

WESTFÄLISCHE
WILHELMS-UNIVERSITÄT
MÜNSTER

ITM | Leonardo-Campus 9 | 48149 Münster

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)868 C

Institut für
Informations-,
Telekommunikations-
und Medienrecht

Prof. Dr.
Bernd Holznapel, LL.M.
Direktor

Dr. Marius Stracke
Geschäftsführer

Leonardo-Campus 9
48149 Münster

Tel. +49 251 83-38641
Fax +49 251 83-9038644
holznapel@uni-muenster.de
<http://itm.uni-muenster.de>

Datum 21.04.2017

STELLUNGNAHME

ZUR ÖFFENTLICHE ANHÖRUNG ZUM ENTWURF EINES GESETZES ZUR FÖRDERUNG DES ELEKTRONISCHEN IDENTITÄTSNACHWEISES

I. Elektronischen Identitätsnachweis nachhaltig fördern

Im Jahre 2010 ist den Bürgerinnen und Bürgern die Möglichkeit eröffnet worden, sich mittels ihres Personalausweises online auszuweisen. Hierzu müssen sie bei der Aushändigung des Personalausweises gegenüber der Personalausweisbehörde erklären, dass sie den elektronischen Identitätsnachweis nutzen wollen. Die Einrichtung einer Funktion zum elektronischen Identitätsnachweis soll elektronische Transaktionen im Verhältnis zu Behörden und Unternehmen sicherer machen. Bisher erfolgt der Nachweis der Identität vor allem im Geschäftsleben durch die Eingabe und online-Übermittlung von Passwörtern. Diese Vorgehensweise ist jedoch anfällig für Angriffe Dritter. Die Kriminalstatistiken zeigen, dass der „Passwortdiebstahl“ in den letzten Jahren sprunghaft zugenommen hat.¹ Mit Einführung der eID-Funktion wird staatlicherseits der Versuch unternommen, eine sichere und verlässliche Infrastruktur zur gegenseitigen Identifikation im Internet zur Verfügung zu stellen. Sie basiert auf

¹ Siehe *Bundeskriminalamt, Cybercrime / Bundeslagebild 2010-2015*.

dem Prinzip einer Zwei-Faktoren-Authentifizierung, welches sich bei der Umsetzung im Alltag bewährt hat.

In der Praxis ist jedoch die Akzeptanz dieser 2010 eingeführten Sicherheitsinfrastruktur gering. Nur ein Drittel der Antragsteller macht von der bereitgestellten Opt-In-Möglichkeit Gebrauch. Mit dem Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises in seiner derzeitigen Fassung (BT-Drs. 18/11279) soll nun die Nutzung der eID-Funktion gefördert werden. Dieses gesetzgeberische Ziel ist nachhaltig zu unterstützen. Die Digitalisierung von Wirtschaft und Gesellschaft hat in den letzten Jahren rasant an Fahrt aufgenommen. Sichere Vernetzungen und Transaktionen sind eine zentrale Voraussetzung dafür, dass der notwendige Transformationsprozess erfolgreich durchgeführt werden kann. Darüber hinaus bedarf es eines angemessenen Schutzes der Bürgerinnen und Bürger, aber auch der Unternehmen, wenn sie online kommunizieren und Transaktionen durchführen. Die Förderung des elektronischen Identitätsnachweises ist hierfür grundsätzlich eine wichtige Maßnahme.

Eine andere Frage ist, ob der hierfür im Gesetzesentwurf gefundene Steuerungsansatz weit genug geht. Schaut man sich das Geschäftsleben außerhalb Europas – zum Beispiel in China oder den USA – an, stellt man fest, dass die Identifizierung immer mehr per Mobiltelefon und vorwiegend auf Basis von Fingerprints erfolgt. Dem Gesetzgeber wäre zu raten, sich auf diese technologische Entwicklung rechtzeitig einzustellen und hierfür zeitnah besondere Förderansätze zu entwickeln. Des Weiteren dürfte die mangelnde Akzeptanz der eID-Funktion in der Bevölkerung auch damit zu tun haben, dass ihr Nutzen für die Bürgerinnen und Bürger nicht hinreichend erkenntlich ist. Es fehlt an Diensten von Wirtschaft und Verwaltung, die erkennbar durch den Einsatz der eID-Funktion einfacher und besser in Anspruch genommen werden können. Schließlich müssen die neuen technologischen Möglichkeiten auch „in den Köpfen“ verankert werden. Hierfür bedarf es permanenter Information und Schulung. Auf diesen Feldern weist die an sich lobenswerte Strategie der Bundesregierung ein deutliches Defizit auf.

II. Opt-In oder Opt-out ?

Um den Gebrauch der eID-Funktion zu fördern, soll nach dem neu gefassten § 10 Abs. 1 PAuswG-E der Personalausweis zukünftig standardmäßig mit dieser Funktion

ausgegeben werden. Der Bürger kann aber jederzeit durch einen Anruf eine sofortige Sperrung des elektronischen Identitätsnachweises veranlassen (§ 10 Abs. 6 PAuswG-E). Die Regelung wird damit im Ergebnis von einer „Opt-In“-Lösung auf ein „Opt-Out“-Modell umgestellt.

In verfassungsrechtlicher Hinsicht ist diese Umstellung hin zu einer dauerhaften Einstellung der eID-Funktion unbedenklich. Es handelt sich wenn überhaupt um einen marginalen Eingriff in die Allgemeine Handlungsfreiheit, da Bürgerinnen und Bürger das „Opt-Out“ jederzeit durch Sperrung formlos vornehmen können und zudem im Alltag weiterhin selbst entscheiden, ob und wie sie die Funktion nutzen (vgl. § 18 PAuswG-E). Vor übertriebenen Erwartungen in diese Maßnahme ist jedoch zu warnen, weil die übrigen tatsächlichen Hindernisse für den Gebrauch der eID-Funktion – zum Beispiel unzureichende Mobilfunkanwendungen, zu wenig attraktive Dienste und mangelnde Verankerung im Bewusstsein – weiterhin bestehen.

III. Ex-Ante- oder Ex-Post-Kontrolle des Diensteanbieters?

Derzeit setzt die Prüfung für Berechtigungszertifikate durch die Vergabestelle ex-ante an. Die Vergabestelle muss detailliert klären, zu welchen Aufgaben oder Geschäftszwecken Daten im Wege des elektronischen Identitätsnachweises beim Inhaber des Personalausweises mittels eines Berechtigungszertifikats angefragt werden können. Hierbei ist auch der Frage nachzugehen, ob den Anforderungen an Datenschutz und Datensicherheit Rechnung getragen wird (vgl. § 21 Abs. 1 und 2 PAuswG). Das bisherige Verfahren mag zwar auf den ersten Blick umständlich erscheinen, dient aber in der Praxis auch der frühzeitigen Sensibilisierung der Antragsteller für die Belange des Datenschutzes und damit proaktiv der Vermeidung datenschutzrechtlicher Beanstandungen. Die Unternehmen werden darüber aufgeklärt, wie der Rechtsrahmen ihrer zukünftigen Tätigkeit in diesem Bereich aussieht. Oft können so die Geschäftsmodelle auf das bestehende Recht von Anfang an eingestellt werden und spätere Konflikte mit dem Datenschutzrecht verhindert werden.

Zukünftig soll anstelle der bisherigen zweckgebundenen Vergabe eine organisationsbezogene Vergabe erfolgen. Der Antragsteller muss nicht mehr den Zweck der Abfrage der Daten aus dem elektronischen Identitätsnachweis benennen. Es soll vielmehr ausreichen, dass der Diensteanbieter das dem Antrag zugrunde liegende Interesse an einer Berechtigung darlegt. Begründet wird dieser Systemwechsel mit dem

Ziel der Vereinfachung. Die Praxis habe gezeigt, dass die Diensteanbieter den bisherigen Zertifizierungsgang scheuten und stattdessen auf alternative Identifizierungsmittel zurückgriffen.²

Die angestrebte „Vereinfachung“ erweist sich bei genauer Betrachtung indessen als ein Scheineffekt. Die Neuregelung ist nämlich nicht mit einer Absenkung der Standards für den Datenschutz und die Datensicherheit verbunden. Die Unternehmen müssen sie selbstverständlich weiterhin einhalten und gehen zukünftig zusätzlich das Risiko ein, dass sie bei einer Unterschreitung von den Datenschutzbehörden ex-post sanktioniert werden. Vieles, was präventiv durch die Vorprüfung an Unsicherheiten aus dem Wege geräumt werden konnte, wird nun nachträglich infolge einer Kontrolle durch die Datenschutzbehörden auf die Unternehmen zurückfallen. Kommt es zu einer Sanktionierung, ist diese für die Diensteanbieter regelmäßig mit erheblichen Belastungen finanzieller Art und mit einem massiven Imageschaden verbunden, der auf die eID-Funktion selbst zurückfallen kann. Die Vermeidung dieser Risiken dürfte den Aufwand, der von den Diensteanbietern im bisherigen Zertifizierungsverfahren aufzubringen ist, im Ergebnis rechtfertigen. Aus diesem Grunde sollte an dem bisherigen Verfahren zur Erteilung der Berechtigungszertifikate festgehalten werden.

IV. Automatisierter Lichtbildabruf für Sicherheitsbehörden und Nachrichtendienste beschränken

Der neu eingefügte § 25 Abs. 2 S. 3 PAuswG-E, der zum 1. Mai 2021 in Kraft treten soll, berechtigt „die Polizeien des Bundes und der Länder, das Bundesamt für Verfassungsschutz, der Militärische Abschirmdienst, den Bundesnachrichtendienst sowie die Verfassungsschutzbehörden der Länder“ dazu, im Hinblick auf Reisepässe und Personalausweise „das Lichtbild *zur Erfüllung ihrer Aufgaben* im automatisierten Verfahren abrufen“. Der automatisierte Abruf wird an keine weiteren Voraussetzungen geknüpft. Die Subsidiaritätsklausel des § 25 Abs. 2 S. 1 2.HS PAuswG soll hier nicht gelten. Hiernach sind die Polizei- und Ordnungsbehörden zum Abruf im automatisierten Verfahren nur dann befugt, wenn die Personalausweisbehörde auf

² BT-Drs. 18/11279, 28

andere Weise nicht erreichbar ist und ein weiteres Abwarten den Ermittlungszweck gefährden würde.

Für die Erweiterung des Kreises der zum Abruf im automatisierten Verfahren befugten Behörden, die § 25 Abs. 2 S. 3 PAuswG-E vorsieht, werden in der Gesetzesbegründung gewichtige Gründe angeführt.³ So wird u.a. darauf hingewiesen, dass die Ermittlung und die Kontaktaufnahme mit der örtlich zuständigen Behörde, die den Pass oder Personalausweis ausgestellt hat, oft zu zeitaufwendig oder zum Beispiel in den Abendstunden oder am Wochenende gar nicht möglich ist. Es ist nachvollziehbar, dass in Eilfällen gleichwohl ein automatisierter Abruf angezeigt ist. Zutreffend ist auch der Hinweis darauf, dass mit der Einzelabfrage der das Lichtbild liefernden Behörde unweigerlich bekannt wird, dass eine Person Gegenstand von Ermittlungen der Sicherheitsbehörden oder Nachrichtendienste ist. Dies ist ein Umstand, der durchaus nicht allen Betroffenen angenehm sein dürfte und im Wege des automatisierten Abrufs vermieden werden kann.

Andererseits wird eine Abfrage des Lichtbildes im automatisierten Verfahren nur daran geknüpft, dass dies für die Erfüllung der Aufgaben der Nachrichtendienste bzw. der Sicherheitsbehörden erforderlich ist. Damit wird das automatisierte Verfahren zu einem Standardverfahren erhoben. Da die Vernetzung der Behörden untereinander heute sehr weit gediehen ist, wird damit eine Situation geschaffen, die funktional dem der Einrichtung einer bundesweiten Datenbank für bestimmte biometrische Merkmale (Lichtbilder) entspricht. § 25 Abs. 6 PAuswG-E, der ein Verbot der Errichtung einer solchen Datenbank vorsieht, wird damit in seinem Sinngehalt unterlaufen. Aus diesem Grunde sollte die Subsidiaritätsklausel beibehalten werden und auch für die Nachrichtendienste gelten. Sie müsste allerdings auf die besonderen Interessenlagen der Nachrichtendienste und Sicherheitsbehörden zugeschnitten werden. So wäre zu berücksichtigen, ob bei einer vorherigen Anfrage bei den zuständigen Behörden die Gefahr der Enttarnung von Personen oder auch der Weitergabe der Nachfrage durch Unbefugte entstünde.

Subsidiaritätsklauseln dieser Art sind im geltenden Recht nicht unbekannt. Ein Beispiel findet sich u.a. in § 10 Abs. 7 BKAG. Die Abfrage des Lichtbildes im automatisierten

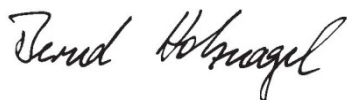
³ 18/11279, 32.

Verfahren könnte etwa daran geknüpft werden, dass gerade diese Form der Datenübermittlung „zur Wahrung des Zwecks der Abfrage unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen oder wegen ihrer besonderen Eilbedürftigkeit“ angemessen ist.

Daneben gilt es, einen Personenkreis zu definieren, der bei den Sicherheitsbehörden oder Nachrichtendiensten zur Abfrage berechtigt ist. Eine solche Regelung wäre allerdings nicht im Gesetz selbst zu treffen, sondern müsste Gegenstand einer noch zu entwerfenden Rechtsverordnung oder einer Verwaltungsvorschrift sein. Der Gesetzgeber sollte erwägen, dazu Leitlinien mindestens in der Begründung des vorliegenden Gesetzesentwurfs vorzugeben.

V. Passversagung

Zu begrüßen ist, dass in § 7 Abs. 1 Nr. 11 PassG-E ein neuer Passversagungsgrund eingeführt werden soll, um die Ausreise von Person zu unterbinden, denen im Ausland gravierende Menschenrechtsverletzungen drohen. Der Gesetzesentwurf verweist insoweit allerdings nur auf § 226a StGB (Verstümmelung weiblicher Genitalien). Es läge nahe, den Gesetzesentwurf dieser Stelle um einen Verweis auch auf § 237 StGB zu ergänzen, um auch Ausreisen zum Zwecke der Zwangsverheiratung unterbinden zu können. Eine Ausreise zum Zweck der Herbeiführung einer Zwangsehe kann ebenso wenig hingenommen werden wie eine Ausreise zum Zwecke einer sogenannten „Beschneidung“. Die Gefahren für die von diesen Menschenrechtsverletzungen betroffenen Mädchen und jungen Frauen und deren Schutzbedürftigkeit sind in beiden Fällen gleichwertig.



Prof. Dr. Bernd Holznagel



Dr. Marius Stracke