



Fraktion im Sächsischen Landtag

Johannes Lichdi  
Mitglied des Sächsischen Landtages

**Dresden, 28.6.2005**

## **Rede zur RFID-Technik**

Mein Vortrag ist in vier Teile gegliedert. Zunächst sage ich etwas zur RFID-Technik. Dann nenne ich einige Einsatzbereiche. Drittens beschreibe ich die Gefahren und viertens versuche ich einige Folgerungen für den Datenschutz zu ziehen.

### **I. Was ist RFID?**

RFID heißt Radio frequency identification, also Radio-Frequenz-Identifizierung. RFID beschreibt eine Identifizierungstechnik, die vermittels eines Art Peilsenders und eines Lesegeräts funktioniert. Die RFID-Technik ist ein Mikrochip, der Daten enthält, der über Lesegeräte ausgelesen werden kann. Lesegeräte funkeln ein Signal an den Chip, der dann die gespeicherten Daten preisgibt. Die Auslesung ist ohne Sichtkontakt möglich, so dass sie heimlich geschehen kann.

Die Daten werden dann mit den in einer Datenbank hinterlegten verglichen. So gelingt die Identifizierung eines Gegenstandes und die Feststellung seines geographischen Ortes. Der RFID-Chip ermöglicht so etwa wie ein Mobiltelefon die Ermittlung des Aufenthaltsortes.

Der Chip ist dünn wie ein Haar, etwa 3 Quadrat-Millimeter. Er passt daher überall hinein, in ein Warenkett, eine Eintrittskarte oder einen Geldschein. In jedem Kleidungsstück, Schuh oder Joghurtbecher ist er unterzubringen. Und er ist sehr billig, die Kosten liegen unter einem Euro!

Die Auslesung ist je nach Bauart in einem Abstand von nur wenigen Zentimetern bis zu 30 Metern möglich. In Zukunft wird vielleicht sogar eine Auslesung über das Global Positioning System - GPS – über Satellit aus dem Weltall vorstellbar. In einer weiteren Stufe können die RFID-Chips auch miteinander Daten austauschen.

### **II. Wo wird die RFID-Technik angewendet?**

Die RFID-Technik wird beim Warenmanagement, bei Zufahrtssperren, bei Elektronischen Wegfahrsperrern, in den neuen biometrischen Pässen und auch bei den WM-Tickets für die Fußballweltmeisterschaften benutzt.

#### 1. Kaufhäuser

Die RFID-Technik könnte bald den Strich-Code auf den Waren im Kaufhaus ersetzen. Der Handel verspricht sich durch die Kennzeichnung mit RFID-Technik eine bessere Kontrolle der Produkte in der Logistikkette. Jedes Produkt erhält eine individuelle Produktnummer, die weltweit einzigartig

ist, den Electronic Product Code, EPC.

Das Produkt kann dann mit Hilfe des EPC von der Produktion, über den Versand, und die Aufstellung im Laden jederzeit identifiziert werden. Die Bekleidungs-Firma Benetton hat bereits RFID-Chips in ihre Klamotten eingewebt.

Wenn das Produkt verloren gegangen ist, kann durch Peilung nach ihm gesucht werden. Und schließlich kann der Weg des Produkts verfolgt werden, wenn es gestohlen worden ist. Für Kaufhäuser und Einzelhändler ist das ein verlockendes Szenario, den erheblichen "Schwund" durch Diebstahl zu verhindern.

Aber es lassen sich noch mehr Einsatzmöglichkeiten denken: Die mit RFID-Chip versehenen Waren im Einkaufswagen melden ihren Preis und der wird dann automatisch von der Kundenkarte des Käufers abgebucht. Oder der Kunde erhält eine Nachricht, wenn er ratlos vor dem vollen Regal steht, um das vorzügliche italienische Pesto wieder zu finden, dass er beim letzten Einkauf gefunden hat.

Oder die Verkäuferin erhält ein Signal zum Aufräumen, wenn die Kundin das Parfüm an die falsche Stelle zurückgestellt hat.

Es lassen sich unendlich viele "nützliche" Anwendungen denken. Die Hauskatze kann schneller gefunden werden oder der ins Gebüsch geschlagene Golfball. Das Hemd kann anfangen zu piepsen, wenn es gewaschen werden will. Besorgte Eltern können ihre Kinder mit Peilsendern ausstatten um sie zu finden. Dies mag ja noch eher drollig klingen. Doch sollen sich in Südamerika bereits über 2000 Personen Chips einpflanzen lassen, um sich vor Entführungen zu schützen.

## 2. WM-Tickets

Aktuell findet eine erste Massen-Anwendung von RFID-Chips statt. Auf den Eintrittskarten zum Confed-Cup und für die WM 2006 in Deutschland sind RFID-Chips angebracht.

Bekanntlich können die Tickets auch nur nach Voranmeldung erworben werden. Dabei muss sich der kaufwillige Fußballfan datenmäßig völlig entblößen. Jeder Antragsteller hat einen kompletten Datensatz einzureichen, mit Name, Geburtsdatum, Postanschrift, Nationalität, Kreditkarten- und Personalausweisnummer.

Die glücklichen Gewinner des Auswahlverfahrens bekommen einige Wochen vor dem Spiel Tickets zugeschickt, auf denen per RFID-Chip mit 64 Byte eine Seriennummer angebracht ist. Der RFID-Chip enthält also selbst keine personenbezogenen Daten. Mit dieser Technik kann man die Nummer auch ohne das Wissen des Kartenbesitzers automatisch auslesen und damit die bei der Bestellung hinterlegten Daten nachschlagen.

Von den elektronisch markierten Tickets verspricht sich der DFB nicht nur absolute Fälschungssicherheit, sondern auch Schutz gegen das nachträgliche Herausschmuggeln von Tickets aus dem Stadion, um zusätzlichen Besuchern unberechtigten Zutritt zu verschaffen.

Fragt sich, wer alles Kenntnis von den Daten erhalten soll. Offensichtlich sollen die Kartenbewerber vorher über die Polizeidatei „Gewalttäter Sport“ abgeglichen werden. Innenminister Schily hat davon gesprochen, dass eine „nationale Stelle“ geschaffen werden soll, bei der alle Informationen zusammenlaufen sollen. Daraus sollen „nationale Lagebilder“ entstehen.

Das Regierungspräsidium Darmstadt als zuständige Datenschutzbehörde hat keine Einwände erhoben. Auch wenn keine persönlichen Daten gespeichert sind, so ist doch über die Erkennungsnummer wenigstens im und um das Stadion eine Ortsfeststellung und Identifizierung durch Abgleich mit der Referenzdatei möglich.

Wie sieht es mit der Weitervermarktung der erhobenen Daten aus? Der Ticket-Bewerber muss ausdrücklich zustimmen, wenn seine Daten für Werbezwecke verwendet werden können sollen.

Das Organisationskomitee erzielt nach eigener Auskunft keine Einnahmen aus der Weitergabe der Daten. Die Daten sollen einen Tag nach dem Spiel gelöscht werden. Allerdings ist damit zu rechnen, dass dieses System auch im Rahmen der Fußball-Bundesliga genutzt werden wird – und ob es dann dabei bleibt, erscheint durchaus fraglich.

### 3. Neue biometrische Pässe

Auch die neuen Pässe mit biometrischen Merkmalen, die ab Herbst 2005 eingeführt werden sollen, enthalten einen RFID-Chip. Die Bundesregierung hat bestätigt, dass der Chip auch noch in einer Entfernung von bis zu 30m gelesen werden kann. Durch Verschlüsselung sei aber sichergestellt, dass Unbefugte „nach dem derzeitigen Stand der Technik“ nicht auslesen könnten. Allerdings hat die Bundesregierung noch im Februar geantwortet, dass noch nicht festgelegt sei, welche Stellen sonst noch die Ausleseberechtigung erhalten sollen.

### 4. Euro-Scheine

2003 wurde sogar berichtet, dass Europäische Zentralbank überlegen würde, auf den Euro-Scheinen RFID-Chips anzubringen. Auf diese Weise könnten echte Scheine von Blüten unterschieden werden.

## **III. Was sind die Gefahren?**

Die Gefahren für die Bürgerrechte lassen sich in vielleicht drei Punkten zusammenfassen:

1. Es finden leicht zu bewerkstellende und massenhafte Eingriffe in die informationelle Selbstbestimmung statt.
2. Die Möglichkeit zur anonymen Teilnahme am gesellschaftlichen Leben wird zusehends unmöglich.
3. Die Verknüpfung zwischen Identifizierungstechniken und Datensammlungen, die zur Zusammensetzung eines Bewegungs-, ja tendenziell eines Lebensbildes taugen, rückt immer näher.

### 1. Leichte und massenhafte Eingriffe

Die Erhebung von Daten ist ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Die Informationstechnologie ermöglicht viel kostengünstigere und massenhaftere Eingriffe als früher.

#### *Die gute alte Verfolgungsjagd*

Dies kann man sich etwa an alten Krimis verdeutlichen:

Wir kennen die Szenen aus ur-alten Krimis. Wenn der Verdächtige morgens aus dem Haus geht, sitzt sein Verfolger bereits in einem Auto an der Ecke, wo er die ganze Nacht gewartet hat. Wenn der Verdächtige in den Bus steigen, setzt sich ein Kollege zwei Bankreihen hinter ihn. Am Arbeitsplatz wird er von der Wohnung gegenüber beobachtet und wenn er nach Hause fahren, ist der Verfolger auch dabei.

In etwas neueren Filmen besteht die Kunst der Verfolger darin, eine Wanze im Auto zu platzieren. Der Peilsender funkt über Kilometer ihren Standort. Der Gejagte versucht das Auto zu wechseln, oder die Wanze zu entfernen, an einem anderen Fahrzeug anzubringen und in die falsche Richtung weiterfahren zu lassen.

Was in alten Filmen mit großem Aufwand inszeniert wird, wirkt heute schon liebenswert komisch, ist aber hoffnungslos antiquiert. Mit der neuen Technik muss kein solcher Personal-Aufwand mehr getrieben werden. Der Computer-Chip und die Rasterung der Datenbank übernimmt die Überwachungsaufgabe.

Denn es ist mit der RFID-Technik möglich in jedem Kleidungsstück, in jedem Etikett, Schmuckstück oder sogar unter der Haut einen Peilsender anzubringen, von dem sie nichts wissen und nichts merken. Der Chip kann jede Menge Informationen enthalten, die sie nicht kennen, und von denen Sie nicht kontrollieren können, wer sie wann ausliest.

Sie werden ständig von Videokameras erfasst. Sie sind über ihr Handy ständig abhörbar. Ich erinnere mich noch gut an den Film „Staatsfeind Nr.1“ von 1999 mit Will Smith in der Hauptrolle, in dem Gene Hackmann das Handy vom Hochhaus schmeißt, um nicht geortet werden zu können.

Der Mensch wird zur wandelnden Datenbank, die ständig persönliche oder unpersönliche, wichtige oder unwichtige Daten an ihnen unbekannte Personen und Institutionen abgibt.

## 2. Verknüpfung zwischen Gegenstand und Person

Richtig gefährlich wird die Geschichte, wenn der geortete und identifizierte Gegenstand mit einer bestimmten Person verknüpft werden kann, etwa weil sie den identifizierten Gegenstand an sich trägt. Dies geschieht etwa, wenn der gekaufte und mit einer EPC versehene Gegenstand auf einer Kundenkarte gespeichert und so mit einer Person verknüpft wird.

Oder wenn die Nummer auf der Eintrittskarte ins Fußballstadion mit der Bestelldatei mit Namen, Personalausweis- und Kreditkartennummer verknüpft wird.

Oder wenn die Meldungen eines RFID-Chips auf den neuen biometrischen Ausweispapieren an einer Polizeikontrollstelle oder Grenze mit dem Namen des Trägers des Ausweis verknüpft werden.

Damit werden zunehmend alle Lebensäußerungen nachverfolgbar, überwachbar und zusammensetzbar. Es kann ein Bewegungs-, Konsum- und Persönlichkeitsbild des Trägers der Kundenkarte, der Eintrittskarte oder des Personalausweises zusammengesetzt werden. Wir tragen dann bald alle so etwas wie eine „elektronische Fußfessel“, die den Aufenthaltsort des Gefangenen an die Polizei sendet, wenn der Gefangene die zugewiesene Wohnung verlässt.

Helmut Bäumler, der ehemalige Landesdatenschutzbeauftragte von Schleswig-Holstein sagte vor einiger Zeit:

*"RFID kann ein Horror-Thema werden, wenn die Kennzeichnung von Gegenständen benutzt wird, um Menschen auszuspionieren. Ich kann ja heute schon eine Verbindung zwischen Gegenstand und Person herstellen. Wenn ich diese Möglichkeit nutze, um die Wege von Menschen nachzuvollziehen, dann geht es uns bald nicht besser als den Rindviechern, die solche Chips bereits unter der Haut tragen und deren Wege man präzise nachvollziehen kann. Das sollte den Menschen eigentlich nicht passieren."*

Die Erstellung von Bewegungsbildern ist nach der Rechtsprechung des Bundesverfassungsgerichts zwar verboten. Doch was nützt dieser allgemeine Rechtssatz, wenn überall die Möglichkeiten des Zugriffs, der Verknüpfbarkeiten und auch der kommerziellen Interessen wachsen?

Es wird immer versichert, dass die RFID-Chips auf den Etiketten nur der Prozeß-Steuerung in der Zulieferkette dient. Ebenso sollen die Eintrittskarten nur der Sicherheit in den Stadien dienen. Und die biometrischen Daten sollen fälschungssicher sein und uns vor Terroristen schützen.

Doch wie schnell die Begehrlichkeiten der Sicherheitsbehörden wachsen, zeigt ein Interview in der Freien Presse, dass der sächsische Innenminister de Maiziere letzten Freitag gegeben hat. - Er sagte: Die Nutzung der Maut-Kontrollen für die Verfolgung von LKWs zur Bekämpfung der Kriminalität dürften nicht länger ein Tabu sein. Es müsse erlaubt werden, Autokennzeichen zu fotografieren, die dann von der Polizei genutzt werden können. Dies steht übrigens schon in der

sächsischen Koalitionsvereinbarung zwischen CDU und SPD.

Unter den Autobahnbrücken sind Kameras angebracht, die nicht nur die Signale der On-Board-Units der LKW zur Kontrolle der Mautzahlungen empfangen, sondern alle PKW fotografieren. Bei der Einführung der Mautkontrollen zum 1. Januar hieß es noch, dass diese Daten ausschließlich der Mauterfassung dienen. Jetzt fordert die Maiziere deren polizeiliche Nutzung.

Hier zeigt sich wieder einmal: Sind die Daten erst einmal erhoben, melden sich schnell Polizei, Verfassungsschutz und private Verwerter, die dann bald auch Zugriff erhalten. Sind die RFID-Chips erst einmal flächendeckend eingeführt, dann wette ich, dass auch dann bald die Rufe nach einer polizeilichen Nutzung laut werden.

#### **IV. Was ist zu tun?**

Zunächst: Angesichts der alles in allem geräuschlosen Entwicklung der Überwachungsgesellschaft in den letzten Jahre habe ich wenig Hoffnung, dass sich die Bürgerinnen und Bürger ihrer zunehmend lückenlosen Erfassung und Verdattung aller Lebensbereiche entgegenstellen.

Dennoch: Es muss Öffentlichkeit hergestellt werden und das Bewusstsein für die Gefahren der Informationsgesellschaft gestärkt werden.

Folgende Grundsätze können formuliert werden:

1. Der Grundsatz der Zweckbindung und der Datensparsamkeit: Es dürfen nur die Daten erhoben werden, die für den Zweck erforderlich sind – und nicht mehr.
2. Jeder, dessen Daten erhoben und verarbeitet werden, muss davon Kenntnis nehmen können. Eine geheime und unbemerkte Auslesung von RFID-Chips darf nicht stattfinden.
3. Im öffentlichen und privaten Leben muss der Grundsatz der Anonymität gewährleistet werden. man muss am Leben teilnehmen können, ohne dauernd zur Hinterlassung von Datenspuren verpflichtet zu werden. Die Kunden müssen das Recht zur Entfernung von RFID-Chips erhalten.
4. Die Verknüpfung zwischen Gegenstand und Person muss verboten werden. Die Erstellung von Persönlichkeitsbildern muss verhindert werden.
5. Jeder muss das Recht haben, Auskunft und Löschung der bei einer öffentlichen oder privaten Stelle vorhandenen Daten mit Aussicht auf Erfolg zu verlangen.

Ich danke Ihnen für Ihre Aufmerksamkeit.