Vertrauenssache

von Dirk Heckmann

Nicht bestimmte IT-Sicherheitsdefizite, sondern ein Ausblenden der Risiken beziehungsweise eine Verlagerung des Sicherheitsmanagements auf die Bürger könnten die Akzeptanz des elektronischen Personalausweises (ePA) schwächen. Eine kritische Stellungnahme.

Der elektronische Personalausweis (ePA) kommt und mit ihm ein weiterer Baustein in der eCard-Strategie des Bundes. Ähnlich wie schon der E-Pass soll er zu einer sicheren Authentifizierung, unter anderem durch biometrische Merkmale, beitragen. Ähnlich wie die elektronische Gesundheitskarte wird er Zusatzfunktionen bieten, die in der alltäglichen elektronischen Kommunikation nützlich sein werden, insbesondere durch die elektronische ID. Dagegen ist nichts einzuwenden, ganz im Gegenteil: Eine sichere Authentifizierung ist dort sinnvoll und geboten, wo das Gesetz eine rechtsverbindliche Feststellung der Identität verlangt. Dem werden Ausweispapiere, welche die Identitätsfeststellung über ein Ähnlichkeitsurteil (beim Lichtbild) auf eine Wahrscheinlichkeitsprognose begrenzen, nicht gerecht. Fraglich ist aber, welche technischen Merkmale einen solchen Sicherheitsgewinn nicht nur versprechen, sondern auch einlösen können. Hierzu ist eine Diskussion entbrannt, wonach biometrische Merkmale keineswegs das Maß an Sicherheit – im Sinne von Eindeutigkeit, Fälschungssicherheit und Angriffssicherheit – bieten, das ihnen gemeinhin zugesprochen wird. Dies sei bei Fingerabdrücken problematisch, die nach dermatologischen Erkenntnissen eine Fehlerquote von drei bis elf Prozent aufweisen sollen. Aber auch die biometrische Gesichtserkennung sei unsicher, weil die hier zugrunde liegenden mathematischen Verfahren einen umso höheren Unsicherheitsfaktor aufweisen, je stärker ein Gesicht vom Normgesicht abweicht. Kritisch gesehen werden zudem die Unwägbarkeiten der eingesetzten RFID-Technologie. Die Validität dieser Erkenntnisse kann hier weder verifiziert noch falsifiziert werden.

So könnte der elektronische Personalausweis aussehen.

Was aber auffällt: In der Begründung zum neuen Personalausweisgesetz werden die Risiken eines Missbrauchs oder Identitätsdiebstahls, von Fälschungen oder fehlgeschlagener Authentifizierung nicht genannt. Im Gegenteil ist die Rede von „hohem sicherheitstechnischen Niveau“. Dies erweckt den Eindruck, als könne der elektronische Personalausweis mit seinen hoheitlichen und nichthoheitlichen Funktionen problemlos eingesetzt werden. Die gute Absicht und das Bemühen um normative und technische Vorkehrungen zur Gewährleistung von IT-Sicherheit sollen nicht in Abrede gestellt werden. Jedoch wäre es wünschenswert gewesen, der Gesetzgeber hätte den Normadressaten das Gefühl vermittelt, er sei sich der IT-Sicherheitsrisiken, die – in welchem Maße auch immer – bestehen, bewusst, um dann die Rechtsfolgen bei Fehlern, Pannen oder Missbrauch aufzuzeigen: Was passiert genau, wenn die Überprüfung der Identitätsmerkmale fehlschlägt? Oder bei einem „Diebstahl“ der eID? Welche Beweislastverteilung gilt? Was können die zivilrechtlichen oder öffentlich-rechtlichen Rechtsfolgen sein? Das wirkliche Problem sind nicht bestimmte IT-Sicherheitsdefizite, sondern die Augen-zu-und-durch-Mentalität beim Umgang, oder besser gesagt Nichtumgang, mit diesen Risiken.

Dabei folgt genau diese staatliche Pflicht, und damit auch jene

des Gesetzgebers, zur Technikfolgenabschätzung aus dem neuen Grundrecht auf Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme. Dieses Grundrecht wurde vom Bundesverfassungsgericht in seinem Urteil vom 27.2.2009 als (weiterer) Bestandteil des Persönlichkeitsrechts – quasi als Schwestergrundrecht zum Recht auf informationelle Selbstbestimmung – entfaltet. Es ist nicht nur ein Abwehrrecht gegen übermäßige staatliche Zugriffe, wie etwa bei der Online-Durchsuchung, sondern begründet zugleich eine objektivrechtliche Dimension in Form von Schutz- und Förderpflichten. Zwar hat der Staat insoweit einen Gestaltungsspielraum. Das Untermaßverbot verpflichtet ihn aber zu einem Minimum an tauglichen Maßnahmen, zu denen eben auch ein IT-Risiko-Management zählt.

Bemerkenswert ist, dass der Gesetzgeber bei der Regelung des neuen elektronischen Personalausweises die Risiken nicht nur ausblendet. Er verlagert das Sicherheitsmanagement zum Teil ausgerechnet auf den Bürger. So heißt es in § 27 Abs. 3 PersAuswG-neu: „Der Personalausweisinhaber soll durch technische und organisatorische Maßnahmen gewährleisten, dass der elektronische Identitätsnachweis gemäß § 18 nur in einer Umgebung eingesetzt wird, die nach dem jeweiligen Stand der Technik als sicher anzusehen ist. Dabei soll er insbesondere solche technischen Systeme und Bestandteile einsetzen, die vom Bundesamt für Sicherheit in der Informationstechnik als für diesen Einsatzzweck sicher bewertet werden.“ Das ist erstaunlich. Damit werden Obliegenheiten zur Gewährleistung von IT-Sicherheit begründet, die der Bürger als Otto Normalnutzer nicht erfüllen kann. Es geht hier nicht um die qualifizierte Minderheit technisch kompetenter IT-Nutzer, sondern um Jedermann, dem das Bundesverfassungsgericht im Urteil zur Online-Durchsuchung eine hohe Schutzbedürftigkeit attestiert hat. Ausdrücklich führt es aus, der Bürger könne Zugriffe in vernetzten, hochkomplexen Systemen zum Teil gar nicht wahrnehmen, jedenfalls aber nur begrenzt abwehren. Ein wirkungsvoller sozialer oder technischer Selbstschutz werfe erhebliche Schwierigkeiten auf und könne zumindest den durchschnittlichen Nutzer überfordern. Zumal er mit einem hohen Aufwand oder mit Funktionseinbußen des geschützten Systems verbunden sei. Und schließlich blieben viele Selbstschutzmöglichkeiten weitgehend wirkungslos. So könne angesichts der Geschwindigkeit der informationstechnischen Entwicklung nicht zuverlässig prognostiziert werden, welche Möglichkeiten dem Nutzer in Zukunft verbleiben, sich technisch selbst zu schützen. Dieses Leitbild macht deutlich, dass der Staat dem Bürger als Durchschnittsnutzer nichts abverlangen kann, er ihn im Gegenteil schützen und fördern muss. Und das besonders bei einer Technologie, die er selbst auf den Markt bringt und an deren Einsatz er ein großes Interesse hat.

Das also sind die eigentlichen Schwächen des neuen Personalausweisgesetzes: Nicht die Innovation eines moderneren Authentifizierungssystems und schon gar nicht erneute Befürchtungen staatlicher Überwachung, denen der Präsident des Bundesverfassungsgerichts in seiner Rede zum 25-jährigen Jubiläum des Volkszählungsurteils überzeugend entgegengetreten ist. Vielmehr fehlt ein Konzept dafür, wie man eine risikobehaftete, nur teilweise und nicht von jedermann beherrschbare Technologie auf eine vertrauenswürdige Basis stellt. Schon wegen der zahlreichen Datenschutzpannen und -skandale sowie einem zunehmenden Misstrauen in die (eigentlich vorhandene) Redlichkeit der staatlichen Akteure sind flankierende vertrauensbildende Maßnahmen bei neuen IT-Projekten dringend erforderlich, damit diese nicht nur erduldet, sondern akzeptiert werden. Es wäre bedauerlich, wenn der im Prinzip sinnvolle elektronische Personalausweis in seinen nicht hoheitlichen Funktionen das gleiche Schicksal erleiden würde wie die digitale Signatur. Er wäre nicht nutzlos, aber ungenutzt.

Prof. Dr. Dirk Heckmann ist Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht sowie stellvertretender Leiter des Instituts für IT-Sicherheit und Sicherheitsrecht an der Universität Passau.