

18.06.2004 - Tech&Science / Tech-Mix

RFID-Chips: Horror für die Datenschützer?

VON RAINER KNYRIM UND VIKTORIA HAIDINGER

Das Datenschutzgesetz schreibt vor, dass die Sammlung und Verarbeitung von Daten nur mit Zustimmung der Betroffenen erfolgen darf.

Als Nachfolger der Strichcodes zur Kennzeichnung von Waren sind RFID-Chips (Ra-dio Frequency Identity Chips) immer häufiger in den Medien zu finden. Im Gegensatz zu den Strichcodes können diese Chips kontaktlos über Funk ausgelesen werden. Die maximale Entfernung zwischen Chip und Lesegerät hängt vom jeweiligen Modell ab und beträgt im Regelfall zwischen wenigen Millimetern bis hin zu einigen Metern. Auch die Größe der Chips variiert von wenigen Millimetern bis hin zu einigen Zentimetern. Besonderheit dieser Chips ist neben dem Auslesen über Funk die Möglichkeit, theoretisch jedes einzelne Produkt der Welt mit einer individuellen Produktnummer zu versehen.

Verlust der Privatsphäre?

Genau hier beginnen die Horrorszenarien, die Datenschützer in verschiedenen Ländern bereits zu Aufschreien gegen diese neue Technologie bewegt haben: Wenn künftig Produkte mit einer eindeutigen, individuellen Nummer versehen sind, so ist das Risiko groß, dass deren Käufer durch eine Datenverknüpfung ebenso eindeutig und individuell identifiziert werden können. Und, was bei der RFID-Technik noch neu dazu kommt ist, dass diese Identifizierung – da sie über Funk funktioniert – auch ohne Wissen des Betroffenen erfolgen könnte.

Bei den Anwendungsmöglichkeiten gibt es eine große Bandbreite. Harmlos ist etwa die Verwendung der RFID-Technologie zur Lagerverwaltung oder Logistik. Bereits dort aber, wo die Gefahr besteht, dass die Nummern einzelner Produkte über eine Kundenkarte einem Konsumenten zugeordnet werden, fürchten Datenschützer den Verlust der Privatsphäre des Konsumenten, wie die Proteste gegen den „Future Store“ von Metro in Deutschland gezeigt haben, wo versucht wurde, der Öffentlichkeit das rasche und bequeme „Einlesen“ eines ganzen Einkaufswagens durch bloßes Vorbeifahren an einer RFID-Kasse schmackhaft zu machen. RFID-Technik ist aber keine Zukunftsmusik: Die Stadt Wien schreibt die Implantierung von RFID Chips zur Identifizierung von Hunden unter deren Haut vor und nützt die Technik in der neuen Hauptbibliothek zur Bücherausleihe. Auch der Einbau der Chips in die geplanten biometrischen Reisepässe wird diskutiert.

Dass auch wirkliche Horrorszenarien rasch Realität werden können, zeigt der „Baja Beach Club“ in Barcelona, der Gästen unter dem Motto „gänzlich unbelastet tanzen und trinken“ anbietet, sich einen RFID-Chip mit Identifikationsnummer und Kreditkartenfunktion unter die Haut des Oberarms implantieren zu lassen.

Wie sieht nun aber tatsächlich die aktuelle Rechtslage aus? Das Datenschutzgesetz lässt die Ermittlung und Verarbeitung von Daten im Regelfall nur mit Zustimmung des Betroffenen zu, wobei die Zustimmungserklärung den Verwendungszweck genau erkennen lassen muss. Die Formulierung datenschutzrechtlicher Zustimmungserklärungen hat sich aufgrund der Judikatur des Obersten Gerichtshofes zu einer eigenen Wissenschaft entwickelt und die meisten in Umlauf befindlichen Zustimmungserklärungen sind unbrauchbar.

Information ist Pflicht

Dort wo die Datenverarbeitung zur Erfüllung eines Vertrages notwendig ist, kann Datenverarbeitung unter Umständen auch ohne eine Zustimmung erfolgen. Dies aber nur unter der Bedingung, dass der Betroffene über die Datenerhebung zumindest informiert wird und die Daten auch nur zum Zweck der Vertragserfüllung verwendet werden. Darauf beziehen sich unter anderem die Kritikpunkte der Datenschützer an Projekten wie dem Metro Future Store: Die Kunden würden über die Datenerhebung nicht informiert und es sei nicht klar, ob die Daten sowohl im Geschäft (z.B. für Kundenstromanalysen) als auch nach Verlassen des Geschäfts (eine einfache Löschung der Chips ist derzeit nicht möglich) über die bloße Abrechnung an der Kassa hinaus ohne Wissen der Kunden ausgelesen werden.

Zu beachten ist auch eine allfällige Registrierungspflicht beim Datenverarbeitungsregister, allenfalls auch eine Genehmigungspflicht bei der Datenschutzkommission (z.B. wenn die Daten innerhalb eines Konzerns „vermischt“ werden).