Humanistische Union

Und noch eine Chipkarte mehr

Die Einführung des elektronischen Personalausweises

Aus: Mitteilungen Nr. 203, S. 4-5

Am 23. Juli stimmte das Bundeskabinett dem Gesetzentwurf zur Einführung des neuen elektronischen Personalausweises zu. Dieser soll ab dem 1. November 2010 den bisherigen Personalausweis ersetzen. Er wird einen sog. „RFID-Chip“ enthalten auf dem alle Daten gespeichert werden sollen, die auf dem bisherigen Personalausweis angegeben sind, u.a. Name, Anschrift, Alter und biometrisches Lichtbild. Vorerst freiwillig können zudem zwei Fingerabdrücke auf dem Chip registriert werden. Mit einem sog. „RFID-Lesegerät“ können diese Daten dann kontaktlos – im Gegensatz zu kontaktabhängigen Medien wie z.B. der EC-Karte – ausgelesen werden. Die Aufnahme von zusätzlichen biometrischen Merkmalen zu einem späteren Zeitpunkt, wie z.B. ein Netzhaut-Scan oder der DNS, wurde im Gesetzentwurf nicht ausgeschlossen.
Laut Bundesregierung wird das Ausweisdokument durch die Aufnahme von biometrischen Daten sicherer vor Fälschungen. Ob es dieser Erhöhung der Fälschungssicherheit wirklich bedarf, sei dahingestellt – eine nennenswerte Zahl gefälschter Ausweise gab es bisher nicht. Deshalb weist die Regierung auf die neuen Funktionen des elektronischen Personalausweises hin: Mit ihm könnten anhand biometrischer Daten die Inhaber schneller identifiziert und authentifiziert werden.

Sicherheitsrisiken
Dennoch birgt die zukünftige Speicherung biometrischer Daten auf dem Personalausweis auch Sicherheitsrisiken. Die Ausweis-Daten könnten zum einen von unbefugten Personen ausgelesen werden. Die Bundesregierung begegnet diesem Risiko mit der Auflage, die Daten mittels Verschlüsselungsverfahren vor dem Zugriff durch Unbefugte zu schützen. Das Lesegerät muss sich mit einem speziellen „Schlüssel“ bei dem RFID-Chip anmelden und identifizieren. Erkennt der Chip diesen Schlüssel an, werden die Daten übertragen. Ob man den Schlüssel auf Dauer geheim halten kann, ist jedoch äußerst fraglich. Schon allein bei der Einreise in ein anderes Land werden die Daten automatisch an verschiedene Behörden und Staaten übermittelt.

Zum anderen ermöglicht die kontaktlose Übertragung der Daten mittels RFID-Chip das Auslesen der gespeichert Daten, ohne dass der/die Ausweisinhaber/in etwas davon bemerkt. Das verstößt gegen das Grundrecht auf informationelle Selbstbestimmung. Computerexperten wiesen bereits darauf hin, dass es möglich ist, die Lesevorgänge „abzuhören“. Aufgrund der kontaktlosen Kommunikation zwischen einem RFID-Chip und einem Lesegerät können Dritte unbefugt Daten „mithören“ und/oder abfangen.
Die zu erwartende massenhafte Verbreitung von RFID-Chips wird zudem zur Entwicklung von Technologien anregen, die die Schwachstellen von RFID-Chips ausnutzen oder schädigen. Wie einfach so etwas gehen kann, bewies erst kürzlich ein niederländisches Forschungsteam: Erfolgreich entwickelte es einen sog. „RFID-Virus“, der einem Computervirus gleichkommt.

Gefahren durch Biometrie
Auch die Speicherung von biometrischen Merkmalen auf dem neuen elektronischen Personalausweis bringt Missbrauchs- und Manipulationsmöglichkeiten mit sich. So wäre z.B. die Anfertigung von Kopien der gespeicherten Fingerabdrücke denkbar. Dass die Nachfrage an „unbelasteten Fingerabdrücken“ im Bereich der „Organisierten Kriminalität“ ansteigen würde, ist leicht nachzuvollziehen. Die Fälschung von biometrischen Merkmalen ist eben deshalb so gefährlich, weil sie nicht wie Passwörter geändert werden können und sie ständig unfreiwillig und überall hinterlassen werden, wie im Sommer auch der

Bundesinnenminister feststellen musste, nachdem der Chaos Computer Club seinen heimlich abgenommenen Fingerabdruck publizierte.

Durch die Überprüfung ihrer Fingerabdrücke bei jeder Passkontrolle sollen die Bürgerinnen und Bürger langsam daran gewöhnt werden, diese zukünftig bereitwillig und ohne Skepsis an jegliche Fingerabdrucksensoren abzugeben, z.B. in Hotels, Kaufhäusern, Videotheken etc.

Die Speicherung biometrischer Daten unterliegt in Deutschland engen Vorgaben. Für andere Staaten oder Geheimdienste gilt dieses Verbot jedoch nicht. Sie hätten nach der Einführung des ePersonalausweises die Gelegenheit, biometrische Daten der Bundesbürger zu erheben und zu speichern. Diese Datenspeicherung könnten weder der deutsche Staat noch die Betroffenen beeinflussen oder kontrollieren.

Elektronischer Identitätsnachweis
Mit dem neuen Personalausweis soll auch ein „elektronischer Identitätsnachweis“ (eID) eingeführt werden. Die Identifizierung und Nutzung von Angeboten im privat-wirtschaftlichen Bereich, besonders im Internet, sollen mit der eID sicherer werden. Laut Bundesregierung sollen somit Dienste wie Online-Banking, Online-Versandhandel und -Auktionen, E-Mail-Accounts und Chat-Foren, Online-Computerspiele etc. aber auch Angebote im sog. E-Government-Bereich, wie die elektronische Steuererklärung (ELSTER-Formular), Kfz-An- und -Ummeldung oder eine elektronische Adressänderung einfacher und schneller in Anspruch genommen werden können.

Um die Funktion des eID im Internet zu nutzen, benötigt der/die Inhaber/in ein zertifiziertes Lesegerät mit dazugehöriger Software. Der Personalausweisinhaber bekommt zudem eine Geheimnummer (PIN). Damit Anbieter von Online-Angeboten die Möglichkeiten des eID nutzen können, müssen sie eine Berechtigung sowie ein „Berechtigungszertifikat“ bei einer staatlichen Stelle beantragen. Der Diensteanbieter übermittelt vor einer Transaktion das Berechtigungszertifikat an den Interessenten. Dieser kann sich somit von der Authentizität des Berechtigungszertifikats überzeugen und die Datenkategorien auswählen, die sie/er übermitteln möchte. Nach der Eingabe der Geheimnummer wird der Personalausweis per Lesegerät am PC ausgelesen und die Daten an den Diensteanbieter übertragen.

Nachteile und Risiken
Ein Risiko, das der „elektronische Identitätsnachweis“ mit sich bringt, ist das sog. „Single Sign-On“-Verfahren. Im Fall des Verlustes eines Personalausweises – laut BMI werden jährlich rund 250.000 Personalausweise gestohlen oder gehen verloren – steigt das Risiko eines Missbrauchs. Dritte könnten mit Hilfe der Ausweise versuchen, auf das Bankkonto, die Steuererklärung oder den E-Mail-Account des Besitzers zuzugreifen. Der Personalausweis als Universalschlüssel wird hier zum Sicherheitsrisiko: Sicherheitsexperten wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) weisen schon seit Jahren daraufhin, nie ein und dasselbe Passwort für mehrere verschiedene Online-Dienste zu nutzen.

Ein zweites Risiko liegt bei den „Berechtigungszertifikaten“ und der staatlichen Vergabe dieser Zertifikate. Mit den Berechtigungszertifikaten sollen Transparenz und Vertrauen zwischen Verbrauchern und Diensteanbietern geschaffen werden. Alle Diensteanbieter, welche den eID für die Authentifizierung ihrer Kunden nutzen wollen, müssen sich bei einer staatlichen Vergabestelle registrieren und prüfen lassen. In Anbetracht des geplanten massenhaften Einsatzes des eID und der weiter steigenden Bedeutung des Internethandels ist mit einem enormen Ansturm auf die Vergabestellen der Berechtigungszertifikate zu rechnen. Ob diese über die nötigen Kompetenzen, personelle Ausstattung und Zeit verfügen, um die Menge der Anträge umfassend und genau zu überprüfen, ist fraglich. Zudem lässt sich aus dem Gesetzentwurf zum neuen Personalausweis entnehmen, dass eine tiefgehende Prüfung der einzelnen Antragsteller gar nicht vorgesehen ist. So wird praktisch jeder, der z.B. nicht wegen Betruges vorbestraft ist, ein Zertifikat erhalten. Das Versprechen der Bundesregierung, dass mit einem Berechtigungszertifikat für den Verbraucher „in jedem Falle transparent [ist], wer welche Daten elektronisch abfragt“, hilft da nur wenig.

Unverständlich ist auch, warum die Vergabestelle und nicht die Datenschutzaufsichtsbehörde prüfen soll, ob

der Datenschutz eingehalten wird. Die Datenschutzaufsichtsbehörde kann nur aufgesucht werden, wenn seitens des Verbrauchers Zweifel an der Echtheit eines Berechtigungszertifikats bestehen. Aber auch hier fehlt es der Behörde an wirksamen Befugnissen, denn laut § 21 des Gesetzentwurfs zum neuen Personalausweis verfügt sie über keinerlei Sanktionsmöglichkeiten im Fall von Datenmissbrauch – sie kann zweifelhaften Anbietern höchstens das Zertifikat entziehen. Ein schwacher Trost für Bürgerinnen und Bürger, die sich auf eine staatlich installierte Infrastruktur verlassen haben.

Bastian Gräbener
studiert Politikwissenschaften in Marburg und absolvierte ein Praktikum in der Bundesgeschäftsstelle der Humanistischen Union

---