nahme der Bundesauftragsverwaltung dar, da es die Bundesauftragsverwaltung zeitlich (erheblich) verkürzt und die Atomaufsicht insbesondere gegenüber den Altreaktoren reduziert[70]. Für die Genehmigung der Standortzwischenlager (§ 9a II 3 AtG) ist der Bund zuständig; die periodischen Sicherheitsüberprüfungen gem. § 19a AtG 2002 stellen nur eine quantitative Erhöhung der Aufgaben der Atomaufsicht gegenüber den bereits vorher gebotenen Sicherheitsüberprüfungen dar; eine qualitativ neue Tragweite haben die periodischen Sicherheitsüberprüfungen nicht.

Im Übrigen sei darauf hingewiesen, dass das *BVerwG* in mehreren Entscheidungen zum AtG 2002 keinen Anlass gesehen hat, die von Amts wegen zu prüfende Frage, ob das AtG 2002 verfassungsgemäß zu Stande gekommen ist, auch nur zu erörtern[71].

VII. Ergebnis

Eine Verlängerung der durch das AtG 2002 begrenzten Betriebsgenehmigungen der Atomkraftwerke bedarf bereits deshalb der Zustimmung des Bundesrats, weil sie die Bundesauftragsverwaltung für den Verwaltungsvollzug des Atomgesetzes verlängert. Darüber hinaus werden den Ländern in der Bundesauftragsverwaltung neue Aufgaben von wesentlich anderer Bedeutung und Tragweite übertragen; dies gilt insbesondere für die Prüfung des Risikos terroristischer Angriffe, der Alterung der Reaktoren sowie der gebotenen umfassenden Nachrüstungen, die auf Grund der Begrenzung der Betriebszeit durch das AtG 2002 unterblieben sind. Aufgaben von wesentlich neuer Tragweite ergeben sich für die Länder ferner durch das Optimierungsgebot der EURATOM-Richtlinie 2009/71 für betriebene Reaktoren sowie für die Genehmigung und Aufsicht bei Stilllegung und Abbau der Kernkraftwerke und für die Planfeststellung und Aufsicht bei Errichtung und Betrieb von Endlagern. Diese Aufgaben werden ausschließlich den Ländern auferlegt; der Bund ist sowohl als Gesetzgeber als auch im Verwaltungsvollzug aus Kompetenzgründen gehindert, diese Aufgaben selbst wahrzunehmen. ■

70 S. o. III 1; faktisch beendete z. B. das AtG 2002 den bereits damals über ein Jahrzehnt andauernden Rechtsstreit zwischen der Betreiberin des Atomkraftwerks Biblis A und dem Land Hessen um die Erfüllung der Auflage v. 27. 3. 1991 zur Einrichtung eines kostenaufwändigen gebunkerten Notstandssystems; s. hierzu die Energiekonsensvereinbarung 2000 (o. Fußn. 6), Anlage 2; sowie *Böwing* (o. Fußn. 26), S. 201, und *Renneberg* (o. Fußn. 17).

71 S. etwa *BVerwG*, NVwZ 2008, 1012, sowie *BVerwG*, NVwZ, 2009, 921 „Übertragung einer Reststrommenge".

Professor Dr. Thomas Hoeren, Münster*

Luftverkehr, Check-In und Pass-/Personalausweisdaten

Die Vorschriften des Pass- und des Personalausweisgesetzes untersagen den automatisierten Abruf personenbezogener Daten mittels Reisepass und Personalausweis im nichtöffentlichen Bereich. Der Autor befasst sich mit der Frage, ob die Vorschriften ein absolutes Verwendungsverbot beinhalten oder den freiwilligen Einsatz des Passes oder des Personalausweises durch den Betroffenen zwecks Identifizierung vor dem Flug zulassen.

I. Einführung

Die großen Fluggesellschaften in Europa erlauben die Identifizierung beim Check-In via Pass oder Personalausweis. Dies erstaunt zunächst. Denn § 18 III PassG und § 4 III PersAuswG untersagen den automatisierten Abruf personenbezogener Daten mittels Reisepass und Personalausweis im nichtöffentlichen Bereich. So lautet § 18 III PassG: „Der Pass darf weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden". Ähnlich formuliert ist § 4 III PersAuswG: „Der Personalausweis darf weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden".

Nach § 25 II Nr. 4 lit. b PassG handelt derjenige ordnungswidrig, der gegen ein Verbot der Verwendung des Passes zum automatischen Abruf oder zur automatischen Speicherung personenbezogener Daten gem. § 18 III PassG verstößt. Ein Verstoß gegen § 4 III PersAuswG ist eine Ordnungswidrigkeit nach § 5 I Nr. 3 lit. b und lit. c PersAuswG.

Fraglich und umstritten ist, ob diese Regelungen ein absolutes Verwendungsverbot beinhalten oder den freiwilligen Einsatz des Passes oder des Personalausweises durch den Betroffenen zwecks Identifizierung vor dem Flug noch zulassen.

II. Rechtsnatur der Vorschriften

§ 18 PassG und § 4 PersAuswG sind von ihrem Wortlaut her datenschutzrechtliche Bestimmungen. Denn hier werden zahlreiche Begriffe verwendet, die durch das Bundesdatenschutzgesetz bzw. die Datenschutzgesetze der Länder vorgeprägt sind. Der Begriff des personenbezogenen Datums findet sich in § 3 I BDSG mit einer ausführlichen Legaldefinition. Der Begriff der Speicherung entspricht dem Begriff der Speicherung in § 3 IV Nr. 1 BDSG und umfasst daher das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung.

Datenschutzrechtlich unbekannt ist der Begriff des „automatischen Abrufs". Hierbei handelt es sich aber wohl nicht um eine bewusste Differenzierung der passrechtlichen Bestimmung im Hinblick auf das allgemeine Datenschutzrecht, sondern um eine sprachliche Ungenauigkeit. Denn einen „automatischen Abruf" gibt es nicht. Gemeint ist wohl der Abruf nach § 3 IV Nr. 3 lit. b BDSG, wonach unter das Übermitteln auch Bekanntgeben von Daten an einen Dritten in der Weise fällt, dass der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder „abruft". In diesem Sinne wird der Begriff des Abrufs auch in § 10 BDSG verwendet (s. dazu unten). Unbekannt ist auch der Begriff „automatisch". Das BDSG spricht stattdessen von automatisierter Verarbeitung (§ 6a BDSG), ohne diesen Vorgang technisch zu konkretisieren oder gar zu definieren. Wenn § 18 III PassG und § 4 III PersAuswG datenschutzrechtlich vorgeprägte Begriffe verwenden, sind die entsprechenden Definitionen des BDSG zur Interpretation heranzuziehen.

* Der *Verf.* ist Direktor des Instituts für Informations-, Telekommunikations- und Medienrecht der Universität Münster.

Für eine datenschutzrechtliche Qualifizierung der Vorschriften spricht im Übrigen auch die Vorgeschichte etwa des Personalausweisgesetzes.

Personalausweise sind als besondere Identifikationspapiere neben Reisepässen seit 1938 gebräuchlich. Auf Grund des Gesetzes über das Pass-, das Ausländer- und das Meldewesen sowie das Ausweiswesen vom 11. 5. 1937 (RGBl I, 589) wurde am 22. 7. 1938 eine Verordnung über Kennkarten erlassen (RGBl 1913). Die Verordnung wurde später ersetzt durch das Gesetz über Personalausweise vom 19. 12. 1950. Es wird wegen der bloßen Rahmengesetzgebung die Kompetenz des Bundes (Art. 75 Nr. 5 GG) durch Ausführungsgesetze der Bundesländer ergänzt. Seit den 70er Jahren stand das Gesetz unter dem Vorwurf, dem Stand der Datenschutzgesetzgebung nicht mehr zu entsprechen. Die Datenschutzbeauftragten warnten vor einer missbräuchlichen Verwendung der Personalausweisdaten und forderten dementsprechende Sicherungen im Personalausweisgesetz[1]. Spätestens seit dem Volkszählungsurteil des *BVerfG*[2] war der Gesetzgeber aufgefordert, das Personalausweisgesetz datenschutzrechtlich zu ergänzen. So wurde das Inkrafttreten des Vierten Gesetzes zur Änderung des Gesetzes über Personalausweise mit Gesetz vom 26. 10. 1984 ausgesetzt[3]. Der Grund hierfür war das Urteil des *BVerfG* zum Volkszählungsgesetz[4]. Nach der Neubildung einer Koalition aus CDU/CSU und FDP konnte dann erst der Entwurf eines Fünften Gesetzes zur Änderung des Gesetzes über Personalausweise in das Parlament eingebracht werden[5]. In diesem Gesetzentwurf fanden sich dann erstmals Vorkehrungen, die den Schutz der im Zusammenhang mit der Ausstellung der Personalausweise erhobenen personenbezogenen Daten verbessern sollten.

Auch die Literatur sieht die Vorschrift als datenschutzrechtliche Bestimmung an. So spricht zum Beispiel *Wache*[6] davon, dass es hier um „Verstöße gegen datenschutzrechtliche Bestimmungen" gehe. Auch *Gola* sieht das Personalausweisgesetz und das Passgesetz als datenschutzrelevante Sondergesetze[7].

III. Verhältnis zum BDSG

Wenn § 18 PassG und § 4 PersAuswG datenschutzrechtliche Vorschriften sind, dann stellt sich als nächstes die Frage nach deren Verhältnis zum BDSG. Es stellt sich dogmatisch die Frage, worauf der Erlaubnistatbestand des § 18 I PassG und § 4 I PersAuswG zielt. Die Vorschrift spricht davon, dass der Personalausweis und der vorläufige Personalausweis auch im nichtöffentlichen Bereich benutzt werden „können". Dies verweist auf eine Referenzregelung, in deren Rahmen der Erlaubnistatbestand des § 4 I PersAuswG zum Tragen kommt. Ohne eine solche Referenznorm wäre der Erlaubnistatbestand sinnlos. Der Referenzrahmen stammt aus dem BDSG selbst. § 1 III BDSG sieht vor, dass andere Rechtsvorschriften des Bundes dem BDSG vorgehen, sofern sie sich auf personenbezogene Daten und deren Verwendung beziehen. Das BDSG ist lediglich lex generalis, die insbesondere bei Lücken in der spezialgesetzlichen Normierung wieder zum Tragen kommt. Die Literatur geht davon aus, dass die Verdrängung des BDSG allerdings nur in dem Umfang stattfindet, in dem nach einem genauen inhaltlichen Vergleich eine abweichende Regelung für den exakt gleichen Sachverhalt vorliegt[8]. Wie *Walz* schreibt, kommt das BDSG auch ergänzend zur Anwendung:

„Auch umfangreiche Spezialnormenwerke sind vielfach keine Vollregelungen und lassen dem BDSG ergänzende Anwendungsfälle. Auch wenn zum Beispiel die Erlaubnistatbestände abschließend geregelt sind (...), ist unter anderem für die Begriffsbestimmungen (§ 3) die Anforderungen an die Einwilligung (§ 4 a) oder die Betroffenenrechte (§§ 19 ff., 34 f.) wieder auf das BDSG zurückzugreifen"[9].

In der Literatur wird ausdrücklich darauf hingewiesen, dass Passgesetz und Personalausweisgesetz als datenschutzrechtliche Sonderbestimmungen einzuordnen sind[10]. So finden sich das Personalausweis- und das Passgesetz auch in der Liste bereichsspezifischer Normen im Handbuch Multi-Mediarecht[11].

Es stellt sich als nächstes die Frage nach den Auslegungsregeln zu § 18 PassG und § 4 PersAuswG. § 18 I PassG und § 4 I PersAuswG lassen eine Nutzung des Personalausweises auch im nichtöffentlichen Bereich als Ausweis- und Legimitationspapiere zu. Diese Regelung ist eine Art „lex generalis". Klargestellt werden soll, dass grundsätzlich Personalausweise als Ausweis- und Legitimationspapier im privaten Rechtsverkehr eingesetzt werden können. § 4 III PersAuswG ist insofern eine Ausnahme von der grundsätzlichen Verwendbarkeit der Personalausweisdaten, für einen klar abgesteckten Bereich der automatisierten Speicherung von Daten.

Die Regelungen beziehen sich insofern auf ein besonderes Gefährdungspotenzial der automatisierten Speicherung, das es näher zu konkretisieren gilt. § 18 III PassG ist das Pendant zu § 22 PassG und der dort geregelten Weitergabe von Daten zwischen Behörden. § 22 II PassG erlaubt die Weitergabe von Daten an andere Behörden nur auf deren Ersuchen. Das Ersuchen ist an besondere Formen- und Inhaltsvoraussetzungen gebunden (§ 22 III und § 22 II 2 PassG). Insbesondere muss die ersuchende Behörde den Anlass des Ersuchens und die Herkunft der übermittelten Daten und Unterlagen aktenkundig machen (§ 22 II 3 PassG). Die Regelung verbietet insofern auch den einfachen automatisierten Zugriff auf Daten der Passstelle. Ähnlich ist die Regelung in § 2 b und § 3 a PersAuswG[12]. Dementsprechend ist nach § 2 c PersAuswG die Verwendung automatisierter Verfahren nur im Zusammenhang mit der Verfolgung von Straftaten und Verkehrsordnungswidrigkeiten beim Abruf von Lichtbildern zulässig. Im Übrigen ist ein automatisierter Abruf durch andere Behörden oder in anderen Konstellationen strikt unzulässig. Der Gesetzgeber geht mit der Regelung in § 18 PassG und § 4 PersAuswG davon aus, dass dies erst recht für den Bereich der Nutzung von Pass- bzw. Personalausweisdaten ohne Zustimmung des Betroffenen seitens Privater gelten muss.

§ 22 PassG war Gegenstand von Auseinandersetzungen zwischen Datenschützern und den Bußgeldbehörden[13]. In dem Verfahren hatten die Bußgeldbehörden automatisiert personenbezogenen Daten des Betroffenen, insbesondere ein bei der Passstelle hinterlegtes Lichtbild, aus dem Passregister abgerufen. Das *AG Stuttgart* sah darin einen Verstoß gegen

1 *Wache*, in: *Erbs/Kohlhaas*, Strafrechtliche Nebengesetze, 76. Aufl. (2009), Vorb. zum PersAuswG Rdnr. 2.
2 *BVerfGE* 65, 1 = NJW 1984, 419.
3 BGBl I, 1305.
4 *Bartels/Dube*, Personalausweis- und PassR, Stand: 2009, K 9 Bund, unter 1.1.
5 BT-Dr 10/2177.
6 *Wache*, in: *Erbs/Kohlhaas* (o. Fußn. 1), § 25 PassG Rdnr. 5.
7 *Gola*, NJW 1986, 1913 (1915).
8 *Walz*, in: *Simitis* (Hrsg.), BDSG, 6. Aufl. (2006), § 1 Rdnr. 170.
9 *Walz*, in: *Simitis* (o. Fußn. 8), § 1 Rdnr. 170.
10 S. *Fritsche*, LKV 1991, 81 (83).
11 *Helfrich*, in: *Hoeren/Sieber*, Hdb. Multi-MediaR, 21. Erg.-Lfg. (2008), Rdnr. 110.
12 *Bartels/Dube* (o. Fußn. 4), zu § 3 a.
13 *AG Stuttgart*, Urt. v. 12. 2. 2002 – 8 OWi 71 Js 98447/01.

die datenschutzrechtlichen Übermittlungsbestimmungen des Passgesetzes. Entscheidend wurde darauf abgestellt, dass hier eine Zweckentfremdung dieser Informationen ohne Einverständnis des Betroffenen vorliege. Es liege eine Verletzung des Persönlichkeitsrechts des Betroffenen vor, die eine Verwertung und Bußgeldverfahren gegen seinen Willen nicht zulasse. Entscheidend war also für das *AG Stuttgart* das Argument, dass die passgesetzlichen Übermittlungsbestimmungen die Persönlichkeitsrechte der Betroffenen schützen und insofern ein automatisierter Abruf von Daten nicht ohne Einverständnis des Betroffenen erfolgen könne.

Ähnlich argumentiert in einem ausführlichen Grundsatzurteil auch das *VG Aachen*[14]. Es ist Justizvollzugsanstalten nach diesem Urteil auf Grund von § 3 a PersAuswG nicht erlaubt, zur Arbeitserleichterung maschinenlesbare Personalausweis- oder Passdaten beim automatischen Lesen in einem elektronischen Pfortenbuch zu speichern. Der Betroffene habe wegen des besonderen Gefährdungspotenzials des automatisierten Speicherns einen Anspruch auf Löschung der unter Verstoß gegen das Speicherungsverbot gespeicherten Daten. Eine hohe Gefährdung liege vor allem darin, dass bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, sondern heute vielmehr mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar seien.

Eine weitere Besonderheit liege darin, dass personenbezogene Daten darüber hinaus mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden könnten, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit hätten sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert. Zu beachten sei daher der besondere Schutzzweck der Bestimmungen zum automatisierten Speichern, nämlich die „mit der elektronischen Datenverarbeitung einhergehenden besonderen Risiken, die wegen der potenziell höheren Möglichkeit und Wahrscheinlichkeit von Grundrechtsgefährdungen erhöhte Schutzmechanismen erfordern"[15].

IV. Tatbestandsvoraussetzungen

Das hier streitgegenständliche Auslesen von Ausweisdaten ist kein automatischer Abruf bzw. keine automatische Speicherung im Sinne der genannten Vorschriften. Auch die Terminologie ist uneinheitlich. § 4 III PersAuswG spricht von einem „automatischen Abruf" und einer „automatischen Speicherung". § 2 c PersAuswG hingegen spricht von einem „automatisierten Abruf". § 3 a PersAuswG wiederum spricht von einem „automatischen Abruf aus Dateien und einer automatischen Speicherung".

Für das Speichern erforderlich ist, dass die Information nach dem Fixieren auf einem Datenträger wiedergewonnen werden kann, sie also für eine spätere Wahrnehmung „nachlesbar" festgehalten wird[16]. Dies wird bei einem reinen Arbeitsspeicher jedenfalls dann nicht der Fall sein, wenn die temporär abgelegten Informationen nicht wenigstens durch Einzeleingabe oder eine besondere Programmierung unter einer speziellen, die Rückholbarkeit gewährleistenden Zwischendatei-Bezeichnung – und sei es automatisch – in einem besonderen temporären Verzeichnis gesichert, sondern lediglich unbenannt bis zu ihrer Überschreibung vorhanden bleiben. Eine Zwischendatei-Sicherung müsste überdies zum Zweck ihrer weiteren Verarbeitung, also zum Zweck des Rückgriffs, erfolgen. Das *VG Aachen* hat aus diesen Gründen mit ausführlicher Begründung die Verwendung von Ausweisdaten aus dem Anwendungsbereich von § 18 III PassG und § 4 III PersAuswG genommen[17]. Im Falle eines Luftfahrtunternehmens werden aber keine Daten eines Reisedokuments (Pässe, Personalausweise, Visa, Resident Card, usw.) dauerhaft gespeichert. Eine Speicherung bzw. Verarbeitung findet nur im Hauptspeicher (= Arbeitsspeicher) des Automaten bzw. Servers statt. Nach Abschluss des Check-In-Vorgangs, unabhängig davon, ob erfolgreich oder nicht, werden die Daten unwiderruflich gelöscht. Pass- oder Personalausweisinformationen werden nie dauerhaft gespeichert, selbst in den Trace-Dateien nicht (in so genannten Trace-Dateien werden Vorgangsdaten gespeichert). Zur Unterscheidung einzelner Reise-Dokumente im Trace eines Check-In-Vorgangs wird ein „Hashwert" gespeichert, der aber keinen Rückschluss auf die Inhalte der maschinenlesbaren Zone zulässt. Insofern fehlt es hier im Check-In-Modell an einer Speicherung i. S. von § 18 III PassG und § 4 III PersAuswG.

Das Check-In-Modell ist aber auch nicht mit einem Abruf i. S. von § 18 III PassG und § 4 III PersAuswG verbunden. Ein Abruf erfolgt niemals automatisch, sondern durch eine Person, die den Abrufvorgang initiiert. Abruf bedeutet nämlich, dass mit Hilfe des automatischen Auslesens Daten aus anderen Datenbanken erschlossen, also Daten daraus durch das Auslesen erschlossen werden[18]. In der passrechtlichen Literatur wird unter dem automatischen Ablesen die „automatische Aufzeichnung personenbezogener Daten unmittelbar durch den Lesevorgang"[19] verstanden. Dementsprechend betonen *Bartels/Dube*:

„Der automatische Abruf personenbezogener Daten aus Dateien im Sinne dieser Vorschrift ist ein Verfahren, bei dem die Zone für das automatische Lesen dazu verwendet wird, mit einem Lesegerät Zugang zu einer automatischen Datei zu erhalten"[20].

Eine Begründung für diese Auslegung findet sich nicht. Man könnte den automatisierten Abruf aber anders verstehen, so wie er zum Beispiel § 24 c KWG zu Grunde liegt. Dann würde sich der automatisierte Abruf auf einen freien durch EDV/Datenfernübertragung ermöglichten Zugriff beziehen. Das Risikopotenzial läge dann in der Dauerhaftigkeit der Abruf- und Nutzungsmöglichkeiten ohne zwischengeschaltete Kontrolle insbesondere des Betroffenen. Insofern sieht etwa das *BVerfG* den Begriff des automatisierten Abrufs in einem Gegensatz zu manuellen Einzelanfragen[21]. Entsprechend wird in der Entscheidung das Problem der Automatisierung des Abrufverfahrens darin gesehen, dass eine solche Automatisierung „das Risiko zahlloser und, wenn sie ohne hinreichende Verdachtsmomente erfolgen, rechtswidriger Routineabrufe begründen".

Losgelöst, wie man nun den Begriff des Abrufs versteht, liegt vorliegend ein Abruf nicht vor. Insofern ist zu beachten, dass

14 DuD 2009, 192 = BeckRS 2008, 38079.
15 *VG Aachen*, DuD 2009, 192 = BeckRS 2008, 38079.
16 *VG Aachen*, DuD 2009, 192 = BeckRS 2008, 38079.
17 *VG Aachen*, DuD 2009, 192 = BeckRS 2008, 38079.
18 *VG Aachen*, DuD 2009, 192 = BeckRS 2008, 38079; ähnl. *Süßmuth/Koch*, Pass- und PersonalausweisR, Stand: 2010, § 3 a PersAuswG Rdnrn. 17 ff.; ebenso die Kommentierung von *Ehmann/Brunner*, Pass- und AusweisR, Stand: 2009, § 17 PassG.
19 *Wache*, in: *Erbs/Kohlhaas* (o. Fußn. 1), § 17 PassG Rdnr. 2. Ähnlich auch *VG Aachen*, DuD 2009, 192 = BeckRS 2008, 38079.
20 *Bartels/Dube* (o. Fußn. 4), K 9 Bund, zu § 3 a PersAuswG.
21 *BVerfG*, NJW 2007, 2464 (2469) Rdnr. 123.

der automatisierte Abruf nur wegen der vom Beginn des Ablaufs in Gestalt des automatischen Lesens bereits gegebenen Zielgerichtetheit auf das Speichern hin im Gesetz geregelt ist. Diesen Zusammenhang von Abruf und Speicherung hat das *VG Aachen* in seiner Grundsatzentscheidung zur Nutzbarkeit von Passdaten deutlich herausgearbeitet[22]. Fehlt es an der Zielrichtung der (dauerhaften) Speicherung, ist ein bloßes Auslesen der Daten unschädlich und irrelevant. Es fehlt dann an dem besonderen Gefährdungspotenzial, der zur Regelung in § 18 III PassG und § 4 III PersAuswG geführt hat. Geschützt werden soll der Betroffene davor, dass die im Ausweis enthaltenen Seriennummern ausgelesen und zur Grundlage der Erstellung von Persönlichkeitsprofilen gemacht werden. Die Seriennummer des Ausweises soll nicht die Qualität einer (verfassungsrechtlich verbotenen) Personenkennziffer bekommen[23]. Im vorliegenden Fall ist jedoch auf Grund der sofortigen Löschung der Daten die Gefahr einer Erstellung von Profilen von vornherein ausgeschlossen. Insofern liegt auch nach dem Sinn und Zweck der Vorschriften kein relevanter Abruf vor.

Im Übrigen scheidet ein „Abruf" auch aus anderen Gründen aus. In der datenschutzrechtlichen Literatur wird im Zusammenhang mit § 10 BDSG über die Definition des Begriffs „Abruf" nachgedacht. Die ganz herrschende Meinung geht davon aus, dass bei einem Abruf „das Auslösen des Übermittlungsvorgangs durch den Datenempfänger erfolgen muss"[24]. Entscheidend sei es, dass der Empfänger den Übermittlungsvorgang auslöse, ohne dass es noch vorher zu einer Überprüfung seitens des Datenbesitzers komme[25]. Im vorliegenden Fall steuert jedoch der Kunde den Check-In-Vorgang und dessen Modalitäten. Er entscheidet frei darüber, wie er sich identifizieren will. Er bestimmt über den Einsatz des Ausweises und veranlasst selbst den Scanvorgang. Er löst folglich auch die weiteren Übermittlungsvorgänge aus, die insofern von seiner freien Entscheidung gedeckt sind. Es liegt also kein Abruf durch das Luftfahrtunternehmen, sondern eine Übermittlung durch den Kunden vor. § 18 III PassG und § 4 III PersAuswG beziehen sich aber nur auf den Abruf, nicht auf die Übermittlung. Es handelt sich um datenschutzrechtliche Vorschriften (s. o.), die datenschutzrechtlich belegte Termini verwenden. Im Übrigen handelt es sich um bußgeldbewehrte Vorschriften, die entsprechend den Vorgaben des Strafrechts eng auszulegen sind. Von daher ist die wichtige Unterscheidung zwischen Abruf und Übermittlung auch zu beachten. Wenn der Kunde aktiv Daten an das Luftfahrtunternehmen übermittelt, ist dies kein Abruf-Vorgang, der ausweisrechtlich geahndet werden könnte.

V. Zwischenergebnis

Die Nutzung von Ausweisdaten für den Check-In unterliegt nicht den Beschränkungen von § 18 III PassG und § 4 III PersAuswG. Insbesondere fehlt es an einem Abruf und einer Speicherung im Sinne dieser Vorschriften.

VI. Informationelle Selbstbestimmung

Selbst wenn man sich der obigen Argumentation nicht anschließt, verstößt das Check-In-Modell nicht gegen § 18 III PassG und § 4 III PersAuswG. Denn diese Vorschriften schützen – wie oben erläutert – die informationelle Selbstbestimmung des Betroffenen gegen einseitige privatwirtschaftliche Verarbeitungsmaßnahmen. Verboten werden soll, dass die im Ausweis enthaltenen Seriennummern ausgelesen und zur Grundlage der Erstellung von Persönlichkeitsprofilen gemacht werden. Die Seriennummer des Ausweises soll nicht die Qualität einer (verfassungsrechtlich verbotenen) Personenkennziffer bekommen[26].

Diese Gefahr ist aber im vorliegenden Fall überhaupt nicht gegeben. Denn im Falle der Identifizierungssysteme eines Luftfahrtunternehmens ist die Situation anders als etwa bei einer dauerhaften Massenspeicherung von Ausweisnummern durch Banken oder Versicherungen[27]. Dem Betroffenen steht es frei, selbst zu entscheiden, wie er sich identifizieren will. Er kann hierzu seine Kreditkartennummer eingeben oder weitere Flugreservierungsdaten verwenden. Er kann aber auch seinen Personalausweis oder Pass zur Identifizierung einsetzen. Dies hat für ihn den besonderen Vorzug besonderer Benutzerfreundlichkeit. Statt komplizierte Flugreservierungsdaten einzugeben, kann er schlichtweg seinen Personalausweis bzw. seinen Pass auslesen lassen. Spart dadurch Zeit und Nerven. Gleichzeitig ist für ihn sehr häufig ein solches Ausweispapier in Griffnähe, da er sich ohnehin für den Flug selbst regelmäßig durch ein entsprechendes Ausweispapier legitimieren muss. Insofern bleibt aber das Prinzip der freien Entscheidung des Betroffenen darüber, wie er sich selbst für den Zugriff auf die Flugunterlagen ausweisen möchte.

Eine andere Auslegung würde das informationelle Selbstbestimmungsrecht des Betroffenen konterkarieren. Das allgemeine Persönlichkeitsrecht trägt in seiner Ausbilligung als Recht auf informationelle Selbstbestimmung, Gefährdungen und Verletzungen der Persönlichkeit Rechnung, die sich für den Einzelnen aus informationsbezogenen Maßnahmen, insbesondere unter den Bedingungen moderner Datenverarbeitung, ergeben[28]. Es gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen[29]. Dieses Recht auf informationelle Selbstbestimmung ist nicht nur verletzt, wenn der Staat oder Private ohne jede Kontrolle auf Daten des Betroffenen zugreifen könnte. Es ist auch dann verletzt, wenn man im Wege der Auslegung einer Vorschrift das Selbstentscheidungsrecht des Betroffenen im Hinblick auf seine informationelle Selbstbestimmung verletzen würde. Dem Staat steht es insofern nicht zu, privatautonome Entscheidungen des Betroffenen als solche nicht zu respektieren und stattdessen staatlicherseits den Betroffenen vor sich selbst zu schützen. Würde man § 18 III PassG und § 4 II PersAuswG so verstehen, dass selbst bei ausdrücklicher Einwilligung des Betroffenen der Personalausweis oder Pass nicht zur Identifizierung von Flugdaten verwendet werden kann, würde dies am Grundsatz der informationellen Selbstbestimmung vorbeigehen und diesen verletzen.

Insofern ist § 4 BDSG in die Auslegung der genannten Ausweisvorschriften einzubeziehen. Wenn der Betroffene der Nutzung seiner Ausweisdaten ausdrücklich zustimmt, ist das Luftfahrtunternehmen zur Verwendung der Daten berechtigt. Im vorliegenden Fall entscheidet der Betroffene selbst, wie er sich identifizieren möchte. Er stimmt also nicht nur einfach den AGB eines Unternehmens zu, sondern entschei-

22 *VG Aachen*, DuD 2009, 192 = BeckRS 2008, 38079.
23 So ausdr. *Medert/Süssmuth* (o. Fußn. 18), § 18 PassG Rdnrn. 6 f.
24 *Ehmann*, in: *Simitis* (o. Fußn. 8), § 10 Rdnr. 15.
25 *Wilde*, in: *Wilde*, BayDSG, Art. 8 Rdnr. 4.
26 So ausdrücklich *Medert/Süssmuth* (o. Fußn. 18), § 18 PassG Rdnrn. 6 f.
27 Zu diesen Beispielen s. *Medert/Süssmuth* (o. Fußn. 18), § 18 PassG Rdnrn. 6 und 10.
28 S. *BVerfGE* 65, 1 (42) = NJW 1984, 419; *BVerfGE* 113, 29 (46) = NJW 2005, 1917; *BVerfGE* 115, 166 (188) = NJW 2006, 976.
29 *BVerfGE* 75, 1 (43) = NJW 1984, 419; *BVerfGE* 84, 192 (194) = NJW 1991, 2411.

det privatautonom über das „Wie" der Identifizierung. Er steuert auch technisch den Auslesevorgang, indem er – aus freien Stücken – sein Ausweispapier durch den Scanner zieht. Dem Staat fehlt hier eine Handhabe, solch selbstbestimmtes Verhalten zu ahnden und den Betroffenen vor sich selbst zu schützen.

Grundsätzlich ist die Verwendung von Personalausweisdaten durch Private auch nicht ungebräuchlich.

So sei auf den Beschluss des *LG Frankfurt a. M.* in Sachen Fußballweltmeisterschaft hingewiesen[30]. Hier wurde der FIFA zugebilligt, die Nummern von Personalausweisen vorübergehend und anlässlich des Besuchs eines Fußballspiels der Weltmeisterschaft 2006 zu speichern. Das *LG Frankfurt a. M.* verwies auf die Notwendigkeiten einer vorbeugenden Gefahrenabwehr, und zugebilligt wurde der FIFA eine Einlasskontrolle, die nicht auf die Überprüfung der Personaldaten beschränkt werden könne. „Insbesondere mit Hilfe des Passfotos dürfte die Identität da nicht zuverlässig zu erkennen sein, wenn das Gesicht des Karteninhabers, wie zunehmend üblich, ganz oder teilweise bemalt ist". Aus diesen Gründen sah das Gericht überwiegende Sicherheitsbelange der Gesamtheit der Besucher im Vorrang vor dem Recht auf informationelle Selbstbestimmung.

Dementsprechend sieht § 1 VI PersAuswG auch die passenden Eigentums- und Besitzverhältnisse am Personalausweis vor. Hiernach bleibt der Personalausweis Eigentum der Bundesrepublik Deutschland, der Ausweisinhaber ist Besitzer des Ausweises. Insofern ist das körperliche Eigentum an dem Dokument selbst geregelt. Davon ist im Umkehrschluss zu unterscheiden, wer Inhaber der darauf gespeicherten Daten ist. Die Daten als solche sind nicht eigentumsfähig, sondern Gegenstand immaterialgüterrechtlicher Befugnisse. Ein solches ist auch das allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung. Immaterialgüterrechtliche Befugnisse der Bundesrepublik Deutschland in Bezug auf die auf dem Pass oder Personalausweis gespeicherten Daten sind nicht ersichtlich.

VI. Ergebnis

Die Verwendung von Ausweisdaten im Rahmen des Automaten-Check-In verstößt nicht gegen § 18 III PassG und § 4 III PersAuswG. Es liegt weder eine Speicherung noch ein Abruf im Sinne dieser Vorschriften vor. Selbst wenn man aber die Vorschriften entgegen ihrem Wortlaut auf den Check-In bezieht, beruht die Nutzung der Daten auf einer freiwilligen Entscheidung des Kunden, so dass der Schutzzweck der Vorschriften nicht tangiert ist. ■

30 *LG Frankfurt a. M.*, Beschl. v. 12. 6. 2006 – 2/1 S 111/06, BeckRS 2007, 06772.

Dr. Jasper Finke, LL. M. (Columbia), Halle/Saale*

Warum das „Burka-Verbot" gegen die EMRK verstößt

Der Vorstoß des belgischen Parlaments, die Verschleierung in der Öffentlichkeit zu verbieten, hat europaweit politische Zustimmung gefunden. Als Rechtfertigung wird auf den Schutz der Frauen selbst, die öffentliche Sicherheit und den Schutz der Demokratie verwiesen. Eine Analyse dieser Argumente zeigt jedoch, dass sie nicht haltbar sind. Das Verbot verstößt gegen die in der EMRK garantierte Religionsfreiheit und das Recht auf Privatsphäre.

I. Einleitung

Das belgische Parlament hat am 29. 4. 2010 als erste europäische Volksvertretung ein so genanntes „Burka-Verbot" beschlossen und damit offensichtlich die gesellschaftlichen Zeichen der Zeit erkannt: Während das französische Parlament am 13. Juli dem belgischen Vorbild folgte, werden entsprechende Vorhaben in den Niederlanden und der Schweiz derzeit noch diskutiert[1]. Hinter dem Schlagwort „Burka-Verbot" verbirgt sich die Verbannung von Kleidungsstücken, die das Gesicht ganz oder hauptsächlich verhüllen. Es bezieht sich vor allem auf die aus Afghanistan stammende Burka, ein Ganzkörperschleier, der mittels eines Stoffgitters auch das Gesicht bedeckt, sowie den aus dem arabischen Raum bekannten Niqab, ein Kopftuch, das nur einen relativ schmalen Sehschlitz lässt[2]. Bemerkenswert ist, dass das Verbot den gesamten öffentlichen Raum betreffen wird, z. B. Straßen, Plätze und öffentliche Verkehrsmittel. Ferner sieht das Gesetz Bußgelder in Höhe von 15 bis 25 Euro oder Haft von bis zu sieben Tagen vor. Ausgenommen sind bestimmte Berufsbekleidungen wie die von Feuerwehrleuten sowie Helme von Motorradfahrern aber auch Karnevalsverkleidungen.

Sicherlich, die Vollverschleierung stellt im Alltag der europäischen Staaten für die Mehrheit einen Fremdkörper dar. Deren heutige Lebensweisen und Vorstellungen von Gleichberechtigung lassen jegliche Form der Vollverschleierung als Symbol der Unterdrückung der Frau, als Negation ihrer Würde und „unserer" Werte erscheinen[3]. Insbesondere das Stoffgitter der Burka ruft Assoziationen von Eingesperrtsein hervor. Nicht umsonst ist sie als „mobiles Gefängnis" bezeichnet worden[4].

Dieser Befund sagt aber zunächst mehr über die Wahrnehmungen und Wertungen der Mehrheitsgesellschaft aus als über die der Burkaträgerinnen. Sie werden bzw. können nur in den seltensten Fällen zu diesem Problem gehört werden. Das heißt natürlich nicht, dass alle voll verschleierten Frauen die Verschleierung freiwillig tragen. Die entscheidende Frage lautet jedoch: Rechtfertigen das Unbehagen der Mehrheitsgesellschaft und wahrscheinliche Fälle von Unterdrückung ein Verbot der Vollverschleierung im öffentlichen Raum?

* Der Autor ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Öffentliches Recht, Europarecht und Internationales Wirtschaftsrecht an der Juristischen und Wirtschaftswissenschaftlichen Fakultät der Martin-Luther-Universität Halle-Wittenberg.

1 Der Text des belgischen Parlamentsbeschlusses ist im Internet unter http://www.senate.be/www/?MIval=dossier&LEG=4&NR=1762&LANG=fr erhältlich. Der Wortlaut des vom französischen Parlament beschlossenen Gesetzes ist im Protokoll der Sitzung vom 23. 6. 2010 Nr. 2648 abgedruckt (www.assemblee-nationale.fr/13/rapports/2648.asp), auf das in der Abstimmung vom 13. 7. 2010 verwiesen wird (www.assemblee-nationale.fr/13/cri/2009-2010-extra/20101016.asp #P371-73265).

2 Zu unterschiedlichen Verschleierungsformen im Islam vgl. *Knieps*, Geschichte der Verschleierung der Frau im Islam, 2. Aufl. (1999), S. 77 ff.

3 Vgl. die Äußerungen belgischer Politiker, zitiert in SPIEGEL ONLINE, Bann per Gesetz – Belgisches Parlament stimmt für radikales Burka-Verbot, 29. 4. 2010, abrufbar unter http://www.spiegel.de/politik/ausland/0,1518,692153,00.html.

4 Vgl. die Äußerungen des belgischen Abgeordneten *Bart Sommers*, sueddeutsche.de, Belgien – Parlament beschließt Burka-Verbot, 30. 4. 2010, abrufbar unter http://www.sueddeutsche.de/politik/772/509899/text.