des Systems, die Art der zu verarbeitenden Daten, den Verarbeitungszweck, ihre Rechte auf Auskunft, Berichtigung und Löschung der Daten zur eigenen Person usw.
8 Mit RFID-Tags versehen Produkte sowie zum System gehörende Lesegeräte sind zu kennzeichnen.
9 Betroffenen Personen ist die Wahrnehmung ihrer Rechte zu gewährleisten.
10 Betroffenen Personen ist der einzelne Verarbeitungsvorgang transparent zu machen, z. B. durch die eindeutige Erkennbarkeit von Kommunikationsvorgängen, die eine Verarbeitung personenbezogener Daten auslösen (optisches/akustisches Signal).
11 Betroffenen Personen sind Möglichkeiten zur Blockierung, Deaktivierung, Löschung oder Entfernung von RFIDs zur Verfügung zu stellen; es darf keinen faktischen Nutzungszwang geben; im Handel z. B. müssen anonyme Kaufmöglichkeiten erhalten bleiben, ohne dass Nachteile in Kauf genommen werden müssten.

8 Europa-Recht

Die Gesundheitssysteme und die einzelstaatlichen Gesundheitspolitiken in der Europäischen Union (EU) sind heute enger als jemals zuvor miteinander verknüpft. Dies ist auf viele Faktoren zurückzuführen, zu denen auch die Verbreitung neuer medizinischer Technologien, wie bspw. der Einsatz der Radiofrequenztechnologie zu Identifikationszwecken, zählt.

Auch auf europäischer Ebene werden die Risiken von RFID gesehen. EU-Kommissarin Viviane Reding hat angekündigt, dass die Europäische Kommission Richtlinien für die Funktionstechnologie RFID entwickeln wird, die in das europäische Datenschutzrecht einfließen sollen. Die Prämisse dabei wird sein, dass zwar der Einsatz von RFID in Europa gefördert werden soll, aber gleichzeitig der Schutz persönlicher Daten und der Privatsphäre sichergestellt werden muss.[50]

Das Europäische Institut für Computer Anti-Viren Forschung (EICAR) hat hierzu einen Leitfaden (EICAR-RFID-Leitfaden) erarbeitet, der konkrete Anwendungsszenarien vorstellt und hinsichtlich datenschutzrechtlicher Aspekte bewertet. EICAR ist eine Plattform für den Informationsaustausch im Bereich der Computer Anti-Viren-Forschung.[51]

Aktuell gibt es auf Europäischer Ebene verschiedene Rechtsgrundlagen, deren Anwendungsbereich sowie Regelungsvorgaben in jedem Einzelfall zu prüfen und bei den Akteuren und Betroffenen Beachtung finden müssen. Im Folgenden werden auf Grund der Auswirkungen des Gemeinschaftsrechts auf die nationale Gesetzgebung, auch im Bereich innovativer Technologien im Gesundheitswesen, einige für den Einsatz der Radiofrequenztechnologie zu Identifikationszwecken relevante Regelungen der EU beispielhaft genannt. An Regelungen der EU für Dienste in der Informationsgesellschaft existieren insbesondere:

- Electronic-Commerce-Richtlinie(RLeG) (2000/31/EG)
- Richtlinie für elektronische Signaturen (RLeS) (1999/93/EG)
- Fernabsatzrichtlinie (1997/7/EG)
- Richtlinie über missbräuchliche Klauseln in Verbraucherverträgen (93/13/EWG)
- Richtlinie über allgemeine Produktsicherheit (92/59/EWG)
- EG-Transparenzrichtlinie (98/34/EG)
- Richtlinie über die Haftung für fehlerhafte Produkte (85/374/EGW)
- Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (95/46/EG)
- Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (2002/58/EG)
- Richtlinie über den Schutz von Datenbanken (96/9/EG)
- Richtlinie über aktive implantierbare und medizinische Geräte (90/385/EWG)
- Richtlinie über Medizinprodukte (93/42/EWG)
- Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste (Rahmenrichtlinie 2002/21/EG)
- Richtlinie über die Genehmigung von elektronischen Kommunikationsnetzen und –diensten (Genehmigungsrichtlinie 2002/20/EG)
- Richtlinie über den Zugang zu elektronischen Kommunikationsnetzen und –diensten (Zugangsrichtlinie 2002/19/EG)
- Richtlinie über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten (Universaldienstrichtlinie 2002/22/EG)

Ein Arbeitspapier mit dem Titel „Datenschutzfragen im Zusammenhang mit der RFID-Technik“ vom 19. Januar 2005 basiert auf Art. 29 der EG-Datenschutzrichtlinie. Die Arbeitsgruppe ist gemäß Artikel 29 der Richtlinie 95/465/EG eingesetzt worden. Sie ist ein unabhängiges EU-Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 15 der Richtlinie 2002/58/EG festgelegt.

9 Resümee und Ausblick

Die Entwicklungsperspektiven der RFID-Technologie werden nicht allein von den technischen Möglichkeiten geprägt. Neben Technologie und Standardisierung sind auch die Markt- und Preisentwicklung, Informationssicherheit und Datenschutz sowie der gesellschaftliche Diskurs zu diesen Anforderungen zu berücksichtigen.

Für die kommenden Jahre ist mit einer weiteren exponentiellen Steigerung der Leistungsentwicklung der Informations- und Kommunikationstechnologie zu rechnen. Neben der Verbesserung des Preis-Leistungsverhältnisses werden sich die eingesetzten technologischen Komponenten weiterhin drastisch verkleinern. Die Miniaturisierung der Mikroelektronik wird voraussichtlich noch etwa zehn Jahre ohne Technologiebruch voranschreiten. Sie ist eine wesentliche Triebkraft für die Realisierung der Vision „Pervasive Computing“.[52]

Schon jetzt ist die nächste Generation von RFID-Tags absehbar, die neben einem einfachen Speichermodul auch Sensorik und Aktuatorik enthalten. Denkbar sind beispielsweise Tags, die die Umgebungstemperatur messen und eigenständig die Kühlung ansteuern oder über GPRS- oder GSM-Meldungen absetzen. Auch wurden bereits so genannte RFIDsecure-Chips vorgestellt, die über eine eingebaute Zugangskontrolle auf der Basis verschiedener Verschlüsselungsstufen verfügen. Der Chip kann somit in unterschiedlichen Nutzermodi arbeiten, die beispielsweise auf den Besitzer des Chips, den Anwender der verarbeiteten Daten oder die aufsetzende Anwendung gerichtet sind.[53]

Der schnelle und effektive Verbraucher- und Patientenschutz ist gerade auch im eigenen Interesse der Gesundheitswirtschaft, die sich große ökonomische Potentiale vom weiteren RFID-Einsatz erhofft. Eine verbindliche, auch mit Sanktionsmaßnahmen verbundene Selbstverpflichtung der Hersteller und Anwender kann ein Weg für vertrauensbildende Maßnahmen sein.

Der ständige technologische Wandel bringt stets potentielle Risiken mit sich. Doch gerade das deutsche Datenschutz- und Datensicherheitsrecht weist im internationalen Vergleich ein besonders hohes Schutzniveau auf. Im Unterschied z. B. zu den Vereinigten Staaten wird es in der Bundesrepublik als eine bedeutende Aufgabe des Staates angesehen, für ein angemessenes Niveau an Datenschutz, Schutz des Fernmeldegeheimnisses und der Datensicherheit zu sorgen.

Um den Vorbehalten gegen RFID Rechnung zu tragen, sollten Vorkehrungen getroffen werden, die über das Bestehen des gesetzlich festgesetzten Schutzniveaus hinausgehen. Hierzu bieten sich Selbstverpflichtungen von beteiligten Unternehmen zur Umsetzung von Hinweispflichten bzw. Kennzeichnung von Produkten an, die mit RFID-Tags ausgestattet sind. Den Verbrauchern sollten weiterhin Auskunftsrechte in Bezug auf die gespeicherten Daten gewährt werden, auch wenn es sich nicht um personenbezogene Daten handelt. Ferner sollte den Verbrauchern die Möglichkeit zur Deaktivierung von RFID-Tags zugesichert werden. Durch Auditierungsverfahren könnte ein freiwilliges Managementsystem zum Schutz persönlicher Daten, der Datensicherheit sowie des Fernemeldegeheimnisses installiert werden. Gütesiegel können mit dazu beitragen, das Vertrauen der Bürger zu stärken, da sie so selbst bewerten können, wie ein Unternehmen mit den Themen Datenschutz und Sicherheit umgeht.[54]

Gegen den Einsatz von RFID-Systmen, soweit er auf gesetzlicher Grundlage und unter Beachtung der datenschutzrechtlichen Bestimmungen erfolgt, ist laut Bundesdatenschutzbericht grundsätzlich nichts einzuwenden: „Es ist legitim, die neuen technischen Entwicklungen zu nutzen [...]. Zugleich werden aber technische Kontrollsysteme und eine Überwachungsstruktur aufgebaut, die, einmal vorhanden, auch noch zu ganz anderen Zwecken genutzt werden könnten und deren gesetzes- und datenschutzkonforme Anwendung letztlich nicht mehr kontrollierbar ist. [...] Auch hier zeigt sich wieder, dass die Summe von nützlichen und für sich gesehen datenschutzkonformen Anwendungen insgesamt ein Bedrohungspotenzial für das Grundrecht auf informationelle Selbstbestimmung darstellt, das von den Betroffenen und auch in der gesellschaftlichen Diskussion so zunächst nicht wahrgenommen wird.“[55]

Auf Europäischer Ebene erweisen sich die bestehenden Regelwerke für die Anwendbarkeit von RFID im Gesundheitswesen als Vorgaben und Hilfestellungen für die Anwendbarkeit der neuen Technologie. Darüber hinaus will die EU-Kommission spezifische Richtlinien für RFID entwickeln.

Aktuell zeigt sich das deutsche Datenschutzrecht als Datensicherheitsrecht flexibel genug, um den Einsatzmöglichkeiten im Gesundheitswesen, die der momentane Stand der Entwicklung der RFID bietet, gerecht zu werden. Ob zukünftig spezifische Regelungen für den Einsatz der RFID-Technologien im Gesundheitswesen vom Gesetzgeber erlassen werden müssen wird sich nach Abschluss von laufenden Pilotprojekten und deren Bewertung zeigen.

Prof. Dr. iur. Heinrich Hanika ist Professor für Wirtschaftsrecht und Recht der Europäischen Union an der Fachhochschule Ludwigshafen a. Rh. und Dozent an der Steinbeis-Hochschule Berlin. Er lehrt und forscht an den Schnittstellen des Rechts zu Informatik, Management, Medizin sowie Ökonomie im Gesundheitswesen (www.h-hanika.de).

Fußnoten

1 Bundesamt für Sicherheit in der Informationstechnik, Risiken und Chancen des Einsatzes von RFID-Systemen 2004, S. 14.
2 Rhiel, Vorwort, in: Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, RFID Geschäftsprozesse mit Funktechnologie unterstützen, 2006.
3 Jell, RFID als funkender Helfer im OP, Krankenhaus 9/2007, S. 881.
4 ACG IDENTIFICATION TECHNOLOGIES GMBH, http://www.acg.de, zit. in: Bundesamt für Sicherheit in der Informationstechnik, (Fn. 1), S. 71.
5 Siehe Hanika, RFID-Technologie im Gesundheitswesen aus rechtlicher Sicht, in: Schmücker/Ellsässer (Hrsg.), Praxis der Informationsverarbeitung in Krankenhaus und Versorgungsnetzen (KIS) 2007, S. 291 ff.
6 Klußmann, Lexikon der Kommunikations- und Informationstechnik 2001, S. 829 ff. (897).
7 Der Begriff Transponder setzt sich zusammen aus den Begriffen Transmitter und Responder, vgl. Lahner, Datenschutzrechtliche Probleme beim Einsatz von RFID-Systemen 2004, S. 1.
8 Association for Automatic Identification and Mobility (AIM), What is Frequency Identification (RFID)? 2004.
9 Holznagel/Bonnekoh, RFID – Rechtliche Dimensionen der Radiofrequenz-Identifikation, www.RFID-support-center.de am 25.05.2008.
10 Finkenzeller, RFID-Handbuch, Grundlagen und Praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten 2003, S. 6 f.
11 Weiterführend Holznagel/Bonnekoh (Fn. 9), S. 10 m.w.N.
12 Schaar, der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, schriftliche Stellungnahme für die öffentliche Anhörung im Landtag Nordrhein-Westfalen am 19.04.2007 zur Thematik „Radio-Frequenziden-

tifikation (RFID)“, s. www.RFID-Support-Center.de.
13 Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, (Fn. 2), S. 6.
14 Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, (Fn. 2), S. 7 f.
15 Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, (Fn. 2), S. 9.
16 Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, (Fn. 2), S. 10 ff. m.w.N.
17 Hessisches Ministerium für Wirtschaft, Verkehr und Landesentwicklung, (Fn. 2), S. 15 f.
18 Siehe Canedo-Lindow, RFID im Gesundheitswesen – Anwendungen, Praxisbeispiele und Ausblick, Tag der RFID-Technologie im Landtag NRW am 19.04.2007, siehe www.RFID-support-center.de.
19 Sokol, Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, Stellungnahme im Rahmen der öffentlichen Anhörung im Landtag Nordrhein-Westfalen am 19.04.2007 zu Radiofrequenzidentifikation (RFID).
20 www.Klinikum-Saarbrücken.de/klinik-news/index.php3?tid=256&a=NEWS.
21 Canedo-Lindow, (Fn. 18), S. 3.
22 Department of Health and Human Services, Food and Drug Administration, 21 CFR Part 880, Docked No. 2004 N-0477, veröffentlicht im Federal Register/Vol.69, No. 237/10. December 2004/Rules and Regulations.
23 Jell, (Fn. 3), S. 881.
24 S. unter www.fda.gov
25 Jell, (Fn. 3), S. 882
26 ORF FutureZone, Ein Rechner aus Pappkarton v. 05.03.2004, http://futurezone.orf.at./futurezone.orf?read=detail&id=219132&tmp=7798
27 Hillenbrand, Wissen ist Verbraucherchermacht, in: Spiegel Online vom 03.09.2003, http://www.spiegel.de/wirtschaft/0,1518,262761,00.html
28 Siehe weiterführend und vertiefend das Rechtsgutachten von Holznagel/Bonnekoh, (Fn. 9), S. 21 ff.
29 Zitiert in: Keymis, Tag der RFID Technologie im Landtag NRW, am 19.04.2007.
30 Tönjes, RFID-Chips, http://www.datenschutz.de/feature/detail/?featid=2 (08.03.2007).
31 Die in dieser Arbeit genannten Paragraphen des Bundesdatenschutzgesetzes (BDSG) beziehen sich alle auf den Gesetzesstand v. BGBl I 2003, 66 idF v. 25.08.2006, BGBl I 2006, 1970.
32 Hanika, Datenschutz, in: Rieger (Hrsg.), Handbuch des Arztrechts 2002, Rn. 5.
33 Artikel-29-Datenschutzgruppe, 10107/05/DE, WP 105, 19.01.2005, abrufbar unter: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_de.pdf.#search=%22arbeitspapier%20rfid-technik%22
34 RFID Support Center, Datenschutz bei RFID-Anwendungen, www.rfid-support-center.de, September 2007, S. 9.
35 Holznagel/Bonnekoh, (Fn. 9), S. 21.
36 Zu alledem Holznagel/Bonnekoh, (Fn. 9), S. 25 ff. (36) m.w.N.
37 Studie des Bundesamtes für Sicherheit in der Informationstechnik (BSI), (Fn. 1), S. 101.
38 Zu den unterschiedlichen Bedrohungslagen umfassend Kapitel 7 der BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, (Fn. 1), wobei hier die verschiedenen Angriffsarten auch nach den unterschiedlichen Bedrohungslagen der aktiven (Betreiber der RFID-Systeme) und der passiven Partei (insbesondere Kunden und Arbeitnehmer) differenziert werden.
39 Holznagel, Recht der IT-Sicherheit, 2003, S. 12 ff.
40 BSI-Studie, Risiken und Chancen des Einsatzes von RFID-Systemen, (Fn. 1), S. 42.
41 Kelter/Wittmann, DuD 2004, S. 331 ff.
42 Kelter/Wittmann, (Fn. 41), S. 333.
43 Kelter/Wittmann, (Fn. 41), S. 333 f.
44 Vertiefend: Holznagel/Bonnekoh, (Fn. 9), S. 41 ff. m.w.N.
45 Unter Backend versteht man die Datenbestände, mit denen die vom Lesegerät erfassten Daten über weitere Kommunikationskanäle verknüpft werden.
46 Vertiefend Ernestus/Geiger, in: Simitis, Kommentar zum Bundesdatenschutzgesetz, 2003, § 9 Rn. 112.
47 Holznagel/Bonnekoh, (Fn. 9), S. 38 ff.
48 Holznagel/Bonnekoh, (Fn. 9), S. 51 ff. m.w.N.
49 Sokol, (Fn.19), S. 1 ff.
50 Schaar, (Fn. 12), S. 4
51 www.eicar.org/taskforces/rfid/RFID-Leitfaden-100406.pdf am 25 03.08.
52 Hilty/Behrendt/Binswanger/Bruinink/Erdmann/Fröhlich/Köhler/Kuster/Som/Würtenberger, Das Versorgungsprinzip in der Informationsgesellschaft Auswirkungen des Pervasive Computing auf Gesundheit und Umwelt. Eine Studie der Eidgenössischen Materialprüfungs- und Forschungsanstalt (EMPA) und des IZT – Institut für Zukunftsstudien und Technologiebewertung im Auftrag des Zentrums für Technologiefolgen-Abschätzung beim Schweizerischen Wissenschafts- und Technologierat (TA-SWISS) von August 2003, TA 46/2003). http://www.ta-swiss.ch/www.remain/projects_archive/information_society/pervasive_d.htm.
53 Bungard/Glage/Schulz/Tönjes/Wehrmann/Wirth, Arbeitskreis „Technische und organisatorische Datenschutzfrage“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Orientierungshilfe „Datenschutzgerechter Einsatz von RFID“ v. 14.12.2006.
54 Holznagel/Bonnekoh, (Fn. 9), S. 66.
55 Bundesbeauftragter für den Datenschutz; Tätigkeitsbericht 2001 und 2002 des Bundesbeauftragten für den Datenschutz. 19. Tätigkeitsbericht, Bundesdatenschutzbericht: http://www.bfd.bund.de/information/19tb0102.pdf.

Kontakt
Heinrich Hanika
Prinz-Rupprecht-Str. 24
67146 Deidesheim
Tel.: +49 (0) 63 26 / 17 88
Fax: +49 (0) 63 26 / 98 24 46
heinrich@h-hanika.de