

DATENSCHUTZ

Etikettengeschwätz



Chipsverseucht: Wenn Etiketten erst einmal Daten funken, bleibt kein Schritt mehr unbeobachtet. (Foto: woxx)

Bislang wussten Supermärkte nur wenig über ihre KäuferInnen. Eine neue Kennzeichnungsmethode macht es möglich, dass sie bald sämtliche persönliche Daten wissen können. Sie schützt vor Ladendieben und gewährt Datendieben freie Hand.

Ein Überwachungsapparat à la George Orwell baut sich im Kaufhaus auf. Was die KonsumentInnen nicht wissen: Eine neue Technologie wird sich wohl schon bald in ihren Einkaufsbeuteln befinden. Die so genannte RFID (Radio Frequency Identification) soll die Strichcodes auf den Verpackungen ablösen. Sie ermöglicht, mittels Radiofrequenzen die Datensätze in Mikrochips von Etiketten kontaktlos und nahezu alle gleichzeitig zu lesen - im Zweifelsfall unbemerkt und aus Entfernungen bis zu zehn Metern.

Was für die einen das Wunderwerk der Technologie ist, ist für die anderen schlicht ein Skandal. Einerseits schützen die fernabfragbaren Mikrochips Unternehmen vor Diebstählen, sorgen für Einsparungen in der Logistik-Kette und optimieren die Verwaltung.

Aber dieser Gewinn kostet. Denn ein aktiver Funkchip greift unberechtigt in die Privatsphäre ein. "Das verträgt sich nicht mit dem Grundrecht auf informationelle Selbstbestimmung", sagt der deutsche Datenschutzbeauftragte Peter Schaar gegenüber dem Internetmagazin Telepolis.

RFID ermöglicht eine eindeutige Identifikation aller Objekte weltweit. Ein Leichtes ist es daher beispielsweise mit Hilfe eines Chip im Schuh, eine Person auszuspionieren – im Supermarkt, aber auch auf politischen Versammlungen. Lesegeräte, eingewebt in Fußböden und in Regalen versteckt, machen es für VerbraucherInnen nahezu unmöglich zu erfahren, wann und wo sie "gescannt" werden.

Der jüngste Sündenfall liegt beim Metro-Konzern. In seinem Future-Store in Deutschland, in dem er den Verkauf einzelner Produkte mit RFID-Etikett testet, verteilte er heimlich auch eine Rabattkarte mit Identifizierungschip an seine KundInnen.

Die neue Technik wird von DatenschützerInnen also zu Recht kritisiert - sogar mit Erfolg. Metro - Vorreiter beim Einsatz der "Schnüffelfchips" in Supermärkten - zog nach Protesten des Datenschutzvereins FoeBuD seine RFID-Kundenkarten per Rückruf-

aktion zurück. Dennoch treibt die Handelskette ebenso wie Tesco, Wal-Mart, Kraft Foods, Gillette, Procter & Gamble den Umstieg vom Barcode auf RFID weiter voran. Ebenfalls interessiert an der neuen Technik sind Büchereien.

Die Marktforschungsinstitute Soreon Research und Logica-CMG erwarten einen großflächigen Einsatz der Technik ab 2008. Laut einer Umfrage von Soreon Research wird Deutschland mit einem Volumen von 600 Millionen Euro dann Marktführer in Europa bei der neuen Etikettierung sein, gefolgt von Frankreich und Großbritannien mit jeweils knapp 500 Millionen Euro.

DatenschützerInnen lehnen die High-Tech-Lösung nicht per se ab. Ein sinnvoller Einsatz in ihren Augen: den Weg von Medikamenten und Gütern vom Herstellungsbis zum Verkaufsort zurückzuverfolgen. Sie fordern vor allem Kontrollmöglichkeiten. Das akzeptieren mittlerweile auch die Unternehmen. "Für uns endet die Supply Chain im Regal. Danach muss der Konsument entscheiden können, ob er den Chip weiter benutzen will", erklärt Volker Heidrun, Vertreter von Kraft Foods auf einer Tagung Anfang Mai beim Handelsblatt in Düsseldorf.

KritikerInnen erwarten noch mehr: Kennzeichnungspflicht für die Schnüffelfchips. VerbraucherInnen müssten die Überwachungswerkzeuge nach dem Kauf im Laden deaktivieren können. Schlafende Schnüffelfchips seien daher ebenso tabu wie Funkchips an Geldscheinen wie sie die Europäische Zentralbank plane. Das wäre das Ende der Anonymität aller KäuferInnen. AnwenderInnen sollen die Verantwortung für die Funkchips übernehmen und Abteilungen einrichten, bei den sich BürgerInnen bei Verletzung der Privatsphäre beschweren können.

Während DatenschützerInnen versuchen, Spielregeln für den Einsatz der neuen Technologie zu etablieren, finden sich immer neue Märkte für die Funkchips. Das Organisationskomitee der Fußball-Weltmeisterschaft 2006

will den Zugang zu den Veranstaltungen in den deutschen WM-Stadien mittels RFID sichern und damit Ticketfälschungen erschweren. "Wir haben den Eindruck, dass hier nicht die Sicherheit im Mittelpunkt steht. Aus den Stadien sollen Einkaufszentren mit eingebautem Fußballplatz werden", sagt Matthias Bettag vom Bund Aktiver Fußballfans. Der Grund für seine Skepsis: Beim Ticketkauf muss auch ein Fragebogen ausgefüllt werden, dessen Daten dann gespeichert werden und im Stadion theoretisch unbemerkt gelesen werden können. "Unternehmen verwenden die geraubten Daten, um mir noch effektiver mit immer weniger Gegenleistung und Vielfalt mein Geld aus der Tasche zu ziehen", sagt der Cyberrights-Aktivist mit dem Künstlernamen padeluun, Mitgründer des "Big Brother Award" in Deutschland, gegenüber Telepolis.

Im Gegensatz zum Strichcode lassen sich die Schnüffelfchips auch unsichtbar in Tiere und Menschen einpflanzen. Veri-Chip, ein US-Unternehmen, bietet solche Implantate im menschlichen Körper an. In Lateinamerika haben sich laut "Consumer Against Supermarket Privacy Invasion and Numbering" bereits rund 2.700 Personen bereitwillig einen Schnüffelfchip einpflanzen lassen, um sich so vor Entführungen zu schützen.

"Viele sagen, ich habe doch nichts zu verbergen. Doch der Big Brother Container kann nicht das Sinnbild einer demokratischen Gesellschaft sein", warnt Deutschlands Datenschutzbeauftragter Peter Schaar. Es ist ja nicht nur der Staat, der mit seinen Kontrollfunktionen hier einen Schritt zu weit gehen kann. Die Jagd nach Persönlichkeitsdaten kann ebenso schnell zu einem prosperierenden Geschäftsfeld werden.

Stephanie Zeiler

Profit gegen Privatsphäre

Die Invasion der RFID-Etiketten wird auch vor Luxemburg nicht halt machen. Die Nationale Datenschutzkommission bereitet sich auf die Verteidigung vor.

(RK) - In Luxemburg, wo "jedeR jedeN kennt", nimmt man es nicht übel, auf der Straße oder im Supermarkt von Unbekanten angesprochen zu werden: "Sie sind doch die Schwester von ..." oder "Du bist doch der Sohn von ..." Ob es den EinwohnerInnen aber auch Recht sein wird, beim Tanken gefragt zu werden: "Ihre am 4.9.2002 gekauften Kimberland-Schuhe lassen auf Naturverbundenheit schließen, Herr X. Dürfen wir Sie zu einer Probefahrt mit unserem neuen Terrestra-Jeep einladen?" Die RFID-Etiketten, die sich schon bald in allen Konsumartikeln wiederfinden könnten, machen so etwas möglich.

Die Nationale Datenschutzkommission (CNPD) befasst sich mit dem Problem. Beim RFID-Seminar, das kommende Woche die Vorteile der RFID-Technologie für Luxemburgs Unternehmen anpreisen soll, wird die CNPD leider nicht auf der Rednertribüne sitzen. "Wir gehen aber hin und hören es uns an", so CNPD-Präsident Gérard Lommel gegenüber der woxx. Über einen Einsatz von RFID-Etiketten in Luxemburger Supermärkten sei der Kommission nichts bekannt. Von der Chambre de Commerce war bis Redaktionsschluss keine Stellungnahme zu bekommen.

"Sobald es um die Erhebung von personenbezogenen Daten handelt, besteht Meldepflicht", erklärt Gérard Lommel. "Personenbezogen" beschränke sich nicht auf "données nominatives", es reiche, dass man anhand der gesammelten Daten eine Person identifizieren könnte. Wenn in Supermärkten RFID-gekennzeichnete Waren in Verbindung mit Kundenkarten erfasst werden, gilt auf jeden Fall die Meldepflicht, versichert der Datenschützer. Das gilt auch, wenn das Unternehmen behauptet, es werde die Daten nur erfassen und nicht auswerten.

Die CNPD orientiert sich an der Arbeit der internationalen DatenschützerInnen. Eine im November vergangenen Jahres in Sydney angenommene Entschliebung der Internationalen Konferenz der Datenschutzbeauftragten zu RFID fordert strenge Auflagen. Vor dem Einsatz dieser Technik sollen Datenverarbeiter "Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen."

Daran, welche Alternativen zumutbar sind, scheiden sich die Geister. In Luxemburg gilt für eine Datenerfassung ohne ausdrückliche Einwilligung die Bestimmung in Artikel 5 des Datenschutzgesetzes: "le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement (...), à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée." Zwischen dem Interesse der Supermarktkette an kostengünstigem Diebstahlschutz sowie effizienter Logistik und dem Interesse der BürgerInnen am vorbeugenden Schutz ihrer Privatsphäre abzuwägen, das sei sehr schwierig, so Gérard Lommel. Mit dieser Aussage bestätigt er indirekt einen Hauptvorwurf der KritikerInnen des Datenschutzgesetzes und der entsprechenden EU-Direktive: dass nämlich die Privatsphäre zu Gunsten des Profitstrebens geopfert werde.

Es sei unklar, welche technischen Möglichkeiten es gebe, die RFID-Technologie im Sinne des Datenschutzes einzuschränken, meint der Präsident der CNPD. Die Hauptgefahr sieht er im "hinterlistigen Ausspionieren der BürgerInnen", nachdem sie die Produkte gekauft haben. Die Ausdehnung der Reichweite der Funk-Etiketten bereitet ihm Sorgen: "Der Bürger kann nicht mehr erkennen, wo und wann Daten über ihn erfasst werden. Unbedingt wünschenswert wäre die Möglichkeit, die Etiketten zu deaktivieren."

Luxemburg könne allerdings nichts im Alleingang unternehmen, sagt Gérard Lommel. Um so wichtiger sind ihm die Arbeiten auf EU-Ebene, im "Komitee Artikel 29". Das soll in den nächsten Monaten eine Empfehlung in Sachen RFID verabschieden. Mit dem Text gewappnet, will die CNPD an die in Luxemburg etablierten Handelsketten herantreten. Gérard Lommel kündigt an: "Wir werden die Antworten veröffentlichen. Wir setzen darauf, dass die Konkurrenz unter den Akteuren zu einer Selbstdisziplinierung führen wird."



Über RFID, die intelligenten Etiketten, und ihre Folgen diskutieren auf einer Konferenz am kommenden Dienstag VertreterInnen der Chambre de Commerce, des Centre de Recherche Public Henri Tudor und von Unternehmen wie Cargolux und IBM.