

RFID – moderne Technik mit Tücken

Frauke Mahrt-Thomsen

Ich möchte mich zu allererst dafür bedanken, dass ich als Referentin zu dieser Tagung eingeladen wurde. 40 Jahre lang war ich in öffentlichen Bibliotheken in dieser Stadt tätig. Weiterhin aktiv bin ich bei Akribie, dem Arbeitskreis Kritischer BibliothekarInnen. Akribie setzt sich seit zwanzig Jahren mit der Beziehung von Bibliothek und Gesellschaft auseinander. Unsere Hauptfragen lauten: Welche Bibliotheken wollen wir? Was ist die gesellschaftliche Verantwortung des Bibliothekars? Welcher bibliothekarischen Ethik sollten wir im Berufsalltag folgen?

Bereits 2006 hat Akribie während des BibliothekarInnentages in Dresden (wir schreiben und sprechen dies immer mit großem I) eine Veranstaltung durchgeführt mit dem Titel: „Der überwachte Mensch: RFID in Bibliotheken. Eine Diskussion über Technik, Bürgerrechte und bibliothekarische Verantwortung“. Sie fand jenseits des offiziellen Konferenzprogrammes statt, mit reger Beteiligung von BürgerInnen, die ihre Sorge über den wenig kontrollierbaren Einsatz dieser komplexen neuen Technologie zum Ausdruck brachten. Auf der am nächsten Tag im Konferenzzentrum angesetzten Veranstaltung zum Thema RFID waren unsere kritischen Nachfragen weniger willkommen. Man war eher daran interessiert, die schöne neue Funk-Welt der Stadtbibliothek München in positiven Farben gemalt zu bekommen.

2007 hielt Ulrike Verch, heute Professorin an der Hochschule für Angewandte Wissenschaften Hamburg, auf dem Leipziger Bibliothekskongress ihren Vortrag „Selbstklebend, selbstverbuchend und auch selbstverpflichtend? Rechtliche Rahmenbedingungen für den Einsatz von RFID-Chips in Bibliotheken“.

<http://www.opus-bayern.de/bib-info/volltexte/2007/305/pdf/verch-leipzig-2007.pdf>

Ihr Beitrag informierte erstmals darüber, wie intensiv und kritisch amerikanische KollegInnen und Bürgerinitiativen über die RFID-Technologie diskutieren.

Der Blick in die Vereinigten Staaten ist auch deshalb für uns spannend, weil es dort Beispiele gibt, dass man sich aus gesellschaftspolitischen Gründen bewusst gegen

RFID entscheidet. So demonstrierten Bürger im Jahre 2004 in San Francisco gegen den Einsatz von RFID in ihrer Bibliothek, und bis heute hat die San Francisco PL - trotz vorhandener Startgelder - diese Technologie nicht eingeführt. Wie mir noch im letzten Jahr eine Kollegin aus San Francisco auf dem Kongress der American Library Association oder ALA in Chicago versicherte, sind nicht nur die Bürger, sondern auch die KollegInnen der San Francisco Public Library weiterhin strikt gegen die Einführung von RFID.

Die Electronic Frontier Foundation (EFF) in den USA erklärt auf ihrer Website: "EFF ist sehr gegen den Einsatz der RFID-Technologie in Bibliotheken ... Bibliotheken, Schulen, die Regierung und der private Geschäftssektor wenden Radio Frequenz-Identifikations-Tags an oder RFID – eine Technologie, die benutzt werden kann, um den physischen Ort jedes einzelnen Objekts anzuzeigen, auf dem sich die Tags befinden. Während RFID eine bequeme Methode ist, Dinge zu verfolgen, ist sie eine ebenso bequeme Methode, um etwas weit weniger Ehrenwertes zu tun: Menschen und ihre Aktivitäten zu verfolgen durch die Dinge, die ihnen gehören. EFF arbeitet daran zu verhindern, dass die Ausbreitung dieser Technologie den Schutz der Privatsphäre und der Freiheit bedroht."

(Übers. v. d. A., Originaltext unter:

<http://w2.eff.org/Privacy/Surveillance/RFID/libraries/> und:

<http://w2.eff.org/Privacy/Surveillance/RFID/>)

Für die ALA hat der Schutz der Privatsphäre und der Vertraulichkeit der Leser seit jeher einen hohen Stellenwert. Unterstützt durch viele Arbeitsgruppen und Komitees verabschiedete sie neben allgemeinen Datenschutzrichtlinien bereits 2005 eine Resolution (*Resolution on Radio Frequency Identification (RFID) Technology and Privacy Principles*)

<http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=85331>

und 2006 Leitlinien oder Guidelines zum Einsatz von RFID in Bibliotheken (*RFID in Libraries: Privacy and Confidentiality Guidelines*),

<http://www.ala.org/Template.cfm?Section=ifresolutions&Template=/ContentManagement/ContentDisplay.cfm&ContentID=85331>,

in denen der Vertrauens- und Datenschutz als Leitprinzipien des bibliothekarischen Handelns verankert werden (*Basic Privacy & Confidentiality Principles*). Eine der Empfehlungen in diesen *Guidelines* lautet, dass die KollegInnen auf Wunsch eines Bibliotheksbenutzers neben der RFID auch eine alternative Verbuchungsmöglichkeit bereit stellen sollten – ein für die BRD geradezu revolutionärer Gedanke, dem wir entschieden mehr Geltung verschaffen sollten.

Dabei stimmt er mit dem Kern einer Entscheidung des Bundesverfassungsgerichts aus dem Jahre 2006 überein, dass eine freiwillige Zustimmung eines Bürgers zu einem bestimmten Verfahren – bei der Verfolgung grundlegender Bedürfnisse - nur vorliegt, wenn man ihm eine Alternative anbietet, es sei denn, es gibt eine gesetzliche Grundlage. Da es in Deutschland fast keine Bibliotheksgesetze gibt und auch in Zukunft mit Sicherheit in keinem Bibliotheksgesetz die Art der Ausleihorganisation festgeschrieben sein wird, bewegen sich die Bibliotheken, wie ein Mitarbeiter des Bundesdatenschutzbeauftragten mir sagte, mit ihrer Festlegung auf eine ausschließliche Form der Ausleihverbuchung „auf dünnem Eis“ (Entscheidung des Bundesverfassungsgerichts vom 23.10.2006, Aktenzeichen 1BvG 2027/02, Amtliche Entscheidungssammlung des BVerfG, Bd. 113, S. 273-348; s. auch § 4 und § 4a des Bundesdatenschutzgesetzes).

Auf dem BibliothekarInnentag in Erfurt 2009 habe ich im Rahmen eines Rückblicks auf zwanzig Jahre Akribie-Arbeit auch ein Kurzreferat zu dem Thema „RFID in Bibliotheken“ gehalten und wir sind damals angesichts der weiterhin bestehenden Risiken der RFID-Technik und der gesellschaftlichen und sozialen Folgeerscheinungen ihres Einsatzes zu dem Schluss gekommen: „Akribie meint, die bibliothekarische Ethik gebietet, auf den Einsatz von RFID in öffentlichen Bibliotheken zu verzichten.“

Als Motto soll mir die Definition von ‚Verantwortung‘ dienen, wie sie die *Gesellschaft für Informatik* (abgekürzt: GI, nicht zu verwechseln mit der *Deutschen Gesellschaft für Informationswissenschaft und Informationspraxis*, abgekürzt: DGI) gefunden hat:

„Da Menschen die Folgen ihres Handelns nicht immer abschätzen können, sollten Entscheidungen stets so getroffen werden, dass sie widerrufbar sind und korrigierbar bleiben. Damit wird der Handlungsspielraum aller Beteiligten erweitert und nicht von vornherein alternativlos eingeschränkt. Gemeinschaftliches Handeln bedarf zusätzlich zur individuellen der gemeinschaftlichen Reflexion. Gemeinschaftliche Verantwortung beruht auf der Möglichkeit, mit Vor-Sicht künftige Handlungen, die sich nicht oder nur teilweise an Erfahrungen und daraus entwickelten Normen orientieren können, gemeinschaftlich zu bedenken.“ (aus: Gewissensbisse, S.122)

Weltweit sollen bereits mehr als 2500 Bibliotheken mit RFID arbeiten und über 500 Millionen Chips in Bibliotheken im Einsatz sein. Die Stadtbibliotheken in München, Wien, Hamburg, Stuttgart, Halle und Münster arbeiten schon längst mit RFID, ebenso die Universitätsbibliotheken in Karlsruhe, Berlin (TU und HU), viele bayrische Fachhochschul-Bibliotheken und die Bücherei des Vatikans.

In den öffentlichen Bibliotheken Berlins wird die RFID-Technik flächendeckend bis Ende 2012 eingeführt. Die lokalen oder regionalen Datenschützer sahen sich nicht berechtigt, ihre Zustimmung zur RFID-Einführung zu verweigern, da sich auf den Medien- oder Leserausweis-Chips keine Klartext-Angaben, sondern nur Nummernfolgen befinden, die erst in den internen Rechnern der Bibliotheken zusammengeführt und entschlüsselt werden.

Wie die Projektmanagerin der Stadtbibliothek München berichtet, verbuchen dort inzwischen ca. 97 % der Benutzer ihre Medien an den Verbuchungsgeräten selbst und sind zufrieden, dass sie ihre Bücher rund um die Uhr in die RFID-Rückgabeautomaten stecken können.

Im Falle der RFID-Einführung in den Berliner öffentlichen Bibliotheken wird es keine generelle Zustimmung oder Ablehnung des obersten Datenschützers geben, sondern er begleitet die vom VÖBB (Verbund der öffentlichen Bibliotheken Berlins) geplante RFID-Einführung in den verschiedenen Phasen der Entwicklung. Derzeit prüft der zuständige Mitarbeiter das nach §5 Abs. 3 Satz 1 BLDnDSG vom VÖBB vorgelegte

Sicherheitskonzept. Vielleicht kann Herr Dr. Dix zu dem Stand des Verfahrens hier noch einige Anmerkungen machen.

In unserer Fachzeitschrift ist in einem Bericht über die Neueröffnung einer Stadtbibliothek nachzulesen, dass die Einführung der RFID-Selbstverbuchung „ein Muss für alle Kunden“ sei (BuB H.3/2009, S.194), und auf der Auftaktveranstaltung zur RFID-Einführung im letzten Sommer in Berlin verkündete der Geschäftsführer der Ständigen Konferenz der Leiterinnen und Leiter der Berliner Öffentlichen Bibliotheken: „Ich persönlich finde RFID ja relativ unspektakulär. Und zwar so unspektakulär wie das Atmen. Man kann viel über das Atmen reden, aber man kann nicht darauf verzichten. Zumindest bekommt es einem schlecht, wenn man darauf verzichtet. Das können Sie ja mal im Selbstversuch testen.“ (in: Technologische Innovation ..., S.14)

Warum also diese Vorbehalte von Akribie?

Wir denken, es reicht nicht aus, sich auf die von interessierten Propagandisten gemachten Aussagen zu verlassen, sondern man muss genauer hinschauen, wie RFID technisch und gesellschaftlich funktioniert. Auch im Bereich der geschlossenen Systeme in Bibliotheken mit ihren passiven, nicht sendefähigen Chips sind Risiken nachweisbar. Über den engeren Datenschutz hinaus müssen die sozialen Auswirkungen und politischen Zusammenhänge bedacht werden.

Ich möchte hier gleich zu Anfang die Aktivistin des Bürgerrechtsvereins FoeBuD e.V. (*Verein zur Foerderung des bewegten und unbewegten Datenverkehrs*), Rena Tangens, zitieren:

„‘Schöne neue Welt‘, Aldous Huxleys Vision eines Staates, in dem Menschen angenehm konsumieren, aber perfekt manipuliert in geistiger Unfreiheit leben, ist weitaus moderner als ‚1984‘, George Orwells Schilderung eines totalitären Überwachungsstaates. Wir sollten aber nicht annehmen, dass der Überwachungsstaat sich damit überlebt hätte. In den letzten Jahren sind die bürgerlichen Freiheiten in Deutschland immer weiter eingeschränkt worden. Einige Stichworte: Vorratsdatenspeicherung sämtlicher Kommunikationsverbindungen, Großer Lauschangriff, Verschärfung der Polizeigesetze der Länder mit Rasterfahndung, Videoüberwachung im öffentlichen Raum und Platzverweis, Kfz-Zeichen-Erfassung an Autobahnen, biometrische

Merkmale in Reisepässen, gespeichert auf RFID-Chip, Ausweitung der DNS-Speicherung etc. Kaum eine Überwachungsmaßnahme, die nicht mit dem angeblich drohenden ‚internationalen Terrorismus‘ begründet würde.

Fast alle diese Maßnahmen zielen allerdings nicht auf Kriminelle oder unmittelbar Tatverdächtige, sondern betreffen Millionen völlig unbeteiligter Bürgerinnen und Bürger. Die Unschuldsvermutung wird faktisch ausgehebelt. Den meisten Menschen ist klar, dass ihre Privatsphäre angegriffen wird, wenn sie Objekt von Überwachung werden (z.B. Videoüberwachung oder Abhören des Telefons) oder wenn ihre persönlichen Geheimnisse an die Öffentlichkeit gezerzt werden. Doch dass ihre Privatsphäre auch verletzt werden kann durch die ständige Sammlung, Auswertung und Nutzung einer Vielzahl von Daten, die bei alltäglichen Handlungen anfallen – dieses Bewusstsein ist erst langsam im Entstehen.“

<http://foebud.org/datenschutz-buergerrechte/linsengericht>

Das FOEBuD-Mitglied *padeluum* sagte mir in einem Telefongespräch: Das Anlegen von solchen Dateien „ist immer böse, ist falsch, jede zentrale Datensammlung kann missbraucht werden.“

Was ist das Neue an der RFID-Technologie, z.B. gegenüber den auch mit einer Zahlenfolge arbeitenden Barcodes? RFID steht für Radiofrequenz-Identifikation, Daten werden mittels Radiowellen, ohne Berührung und ohne Sichtkontakt übertragen. Ein RFID-System umfasst einen Transponder, einen winzigen Computerchip mit einer Antenne, der in ein Klebeetikett oder eine Plastikkarte integriert werden kann, sowie ein Sende-Empfangs-Gerät und ein im Hintergrund wirkendes IT-System. Auf jedem Chip ist eine weltweit eindeutige Seriennummer verzeichnet, jedes Objekt, das diesen Chip trägt, z.B. eine Obstkiste oder ein Joghurtbecher, ist damit weltweit identifizierbar und potentiell auch der Käufer, wenn er den Becher mit Bank- oder Kundenkarte bezahlt. Die Funkübertragung erfolgt geräuschlos und nahezu unsichtbar, da sich auch die Lesegeräte in manchen Fällen nur schwer erkennen lassen. Selbst ein versteckter Einbau in Türrahmen, Fußböden oder Schuhen ist kein Problem.

FoeBuD e.V. schreibt, „dass die Chips so klein und billig sind, dass sie bald in jeden Jackenkragen, jede Schuhsohle eingepflanzt werden können. Dort lassen sie sich auch nicht mehr entfernen, ohne das Produkt (z.B. den Schuh) zu zerstören. Das

bedeutet: jede Lese-Antenne, an der Sie vorbei kommen, erfasst ihren Chip aufs Neue (vielleicht im Bus, an der Tankstelle, im nächsten Supermarkt. Die uns bekannten ‚Deaktivatoren‘ haben das nicht verhindert. Unser Einkaufsverhalten wird ausspioniert, ohne dass wir es merken. Z.B. wer steht wie lange vor welchem Regal? Welche Werbung kann man diesem Kunden gezielt zuschicken?“

[\(http://www.foebud.org/rfid/das-problem/\)](http://www.foebud.org/rfid/das-problem/)

Lesegeräte sind inzwischen so billig geworden (20 €), dass sie jeder Technik-Fan kaufen und damit herumexperimentieren kann. Wenn er zum Beispiel mit seinem Lesegerät neben einem Bibliotheksbenutzer steht, der seine gerade entliehenen in Bücher in der Tasche trägt, kann er die Chip-Nummern auslesen und anhand der *Application Family Identifiers (AFI)* erkennen, dass es sich um Bibliotheksmedien handelt.

Er kann sogar anhand der ISIL(International Standard Identifier for Libraries and Related Organizations) –Sigelnummern, die nach dem Dänischen Datenmodell in die Seriennummern der RFID-Chips integriert werden, exakt feststellen, aus welcher einzelnen Bibliothek oder welchem Bibliotheks-System die Medien stammen. Wenn sich eine dieser Bibliotheken in der Nähe befindet, kann er anhand mehrfach wiederkehrender Nummern eventuell sogar herausfinden, zu welcher Bestandsgruppe die entliehenen Bücher gehören - wenn die Bibliothek nicht darauf geachtet hat, die Nummern nicht fortlaufend zu vergeben, sondern nach dem Zufallsprinzip zu streuen. (Hinweis von Mitarbeitern des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein).

Völlig realistisch und mehrfach beschrieben ist das Missbrauchs-Szenario, das Ulrike Verch schildert: „Wenn ich beispielsweise in einem Kaufhaus, das bereits RFID-Kundenkarten einsetzt, an der Kasse zahlen möchte und dazu bequemerweise meine Tasche, in der sich mein Portemonnaie befindet, vor das RFID-Lesegerät halte, so erkennt dieses anhand des eindeutigen Application Family Identifiers (AFI), dass ich auch Bibliotheksbücher bei mir trage. Dem Kaufhaus wäre damit die Gelegenheit eröffnet, in meiner dort geführten Kundenkartei den Vermerk „Bibliotheksnutzerin“ zu hinterlegen. Die Möglichkeit, persönliche Profile zu erstellen, sobald die mitgeführten und mit RFID-Chips bestückten Gegenstände mit Personendatenbanken verknüpft

werden, nimmt aufgrund der Radiofrequenztechnik und der vielen elektronischen Datenspuren, die wir im Alltag hinterlassen, unweigerlich zu.“

Dass auch in Berliner Kaufhäusern und Geschäften die Lesegeräte auf RFID-Chips aus Bibliotheken reagieren, wurde mir erst vor kurzem von einer Benutzerin der Universitätsbibliothek der TU bestätigt.

Ein weit größeres Sicherheitsloch bei bestimmten RFID-Anwendungen, das sich auch gravierend auf Bibliotheken auswirken könnte, ist schon vor 2-3 Jahren von Mitgliedern des Chaos Computer Clubs und Forschern aus amerikanischen und niederländischen Universitäten aufgedeckt worden. Es handelt sich um das meistgenutzte Chip-System Mifare (Hersteller: NXP und Infineon Technologies), von dem weltweit bereits ca. 1 Milliarde Karten und mehr als 5 Millionen Lesegeräte verkauft wurden. Das Mifare-System wird zum großen Teil auch in Bibliotheken eingesetzt, so bereits in München und in Zukunft auch in den Berliner öffentlichen Bibliotheken, in der Version Mifare Mini.

Auf dem Hackerkongress im Dezember 2007 und in einem Aufsatz im Heft 8/2008 der Zeitschrift c't wurde vorgestellt, wie der Algorithmus von Mifare „gebrochen“, d.h. analysiert und ein systematischer Fehler gefunden werden konnte, der die Verschlüsselung praktisch nutzlos macht. „Die Sicherheit des Algorithmus“, so das Fazit der Forscher, sei „nahe Null...Die Schwächen von Mifare stecken nicht nur im Abfangen der Schlüssel von Lesegeräten. Die Karten können auch vergleichsweise einfach ‚geklont‘ oder kopiert werden. Wenn keine anderen Sicherungsmechanismen verwendet werden, können sich Personen mit dem Duplikat einer RFID-Karte Zugang zu Gebäuden oder anderen Sicherheitsbereichen verschaffen.“

In einem YouTube-Video auf der Website ([http://golem.de/087\(60973.html\)](http://golem.de/087(60973.html))) zeigt der Forscher Bart Jacobs von der Radboud-Universität in Nijmegen vor laufender Kamera, wie er eine Mifare-Karte dupliziert und damit gratis die Londoner U-Bahn benutzt. Nach den Angaben des an der Entschlüsselung beteiligten Forschers Karsten Nohl funktioniert der Angriff auch mit dem verbesserten Nachfolger Mifare Plus, sofern nicht ebenfalls die Lesegeräte auf den ‚Plus‘-Standard umgerüstet wurden. Mifare Plus verwendet eine andere Verschlüsselung, doch für die Kommunikation mit den

alten Lesegeräten fällt er auf den unsicheren Algorithmus der Vorgängerversion zurück.

Bei Mifare Mini handelt es sich um eine abgespeckte Version von Mifare für Anwendungen mit reduziertem Speicherbedarf. Auf meine Frage an den Technik-Experten des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, ob diese Version von Mifare noch sicher sei, bekam ich die Antwort: „Nach unseren Informationen ist die Kryptographie dieses Chips ebenfalls gebrochen.“ Die Verarbeitungsdauer für einen Angriff liege „auf einem Standard-PC ohne besondere Hardware und ohne vorberechnete Tabellen bei etwa 200 Sekunden.“ Das könne er jedem Schüler in etwa 20 Minuten beibringen.

Wenn es für einen Schüler kein Problem ist, die Mifare-Karte zu entschlüsseln, dann kann er nach dem Beispiel von Bart Jacobs unbemerkt, im Vorbeigehen eine andere Lesernummer einfangen und mit seinem Ausweis-Duplikat Bücher ausleihen, mit denen der ‚echte‘ Leser belastet wird, der unter Hinweis auf die Sicherheitslücken vielleicht beschließt, nie mehr diese Bibliothek zu benutzen. Der Missbrauch ist in Zukunft umso einfacher, da der Leser nicht mehr an der Verbuchungstheke einem Bibliotheksangestellten gegenüber treten muss, dem sofort der falsche Ausweis oder der Namensmissbrauch auffallen würde, weil er unter Umständen den echten Karten-Inhaber kennt.

Erst vor wenigen Tagen hörte ich von dem für die RFID-Planung in den öffentlichen Bibliotheken verantwortlichen Kollegen als Begründung für den Wunsch nach Mifare-Karten: „Die sind viel fälschungssicherer als Barcode-Ausweise, weil man die Barcodes ja jederzeit kopieren und damit unbeobachtet am Selbstverbuchungsautomaten ausleihen kann.“ Ich glaube, da unterschätzt er das Potential der vielen Computer-Freaks in dieser Stadt.

Die in den Bibliotheken verwandten Transponder sind bisher in der Regel passiv und können nur dank des Magnetfeldes des Lesegeräts bewogen werden, ihren Nummerncode zu senden. Das IT-System entschlüsselt den Code und verknüpft ihn mit Informationen, die in der Datenbank hinterlegt sind. Das Wissen bzw. die Intelligenz des Systems liegt dabei nicht im Transponder, sondern in den Datenbanken.

Längst gibt es aber auch „intelligente“ Transponder oder „smart“ Chips, die eine eigene Batterie haben, eine große Menge von Informationen speichern und Signale über eine beträchtliche Distanz senden, empfangen und verarbeiten können. Passive, aber zunehmend auch „smart“ Chips werden bereits in großen Teilen der Arbeitswelt und des Alltags eingesetzt, die Anwendungsbereiche lassen sich kaum noch überblicken.

Hier einige Beispiele:

- Logistik (Güter-, Transportbehälter-, Päckchenversand weltweit, DHL)
- Transportwesen (elektronische Mautsysteme)
- Gepäcksteuerung auf Flughäfen
- Produktion und Fertigungsplanung: Computer Integrated Manufacturing (CIM), Schwerpunkt: Automobilindustrie (BMW, Volkswagen)
- Personennahverkehr (London, Niederlande, Verkehrsverbund Rhein-Ruhr)
- Schlüsselsysteme, Wegfahrsperren
- Strom-Verbrauchsdaten-Erfassung
- Gefahrgutlagerung
- Gesundheitswesen, Pharmaindustrie, Kranken- und Altenpflege (AAL = Ambient Assisted Living)
- Handel und Gewerbe (Wal-Mart und Zuliefer-Firmen, Metro-Group („Future-Store“), Warenlager-Verwaltung, Rabatt- und Kundenkarten)
- Wartungs- und Reparaturmanagement (Airbus A380)
- Forstwirtschaft (Cambium-Forstbetrieb Odenwald), Baumpflege
- Freizeit (Ticketsysteme, Fahrkarten, Ski-Pässe)
- Sport (Marathonläufer: Chip im Schuh)
- Firmen- / Mitarbeiter-Ausweise
- Berufskleidung
- Verwaltung (US-Sozialversicherungs-Akten)
- Meldewesen (BRD-Reisepässe, Personalausweise ab Herbst 2010)
- Tiere (Hunde, Katzen, Rinder: Anhänger im Ohr, Kapseln im Magen)
- Menschen (Identifizierung von Kriminellen oder Mitgliedern von Beach-Clubs und Security-Firmen durch Implantate unter die Haut, vorbeugende Zahn-Implantate zur Identifizierung der Betroffenen im Falle einer Katastrophe).

Die RFID-Chips verhalten sich zum Teil wie Schnüffelchips, weil sie - oft unbemerkt und ungewollt - etwas über uns verraten, unsere Konsumgewohnheiten, unseren Aufenthaltsort, unsere Kommunikation, unsere Vorlieben und Abneigungen, möglicherweise sogar die Farbe und Größe unserer Unterwäsche - der Versuch eines

weltweit agierenden Kleiderherstellers, Damenunterwäsche mit RFID-Chips zu versehen, wurde nur dank der FoeBuD-Kampagne „I'd rather go naked“ – „Lieber gehe ich nackt“ vereitelt.

Durch die ‚smart‘ Chips werden Alltagsgegenstände ‚intelligent‘, die universelle Verfügbarkeit von Informationen für uns im Internet verlagert sich auf bewegliche Dinge und Objekte in der realen Welt. Die RFID-Technologie ist die entscheidende Voraussetzung für das „Internet der Dinge“ (Internet of Things, abgekürzt: IoT), in dem sich die Dinge direkt austauschen und möglicherweise eigenständig ihren Weg suchen, da sie und die sie umgebende Netzstruktur ‚wissen‘, wohin sie müssen. Waren und Objekte aller Art werden weltweit vernetzt, identifizierbar und handlungsfähig gemacht.

Die Auswirkungen auf weite Bereiche von Wirtschaft, Verwaltung, Wissenschaft und insbesondere auf die Arbeitswelt sind enorm. Im Produktionsprozess ist es immer öfter so, dass nicht der Arbeiter bestimmt, was die Maschine macht, sondern der Arbeiter bekommt über ‚intelligente‘ Geräte die Anweisungen vom RFID-gesteuerten System. Der Mensch wird zum Befehlsempfänger, um prozessoptimierte Handgriffe zu tun, die heute noch zu kompliziert für eine Automatisierung sind, sagen Alfons Botthof und Marc Bovenschulte, in ihrer Studie „Das ‚Internet der Dinge‘. Die Informatisierung der Arbeitswelt und des Alltags“.

Die Studie kommt zu dem Schluss, dass RFID eine Rationalisierungstechnologie ist, die von den Unternehmen meist ‚schleichend‘ eingeführt wird, ohne rechtzeitige Information und Einbeziehung der Arbeitnehmer, und dass sie eine massive Veränderung oder den Wegfall vieler Arbeitsplätze bewirkt.

Die Logik hinter der RFID-Einführung besteht aber nicht nur in der Wegrationalisierung von Stellen, sondern in der Kontrolle der logistischen und Arbeitsprozesse. So können mit Hilfe der RFID auch Personen im Arbeitsprozess zeitlich und örtlich erfasst, verknüpft und kontrolliert werden, bis hin zur genauen Zeiterfassung für bestimmte Arbeitsschritte und Pausen. Diese Daten bilden eine hervorragende Grundlage für Personalentscheidungen bei der nächsten Rationalisierungswelle, Daten-

schutzauflagen wie Anonymisierung sind in diesen Verfahren oft gar nicht vorgesehen.

Auf der anderen Seite wird ein enormes Wachstum der RFID-Technologie-Anwendungen vorausgesagt und damit auch das Ansteigen der Arbeitsplätze in diesen Bereichen. Die zuständige Abteilungsleiterin beim Berliner Wirtschaftssenat berichtet: „Die Analysten ... prognostizieren beispielweise eine Entwicklung des Weltmarktes für RFID-Anwendungen von ca. 5 Mrd. Euro im Jahr 2007 auf über 16 Mrd. Euro im Jahre 2016. In Deutschland wird der RFID-Markt im gleichen Zeitraum ebenfalls wachsen, wobei jährliche Zuwachsraten von durchschnittlich 19 % erwartet werden.“ Sie ergänzt, dass diese Zahlen „selbstverständlich“ vor der Wirtschaftskrise erhoben wurden, und es sei eher zweifelhaft, ob sie erreichbar sind, aber „die Tendenz ist sicher richtig“. (in: Technologische Innovation ..., S.9)

Die RFID-Lobby veröffentlicht Zahlen über die „RFID-beeinflusste Wertschöpfung in Deutschland“, diese habe im Jahre 2004 3,4 Mrd. Euro betragen und werde bis 2010 auf 62,14 Mrd. Euro steigen. („Basiswissen RFID“, S.11) Was bedeuten diese Zahlen? Ist damit der Wert aller Produkte gemeint, die mit Einsatz von RFID-Transpondern hergestellt und vertrieben werden? Wurde der Wert der eingesparten Arbeitsplätze mit hinein gerechnet, und wenn ja, in welcher Höhe?

Auch auf europäischer Ebene wird die neue Technologie nachhaltig gefördert. So veröffentlichte die EU-Kommission am 19.6.2009 die Erklärung: „Internet der Dinge – ein Aktionsplan für Europa“, in der sie ein ganzes Szenario von Maßnahmen entwickelt, um die Verbreitung der neuen Technologie abzusichern.

Anträge in Millionenhöhe an die sonst oft schwer zugänglichen Fördertöpfe der EU (z.B. an EFRE, den Europäischen Fonds für Regionale Entwicklung) haben eine gute Chance, binnen weniger Monate bewilligt zu werden, wenn es sich um die Einführung von RFID handelt, das zeigen mehrere Berliner Beispiele. So wurden 2009 neben der RFID-Einführung in den öffentlichen Bibliotheken, die den schönen Projektnamen TENIVER (Technologische Innovation in der Informationsversorgung) bekommen hat, auch EFRE- Gelder für RFID-Anwendungen in der UB der Humboldt-Universität bewilligt und für das Projekt „POSEIDON – Positions- und kontextintensi-

ve Informationssysteme für Museen zur Demonstration des Potenzials der RFID-Technik“.

Mir fiel auf, dass bei dem Projektnamen TENIVER der Hinweis auf die Bürger gestrichen wurde, der bei der Auftaktveranstaltung im Mai 2009 noch sehr betont wurde. Dort lautete das Motto: „Technologische Innovation als Stärkung der Bürgerkommune“.

Die deutsche RFID-Lobby ist seit Jahren gut aufgestellt. 2005 wurde das ‚Informationsforum RFID e.V.‘ gegründet, mit dem Ziel, „das Zukunfts- und Innovationspotenzial der Radiofrequenz-Identifikation (RFID) stärker in das Bewusstsein der Öffentlichkeit zu rücken und den Einsatz der zukunftsweisenden Technologie durch einen offenen Dialog zu fördern.“ (Basiswissen Internet der Dinge, S.19) Das Informationsforum hat sein Domizil in dem äußerst repräsentativen Haus Dorotheenstraße 37 gefunden, im obersten Stockwerk, sozusagen mit direktem Blickkontakt zum Regierungsviertel. Zu den Mitgliedern des Informationsforums gehört die Crème der Produzenten, Anwender und Dienstleister der RFID-Branche: IBM, Siemens, Hewlett-Packard, Intermec (Systementwickler), Bitkomm (Berufsverband der Informations-, Telekommunikations- und Medienwirtschaft), Volkswagen, Metro Group, Henkel, Proctor & Gamble, DHL, Oracle (Software- und Systementwickler), BVL (Bundesverband Logistik, T-Systems (RFID-Lösungen für Groß-Anwender), GS1 Germany (Rationalisierungs- und Standardisierungs-Verband) und die Fraunhofer-Gesellschaft (industriennahe, anwenderorientierte Forschungsgesellschaft).

Ein Problem wird vom Informationsforum immerhin als „noch nicht endgültig geklärt“ bezeichnet: die Frage der Entsorgung. Die Chips sind Sondermüll, da sie verschiedene Metalle enthalten, und bei den angestrebten, exponentiellen Steigerungsraten der Verwendung von RFID-Chips bei Konsumgütern aller Art ist das Entsorgungsproblem keine Bagatelle. Jetzt hofft man auf die Fortschritte in der Materialforschung, die Polymertechnologie soll Entlastung bringen, da Polymere weder Metalle noch Silizium enthalten.

Eine weitere Gefährdung bei dauerhaftem und flächendeckendem Einsatz von RFID ist die mögliche Strahlenbelastung. Bei ständiger Exposition von RFID-Strahlen gel-

ten ähnliche Folgerisiken wie beim Einsatz von WLAN. In Pariser Bibliotheken soll WLAN wegen der gesundheitlichen Beschwerden mehrerer Bibliothekarinnen abgeschaltet worden sein. Im Informationsforum RFID wird immerhin eingeräumt: „Das Strahlungsthema ist die große Unbekannte.“

Das sind jedoch Fragen, die die Vertreterin des Berliner Wirtschaftssenats nicht bewegen, als sie bei der Auftaktveranstaltung zur RFID-Einführung euphorisch die Ausweitung des Marktes für Wireless-Anwendungen, insbesondere im Bereich RFID- und NFC (Near Field Communication)-Technologien in den letzten Jahren in Europa, Deutschland und in der Region Berlin-Brandenburg schildert. Sie fährt fort: „Wir wissen, dass sich RFID schneller entwickelt, wenn erfolgreiche Pilotprojekte die Vorteile für alle Beteiligten deutlich machen und Lösungsmöglichkeiten für Fragen wie Datenschutz, Datensicherheit, Akzeptanz aufzeigen. Deshalb ist das Bibliotheksprojekt auch aus technologiepolitischer Sicht sehr wichtig.“ (in: Technologische Innovation..., S.9/10)

Ausgangspunkt der Senatsstrategie ist also nicht das Interesse an der Förderung der öffentlichen Bibliotheken in den Bereichen, wo sie am dringendsten der Unterstützung bedürfen, wie z.B. bei den Erwerbungssetats. Die Bezuschussung der bezirklichen Ankaufsetats mit 1,7 Mill Euro jährlich hat der Regierende Bürgermeister und Kultursenator noch vor kurzem brüsk abgelehnt, mit den Worten: „Das Geld hab ich nicht, interessiert mich nicht“. Jetzt zögert er nicht, 10 Mill. € in die RFID-Technologie zu investieren, davon kommt zwar die Hälfte aus den Töpfen der EU, aber immerhin muss der Senat noch 2,5 Mill. € selber zahlen, den Rest die ZLB (Zentral- und Landesbibliothek Berlin) und die zum Teil schon zwangsverwalteten Bezirke. Selbst der Mitarbeiter im Informationsforum RFID sagt: „Billig ist das nicht, die RFID-Einführung.“

Das wichtigste Motiv für die Entscheidung zur RFID-Einführung in den öffentlichen Bibliotheken ist daher die Technologie- und Wirtschaftsförderung, die Suche nach einem möglichst großen und publikumswirksamen Anwendungsfeld, wo allein durch den massenhaften Einsatz RFID-Akzeptanz erzeugt und datenschutzrechtliche Bedenken nivelliert werden können. Nachdem die RFID-Anwendung und das Selbst-Scannen in manchen Bereichen des Handels (z.B. Future-Store der Metro-Group,

IKEA und Real) auf Ablehnung oder verhaltene Resonanz gestoßen sind (80% nutzen die Selbst-Scanner-Kassen von IKEA nicht, s. TAZ-Bericht vom 24/25.10.2009), beschert der RFID-Einsatz in großen öffentlichen Einrichtungen, die vom Vertrauen ihrer BenutzerInnen getragen werden, der RFID-Industrie einen ganz anderen Akzeptanz-Schub.

Die BibliothekarInnen müssen prüfen, ob sie den Vertrauensvorschuss ihrer BenutzerInnen nicht missbrauchen, wenn sie allzu bereitwillig, im Sinne einer von oben gelenkten Strategie, auf diese „Technik mit Tücken“ umsteigen.

Ich möchte zum Schluss noch einmal stichwortartig auf einige Argumente der Befürworter des RFID-Einsatzes in Bibliotheken zurückkommen und diese - natürlich kritisch - kommentieren:

- 1) begrenzte Reichweite der RFID-Chips (ca. 30-50 cm, Mifare Mini nur 5 cm)
- 2) auf den RFID-Chips sind nur Nummern gespeichert
- 3) RFID sorgt gleichzeitig für Mediensicherung und vereinfachte Bestandsrevision
- 4) mit RFID wird die Möglichkeit der 24-Std-Rückgabe geschaffen,
- 5) beim RFID-Einsatz in Bibliotheken handelt es sich um geschlossene Systeme
- 6) die Datenschützer wurden einbezogen und haben die RFID-Einführung in den verschiedenen Regionen ohne größere Probleme genehmigt

Zu den einzelnen Punkten:

1) Wie bereits oben berichtet: die Reichweite bei den Medienchips von 50 cm genügt vollumfänglich für vielfältige Auslesemöglichkeiten. Außerdem ist der Algorithmus des meistgenutzten RFID-Systems Mifare ‚gebrochen‘ und die Karten können von etwas geschickteren Leuten jederzeit dupliziert werden.

2) Zwar kann ein Unbefugter nur Nummern auslesen, aber die sind nach einer bestimmten Struktur aufgebaut und geben eine Reihe von Hinweisen: auf die Art der Objekte (Bibliotheksmedien) und Herkunft der Medien (Bibliothekssigel und Land), unter Umständen auch auf Bestandsgruppen. An RFID-Kaufhauskassen ist es beim Bezahlen mit Kundenkarten möglich, personenbezogene Kundendaten mit der Kennzeichnung als Bibliotheksbenutzer zu speichern und für Werbezwecke zu missbrauchen.

3) zunächst wird gesagt: mit RFID gibt es vollkommene Sicherheit, aber kaum ist die RFID-Technologie da, entsteht das Bedürfnis nach noch perfekterer Sicherheitstechnik. So wurden in den bereits flächendeckend mit RFID arbeitenden Bibliotheken von Singapur Videokameras installiert, die jede Regalreihe, jeden Leser im Visier haben. 100%ige Sicherheit gibt es nicht und sollte von den Bibliotheken auch nicht angestrebt werden.

Die anfangs versprochene, problemlose Bestandsrevision mit RFID-Handlesegerät funktioniert in vielen Fällen schon deshalb nicht, weil viele Regale, Stützpfeiler etc. aus Metall sind. Das stört die Funk-Signale nachhaltig.

4) Die Rückgabemöglichkeit von Bibliotheksmedien rund um die Uhr ist ein alter Hut, z.B. für amerikanische Bibliotheken. Dort hat so ziemlich jede Public Library eine Rückgabebox, die von außen für die LeserInnen zugänglich ist – das funktioniert seit Jahrzehnten, auch ohne RFID.

5) Zum Thema geschlossene Systemen merkt FoeBuD mit direktem Bezug auf Bibliotheken an: „Obwohl RFID-Applikationen heute auf geschlossene Systeme beschränkt sind, wird es große Nachfrage nach standardisierter Etikettierung geben. Verleger zum Beispiel könnten eines Tages Bücher an Bibliotheken und Buchhandlungen ausliefern, die beschreibbare Etiketten haben. Jedes Exemplar von ‚Die Früchte des Zorns‘ würde dann einen Teil seines Standard-Warencodes tragen, der mit dem auf jedem anderen Exemplar identisch ist. Die Bibliothek wird in der Lage sein, den restlichen Code anzupassen, so dass er ihren Anforderungen der Inventarkontrolle gerecht wird....Selbst wenn geschlossene Systeme geschlossen bleiben, macht ihr Mangel an Transparenz sie beunruhigend von Standpunkt der Privatsphäre aus. Weil bestimmte Details über geschlossene Systeme möglicherweise nicht leicht erhältlich sind, hätten Konsumenten große Schwierigkeiten bei der Beschaffung der Informationen, die sie benötigen, um Gefährdungen ihrer Privatsphäre einschätzen und sich schützen zu können.“ (<http://www.foebud.org/rfid/unsere-positionen>)

Dieses Szenario ist auch deshalb sehr realistisch, weil Bibliotheken schon seit langem Standing-Order-Liefermodelle mit der EKZ (Einkaufszentrale für die öffentlichen Bibliotheken) und mit Buchhandlungen praktizieren und weil die Übernahme weiterer Dienstleistungen durch die Lieferanten, welche die Bereitstellung der Medien be-

schleunigt, bei den Bibliotheken sehr erwünscht ist. Technisch dürfte es kein Problem sein, dass z. B: die EKZ die Medien gleich mit eingeklebtem RFID-Chip liefert, es bleibt die Frage, wieweit sie für die Nummernvergabe den Zugriff auf die lokalen Datenbanken braucht.

Die KollegInnen der ALA haben einen weiteren Kreis von Personen frühzeitig in ihre datenschutzrechtlichen Überlegungen einbezogen. Ulrike Verch schreibt: „Schließlich gehen die Musterleitlinien noch auf den bislang wenig beachteten Aspekt der vertraglichen Beziehungen zu den Anbietern von RFID-Verbuchungssystemen ein (*Talking to Vendors about RFID*), indem sie beispielsweise fordern, dass die Datenkontrolle allein bei der Bibliothek liegt, dass die Geschäftsbedingungen des Systemlieferanten allen Datenschutzanforderungen gerecht werden und dass bei den Vertragsverhandlungen Sicherheitsaspekte zu beachten sind.“

6) Auch meinem Eindruck nach haben es sich einzelne Datenschützer mit der Absegnung von RFID-Anwendungen in Bibliotheken nicht allzu schwer gemacht. Obwohl auf dem BibliothekarlInnentag in Dresden 2006 ausdrücklich berichtet wurde, dass auf Wunsch des Bayrischen Datenschutzbeauftragten die alten Barcode-Leserausweise beibehalten werden, hat die Stadtbibliothek München 2009 neue Ausweise mit RFID-Chips eingeführt. Ein einfacher Brief an den Datenschutzbeauftragten und die beruhigende Erklärung der Stadtbibliothek, dass auf den neuen Ausweis-Chips auch nur Nummern gespeichert sind, genügte, und schon wurden die Mifare Karten genehmigt.

Das verweist auf den starken Wunsch nach einem Upgrading, sobald die ersten Schritte zur Einführung der RFID-Technologie getan wurden. In Berlin informierte mich der zuständige Datenschutzbeauftragte bei einem Telefongespräch, dass der VÖBB laut Antragsunterlagen den Barcode-Ausweis beibehalten will. Kaum eine Stunde später sagt mir der Verantwortliche für die RFID-Einführung: „Wir wollen auch RFID-Leserausweise haben, ein entsprechender Brief ist gerade an den Datenschutzbeauftragten geschickt worden.“

Der Berliner Datenschutzbeauftragte wird sicher sorgfältig prüfen, ob er das genehmigen will, aber ihm sind voraussichtlich schnell die Hände gebunden, weil er nicht nachweisen kann, dass es sich bei den RFID-Ausweisen zum gegenwärtigen Zeit-

punkt um „mobile personenbezogene Speicher- und Verarbeitungsmedien“ nach § 6c des Bundesdatenschutzgesetzes oder entsprechenden Ländergesetzen handelt. Außerdem stehen auch die Datenschützer unter dem Druck, als „Bedenkenträger“ angefeindet oder in ihren Kompetenzen beschnitten zu werden, wenn sie sich bei technologischen Modernisierungsmaßnahmen quer stellen.

Bei der Durchsicht der Broschüre zur „RFID-Einführung in die Öffentlichen Bibliotheken Berlins“ fällt auf, dass alle Beteiligten sehr oft darüber reden, was in Zukunft alles möglich sein soll dank RFID: mehr Beratung, mehr Leseförderung, mehr Weiterbildung und -qualifizierung, der Kulturstatssekretär träumt sogar von der Sonntagsöffnung und der Zentrale Projektleiter entwickelt Vorstellungen, wie für die öffentlichen Bibliotheken mit RFID in der Stadt „Flächen und Räume zurückerobert werden können.“

Keiner spricht darüber, was diese RFID-Einführung tatsächlich für die Beschäftigten bedeutet: Stellenabbau. Der Hauptpersonalrat wurde bisher offiziell noch gar nicht an der RFID-Einführung beteiligt, aber für ein aus dem Bibliothekswesen stammendes Mitglied des HPR ist klar: „Das ist eine Rationalisierungsmaßnahme vom Feinsten.“ Der Senat spreche nicht gern vom Stellenabbau, aber er werde das auf die Bezirke verschieben. Ganz besonders betroffen von den kommenden Stellenstreichungen werden die FAMIs, die Fachangestellten, sein, denn bis zu 50 % ihrer Aufgaben fallen durch die Selbstverbuchungsautomaten weg.

„In jedem Fall nimmt das Bibliothekswesen eine Vorreiterrolle in der Verbreitung der RFID-Technik in Deutschland ein und sollte dieser besonderen Verantwortung Rechnung tragen, indem es sich eng an datenschutzrechtlichen Leitlinien und ethischen Grundsätzen orientiert“, sagt Ulrike Verch.

Sie empfiehlt, dass die hiesigen Bibliotheken sich angelehnt an amerikanische Empfehlungen eigene Datenschutzkonzepte erarbeiten und diese im Rahmen einer öffentlichen Selbstverpflichtung für verbindlich erklären.

An erster Stelle steht die Verpflichtung zur Transparenz und Offenheit, zur umfassenden Information der Bürger über Einsatz, Inhalt und den Verwendungszweck von RFID. Dazu gehört unbedingt auch die deutliche Kennzeichnung aller Verbuchungs-

und Lesegeräte mit einem sehr gut erkennbaren Logo und Klartext-Informationen an den Geräten und zum Mitnehmen.

Weder in München noch an der TU- oder HU-Bibliothek in Berlin gibt es an den Geräten einen deutlich sichtbaren Hinweis auf die Verwendung der RFID-Technologie, höchstens im Kleingedruckten der Benutzungsordnung kann der Leser Informationen darüber entdecken.

Das ist entschieden zu wenig!

Die Bibliothek sollte sich verpflichten, dass sie die Prinzipien der Datensparsamkeit, Datensicherheit und Transparenz einhält und alles tut, um das Recht eines jeden Bibliotheksbenutzers auf Vertraulichkeit und Privatsphäre zu schützen. Sie sollte ein eigenes Datenschutzkonzept entwickeln und sich zu dem Grundsatz der Datenvermeidung bekennen und zu weiteren, Transparenz schaffenden Maßnahmen. Bei der Datenübermittlung, den Datenbanken und in Bezug auf den Systemzugriff müssen Sicherheitsstandards eingehalten und auch durch eine neutrale Instanz überprüft werden können.

.Die Bibliotheken sollten RFID-Beauftragte in der Bibliothek ernennen, regelmäßige Fortbildungen des Personals zu RFID durchführen und mit dem Personalrat und dem Datenschutzbeauftragten eng zusammenarbeiten.

Insbesondere aber sollten die Bibliotheken - und das ist eine Hauptforderung von Akribie - dem Prinzip der Wahlfreiheit Rechnung tragen, und für alle, die RFID ablehnen, alternative Verbuchungsmöglichkeiten zur Verfügung stellen!

In ihrer 2007 abgeschlossenen Magisterarbeit über „RFID in Bibliotheken“ am Institut für Bibliotheks- und Informationswissenschaft an der Humboldt Universität zu Berlin schreibt Jenny Oltersdorf:

„Trotzdem hat der Einsatz von RFID im öffentlichen Raum eine sehr wohl die Privatheit bedrohende Dimension...Die Menschen der Gegenwart sind beunruhigt, weil die realen und potentiellen Möglichkeiten von RFID für sie nicht begreifbar sind und die Auswirkungen der Technik langfristig bisher als kaum kontrollierbar erscheinen.“

Ein Gefühl der Unsicherheit mache sich breit, das auf lange Sicht zu Verhaltensänderungen führen könne.

Sie fährt fort: „Die Bemühungen öffentlicher Bibliotheken um soziale Gerechtigkeit und Chancengleichheit werden ad absurdum geführt, wenn unsichere Kunden überlegen, welches Medium sie besser nicht entleihen, weil sie nicht abschätzen können, welche potentiellen Eingriffe in die Privatsphäre mit dem Ausleihen eines Bibliotheksmediums mit RFID-Etikett möglich sind.“

Im Namen von Akribie möchte ich deshalb zum Schluss noch einmal betonen: bei der Verwendung der RFID-Technologie in Bibliotheken ist ein Missbrauch zu Lasten der LeserInnen prinzipiell nicht auszuschließen.

Daher sagen wir: die bibliothekarische Ethik gebietet, auf den Einsatz von RFID in Bibliotheken zu verzichten.

Ich danke für Ihre Aufmerksamkeit.

Literaturangaben:

Basiswissen RFID. 2.Aufl. Berlin: Informationsforum RFID, 2007

Basiswissen Internet der Dinge. Berlin: Informationsforum RFID, 2009.

Gewissensbisse. Ethische Probleme der Informatik. Biometrie – Datenschutz – geistiges Eigentum. Hrsg. v. Debora Weber-Wulff u.a. Bielefeld 2009.

Das „Internet der Dinge“. Die Informatisierung der Arbeitswelt und des Alltags. Erläuterungen einer neuen Basistechnologie. Hrsg. Alfons Botthof / Marc Bovenschulte. Düsseldorf: Hans-Böckler-Stiftung, 2009.

http://www.boeckler.de/show_product_hbs.html?productfile=HBS-004457.xml

Oltersdorf, Jenny: RFID in Bibliotheken – Ökonomische, juristische und informationsethische Aspekte des Einsatzes von Radio Frequency Identification in Öffentlichen Bibliotheken. Magisterarbeit. Humboldt-Universität zu Berlin, 2008.

<http://edoc.hu-berlin.de/master/oltersdorf-jenny-2008-02-14/HTML/>

Technologische Innovation als Stärkung der Bürgerkommune: RFID-Einführung in die Öffentlichen Bibliotheken Berlins. Auftaktveranstaltung am 29.Mai 2009 im Ernst-Reuter-Haus. Hrsg. ZLN-Zentral- und Landesbibliothek Berlin, VÖBB-Servicezentrum, 2009.

Aktuelle Informationen zum Projekt:

<http://www.bibliotheksportal.de/hauptmenue/Themen/rfid/praxis/voebb>

Verch, Ulrike: Selbstklebend, selbstverbuchend und auch selbstverpflichtend? Rechtliche Rahmenbedingungen für den Einsatz von RFID-Chips in Bibliotheken.

<http://www.opus-bayern.de/bib-info/volltexte/2007/305/pdf/verch-leipzig-2007.pdf>

Zu der Arbeit von Akribie s. www.akribie.org

Berlin, den 26.2.2010