Zeitschrift für
Informations-,
Telekommunikations-
und Medienrecht

MMR

MultiMedia und Recht

10/2012



EDITORIAL

# Brüsseler Angriff auf den neuen Personalausweis?

Die Umsetzung großer IT-Infrastrukturprojekte gleicht bisweilen dem Versuch, den Wind einzufangen: Sie sollen einen ökonomischen Nutzen für alle Beteiligten erzeugen, rechtsverbindliche Transaktionen ermöglichen, die Schutzziele der IT-Sicherheit gewährleisten, das Vertrauen der Kommunikationspartner stärken, möglichst rasch von Wirtschaft, Verwaltung und Bürgern akzeptiert werden und schließlich die Persönlichkeitsrechte der Nutzer und etwaiger Dritter fördern oder zumindest nicht gefährden.

Auch der neue Personalausweis kann nicht alle diese Ziele gleichermaßen und in gleicher Geschwindigkeit erreichen. Er ist aber auf einem guten Weg: Die Ausweisinhaber können nach § 18 Abs. 1 Satz 1 PAuswG ihren Personalausweis dazu verwenden, ihre Identität gegenüber öffentlichen und nichtöffentlichen Stellen elektronisch nachzuweisen. Dies ermöglicht rechtsverbindliche Authentisierungen im Internet, die die ökonomischen Risiken von Transaktionen mit unbekannten Kommunikationspartnern vermindern und bestimmte Verwaltungsprozesse im Internet überhaupt erst ermöglichen. Der neue Personalausweis erreicht ein hohes Maß an technischer Sicherheit (s. *Bender/Kügler/Margraf/Naumann*, DuD 2008, 173; DuD 2010, 295; DuD 2010, 761), auch wenn im Bereich der Endgeräte der Nutzer Risiken fortbestehen.

Prof. Dr. Gerrit Hornung

Insbesondere handelt es sich bei dem elektronischen Identitätsnachweis um ein datenschutzrechtlich vorbildliches Konzept (dazu und zur Struktur s. *Roßnagel/Hornung/Schnabel*, DuD 2008, 168; *Roßnagel/Hornung*, DÖV 2009, 301; *Schulz*, CR 2009, 267; *Polenz*, MMR 2010, 671; *Borges*, NJW 2010, 3334; *Möller*, in: Hornung/Möller, PassG/PAuswG, 2011, § 18 PAuswG Rdnr. 3 ff.): Die Funktionalität ist freiwillig sowohl hinsichtlich der grundsätzlichen Aktivierung (§ 10 Abs. 1 PAuswG) als auch hinsichtlich der Nutzung im Einzelfall (PIN-Eingabe, § 18 Abs. 4 PAuswG). Die Übermittlung erfolgt nur an Diensteanbieter mit Berechtigungszertifikat zum Datenzugriff, und dieses Zertifikat wird nur nach Prüfung der datenschutzrechtlichen Erforderlichkeit, bei Einhaltung technischer Sicherheitsanforderungen und nicht an Adresshändler ausgestellt. Es wird vor Übermittlung der Daten angezeigt und sorgt so für Transparenz hinsichtlich der verantwortlichen Stelle und der für sie zuständigen Datenschutzbehörde. Schließlich ermöglicht der elektronische Identitätsnachweis auch die isolierte Übermittlung des Über- oder Unterschreitens eines bestimmten Alters, der Angabe, ob ein Wohnort dem angefragten Wohnort entspricht, sowie eines dienste- und kartenspezifischen Kenn-

zeichens (Pseudonym). Hierdurch werden entsprechend den Grundsätzen der Datenvermeidung und Datensparsamkeit (§ 3a BDSG) Geschäftsmodelle für solche Anbieter ermöglicht, die lediglich diese Angaben, nicht aber die Identität des Ausweisinhabers erfahren müssen.

Während die qualifizierte elektronische Signatur auch 15 Jahre nach dem ersten Signaturgesetz noch ihres Durchbruchs harrt und die elektronische Gesundheitskarte mehr als sechs Jahre nach der in § 291a Abs. 1 Satz 1 SGB V angeordneten Einführung „spätestens zum 1. Januar 2006" immer noch kaum mehr kann als ihre Vorgängerin, ist der neue Personalausweis auf der Nachfrageseite eine Erfolgsgeschichte: Etwa ein Drittel der Inhaber der bisher knapp 18 Millionen neuen Personalausweise und elektronischen Aufenthaltstitel hat sich für die Freischaltung des elektronischen Identitätsnachweises entschieden. Der Ball liegt damit im Feld der Anbieter: Staatliche und private Stellen sind aufgerufen, attraktive Anwendungen für diese große und ständig steigende Zahl potenzieller Nutzer bereitzustellen. Es ist verständlich, dass die Anbieter sich eine noch höhere Aktivierungsquote wünschen würden. Angesichts der in naher Zukunft zweistelligen Millionenzahl von Nutzern, die sich überdies aktiv für die Funktion entschieden haben, ist das Argument der fehlenden Nachfrage aber kaum überzeugend – welche andere Infrastruktur hätte in derart kurzer Zeit eine vergleichbare Verbreitung erzielt?

Diese Entwicklung würde indes abrupt enden, wenn der Vorschlag der *EU-Kommission* für eine Verordnung über die elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (KOM(2012) 238 endg.) in der derzeitigen Form verabschiedet würde. In zwei völlig losgelöst voneinander stehenden Teilen enthält dieser zum einen eine Fortschreibung der bisherigen Signaturrichtlinie nebst Erweiterung um Angebote wie elektronische Zustelldienste (zusammengefasst als „Vertrauensdienste" bezeichnet), zum anderen erstmals europäische Vorgaben für die elektronische Identifizierung. Ersteres betrifft die staatliche Regulierung privater Angebote, Letzteres die gegenseitige Anerkennung staatlich bereitgestellter Identifizierungsdienste.

Der Vorschlag enthält keine Pflicht der Mitgliedstaaten, elektronische Identifizierungssysteme bereitzustellen. Werden diese allerdings für nationale Onlinedienste verlangt, so müssen alle Identifizierungssysteme aus anderen Mitgliedstaaten ebenfalls akzeptiert werden, die in einem entsprechenden Verfahren bei der *EU-Kommission* notifiziert worden sind.

Dieser grundsätzliche Ansatz ist begrüßenswert, weil Identifizierungssysteme wie der elektronische Identitätsnachweis des neuen Personalausweises auch in grenzüberschreitenden Transaktionen einsetzbar sein sollten. Der Teufel steckt indes im Detail, nämlich in der Frage, unter welchen Voraussetzungen eine Notifizierung möglich ist. Hier fällt zunächst auf, dass der Entwurf keinerlei Minimum-Sicherheitsniveau für die Identifizierungssysteme enthält (dieses würde die *Kommission* mittels delegierter Rechtsakte nach bisher unbekannten Kriterien festlegen), während auf der Diensteseite alle Systeme akzeptiert werden müssen und keine Unterscheidung zwischen einfachen und sicherheitsbedürftigen Applikationen erlaubt wird – eine Form von Gleichmacherei, die den Praxisanforderungen kaum genügen dürfte.

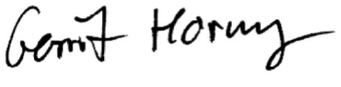
Für Deutschland entscheidend ist dann aber, dass „keine bestimmten technischen Vorgaben" (Art. 6 Abs. 1 lit. d des Entwurfs) für die Verwendung gemacht werden dürfen. Abgesehen davon, dass diese Vorgabe evident zu weit geraten ist – jeder Identifizierungsdienst ist von derartigen Vorgaben abhängig –, hat es dieses Detail in sich: Es stellt einen direkten Angriff auf das deutsche System der Berechtigungszertifikate dar und führt dazu, dass der elektronische Identitätsnachweis in seiner heutigen Form nicht notifizierungsfähig wäre. Das System bliebe zwar formal rechtmäßig, wäre der Sache nach als Insellösung jedoch zum Scheitern verurteilt. Dem Vernehmen nach ist dies der *Kommission* auch bewusst: Das Ende des deutschen elektronischen Identitätsnachweises wird dort sehenden Auges in Kauf genommen.

Das gesetzgeberische Ziel der Interoperabilität ist zu begrüßen, technisch aber lösbar: Im EU-Projekt STORK (https://www.eid-stork.eu/) wurden zwei Ansätze konzipiert und pilotiert: der „Proxy-Ansatz", bei dem jeder Mitgliedstaat ein zentrales Gateway betreibt, das zwischen den verschiedenen eID-Systemen übersetzt, und der „Middleware-Ansatz", bei dem der Dienstanbieter selbst über eine Middleware verfügt, die an die verschiedenen eID-Systeme angebunden ist. Das zweite System ist mit dem deutschen Ansatz kompatibel, wird von der *Kommission* trotz der Sicherheits- und Datenschutzprobleme des Proxy-Ansatzes aber offenbar nicht weiter verfolgt.

Insofern wäre es allerdings geradezu absurd, wenn die *Kommission*, die im Januar 2012 einen Vorschlag für eine Reform des europäischen Datenschutzrechts vorgelegt hat, die auch im internationalen Vergleich datenschutzrechtlich vorbildliche (*Geers*, Comparison of eID Solutions with Privacy preserving Characteristics, http://tinyurl.com/cghuv4n) deutsche Infrastruktur aus dem europäischen Verbund ausschließen würde. Der Verordnungsentwurf erwähnt das Wort Datenschutz im Zusammenhang mit den Identifizierungssystemen noch nicht einmal und ignoriert alle Ansätze für ein selbstbestimmtes und datenschutzfreundliches Identitätsmanagement: Die Verwendung von Pseudonymen, der anonyme Nachweis bestimmter Attribute und der Einsatz unterschiedlicher Identifizierungsmechanismen in verschiedenen Lebensbereichen wurden offenbar noch nicht einmal in Erwägung gezogen. Stattdessen läuft der Vorschlag auf staatliche Gateways in jedem Mitgliedstaat hinaus, über die grenzüberschreitende Transaktionen abgewickelt werden – derartige zentrale Stellen sind aber die datenschutzrechtlich schlechteste Lösung des Authentisierungsproblems im Internet.

Der Vorschlag der *Kommission* läuft damit nicht nur dem selbstgesteckten Ziel zuwider, „keinen Eingriff in die in den Mitgliedstaaten bestehenden elektronischen Identitätsmanagementsysteme" vornehmen zu wollen (EG 11). Der Ausschluss des deutschen elektronischen Identitätsnachweises würde überdies ein sinnvolles, technisch sicheres und datenschutzfreundliches System abrupt beenden, das gerade dabei ist, sich durchzusetzen – und das alles auch noch unnötigerweise. Noch ist Zeit, dies zu verhindern.

Passau, im Oktober 2012



**Professor Dr. Gerrit Hornung**
ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau.