

An das  
Verwaltungsgericht Gelsenkirchen  
Bahnhofsvorplatz 3

Bochum, 19.11.2007

45879 Gelsenkirchen

## **Klage**

des Rechtsanwalts Michael Schwarz, Hellweg 21-23, 44787 Bochum

(Klägers)

gegen

die Ordnungsbehörde der Stadt Bochum als Passbehörde

(Beklagte)

wegen: Erteilung eines Reisepasses

Ich erhebe Klage mit dem Antrag, die Beklagte unter Aufhebung des Ablehnungsbescheides vom 8. November 2007 zu verpflichten, mir den beantragten Reisepass zu erteilen, ohne Fingerabdrücke von mir zu erfassen.

Auf anliegende Erklärung zum Verwaltungsvorgang vom 8. November 2007 wird Bezug genommen.

## **Begründung**

Die obligatorische Erfassung von Fingerabdrücken bzw. die Nichterteilung von Reisepässen – hier: unter Berufung auf § 6 Abs. 2 S. 3, § 4 Abs. 4 und Abs. 3 S. 1 des Passgesetzes vom 20. Juli 2007 in Verbindung mit der Verordnung (EG) Nr. 2252/2004 des Rates der Europäischen Union vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten – verstößt gegen höherrangiges Recht.

Beklagt wird die Verletzung des Rechts auf informationelle Selbstbestimmung bzw. die Verletzung des Rechts auf Freizügigkeit der Person sowie Verstöße gegen Rechtsstaats- und Demokratiegebote nach dem Grundgesetz sowie nach dem europäischen Gemeinschaftsrecht. Die Verletzungen und Verstöße sind dermaßen breit, tief und weitreichend sowie derart komplex, dass die Klagebegründung hier Angemessenerweise in drei Abschnitten erfolgt<sup>1</sup>: Zunächst werden die grundlegenden Aspekte festgestellt und weiter historisch entwickelt (1). Sodann wird die Rechtswidrigkeit der beklagten Maßnahme im Einzelnen dargelegt (2). Schließlich werden weitere Perspektiven eröffnet (3).

### **1 Grundlagen**

Jedes Artefakt, z. B. ein Reisepass, ist lediglich aus dem Sinn deutbar und verständlich, den menschliches Handeln (von möglicherweise sehr verschiedener Zielrichtung) der Herstellung und Verwendung dieses Artefakts verlieh (oder verleihen wollte); ohne Zurückgreifen auf ihn bleibt er gänzlich unverständlich. Das Verständliche an einem Reisepass ist also die Bezogenheit menschlichen Handelns darauf, entweder als „Mittel“ oder als „Zweck“, der dem oder den Handelnden vorschwebte, und woran ihr Handeln orientiert wurde (vgl. *Max Weber*, *Wirtschaft und Gesellschaft*, 5. Aufl., Tübingen 1976, 1. Halbband, S. 3).

So sind denn offenbar grundlegende Gesichtspunkte im Zusammenhang mit der obligatorischen Erfassung von Fingerabdrücken solche des Rechts und solche der Technik. Beides kann - wie jegliches Menschenwerk - nur aus seiner Idee begriffen werden. Das Recht wird von seiner sozialen Funktion her gesehen und aus seinem Zweck abgeleitet, soziale Ordnungen aufrechtzuerhalten und auszugestalten (vgl. *Creifelds*, *Rechtswörterbuch*,

<sup>1</sup> Die Abschnittsgliederung erfolgt mit Ziffern. Der Text findet sich mit Worten kurz vorbezeichnet.

16. Aufl. (2000), Stichwort „Rechtsphilosophie“). Danach ist Rechtswissenschaft die Erkenntnis vom gesellschaftlichen „Sein“ und „Sollen“, mithin: eine normative Gesellschaftswissenschaft, und sonst gar nichts. Technik hingegen sind alle Maßnahmen, Einrichtungen und Verfahren, die dazu dienen, die Erkenntnisse der Naturwissenschaften für den Menschen praktisch nutzbar zu machen (vgl. *Duden*, Deutsches Universalwörterbuch, 4. Aufl. (2001), Stichwort „Technik“).

Technisch grundlegende Aspekte im Zusammenhang mit der obligatorischen Erfassung von Fingerabdrücken stammen aus der Biometrie und Daktyloskopie, den Anwendungen von „AFIS“ (Automatisierten-Fingerabdruck-Identifikations-Systemen) und der Technologie von „RFID“ (Radio-Frequenz-Identifikation). Rechtlich grundlegende Aspekte im Streitgegenständlichen Zusammenhang stammen aus dem Verfassungs- und Gemeinschaftsrecht, dem Datenschutzrecht und dem Pass- sowie Personalausweisrecht. Aber damit noch nicht genug.

Politische und ökonomische Machtinteressen muss man immer hinzudenken, nicht nur für die Technik, sondern auch für das Recht. Die „Rationalität des Rechts“ im Unterschied zur „Willkür der Macht“ gebietet, das gesellschaftliche „Sein“ und „Sollen“ umfassend in Betracht zu ziehen. Daraus folgt der Grundsatz, keine gesellschaftstheoretische Verkürzung bei den Wirklichkeitsurteilen (Seinssätzen) und Werturteilen (Sollenssätzen) vorzunehmen, wenn sie denn der Sache nach einschlägig sein können. Bei darauf eingehender Betrachtung erweist sich im Falle der obligatorischen Erfassung von Fingerabdrücken, dass die rechtliche wie technische „Bezogenheit menschlichen Handelns darauf“ beeinflusst wird von ökonomisch-, „partikularen“ und politisch-, „antagonistischen“ Interessen, die sich aber in den Medien von „Globalisierung“, „Terror“ und „Krieg“ auch wechselseitig so verstärkt haben, dass sie schier allenthalben „Totalitätsansprüche“ erheben.

Ohne derartige Herrschafts- und Machtansprüche, die „Anlass“ und „Förderung“ u.a. aus den tragischen Ereignissen des 11. September 2001 und anderen Ausnahmeereignissen nahmen, wäre die obligatorische Erfassung von Fingerabdrücken letztlich ebenso wenig verständlich wie die „präventive polizeiliche Rasterfahndung“ (vgl. *BVerfG*, NJW 2006, 1939 ff.), die „vorbeugende/ vorsorgende Telekommunikationsüberwachung“ (vgl. *BVerfG*, NJW 2005, 2603 ff.), der „Große Lauschangriff“ (vgl. *BVerfG*, NJW 2004, 999 ff.), „heimliche Online-Durchsuchungen“ (vgl. *BGH*, MMR 2007, 174 ff.), die „automatisierte Abfrage von Kontenstammdaten“ (vgl. *BVerfG*, NJW 2007, 2464 ff.), die „Videoüberwachung“ (vgl.

*BVerfG*, NVwZ 2007, 688) und das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ (vgl. BT-Drucksache 16/5846; *Jens Eckhardt*, CR 2007, 336 ff.), mithin auch die „Vorratsspeicherung von Telekommunikationsdaten“ (vgl. Abl. L 105, 54 ff.; *Sabine Leutheusser-Schnarrenberger*, ZRP 2007, 9 ff.), also Aufschluss darüber, wer wann mit wem von wo aus kommuniziert hat, sei es per Telefon, Handy, Email, oder Internet..., u.v.a.m.

„So wird der Mensch maschinenlesbar, nehmen George Orwells düstere Visionen vom überwachten Menschen reale Konturen an“ (vgl. *Christine Hohmann-Dennhard*, Freiräume – Zum Schutz der Privatheit, NJW 2006, 545 ff. [547], mit Verweis auf: *George Orwell*, 1984, 27. Aufl., Berlin 2005). Das „Idealbild“ des gläsernen Bürgers teilt die Staatsverwaltung mit den zentralen Einrichtungen der Wirtschaftsgesellschaft:

Anders als der Staat, der sämtliche Daten zu einem Gesamtbild der Person vereinen möchte, zielt der Markt zunächst nicht auf eine zentrale Erfassung. Jeder Konkurrent möchte einen kommerziellen Informationsvorteil erlangen und die Daten seiner Kunden für sich behalten. Gleichzeitig sind die Unternehmen zum ständigen Ausbau ihrer Datenbasis gezwungen, um in der Konkurrenz zu überleben. So braucht am Ende die Obrigkeit viele Daten gar nicht mehr selbst zu erheben. Sie kann auf alles zurückgreifen, was private Einrichtungen bereits gesammelt haben - wie etwa im vorbezeichneten Falle der Vorratsspeicherung von Telekommunikationsdaten. Und manchmal bieten die Firmen diese Dienstleistung schon von sich aus an, wenn ihnen ein lukrativer Suchauftrag winkt. Schließlich zwingt der Staat die Menschen sogar dazu, ihm *und* Dritten nicht nur *personenbezogene*, sondern selbst *personenbezogene* Daten von sich preiszugeben - wie etwa im Falle der obligatorischen Erfassung von Fingerabdrücken. Dafür bieten längst beteiligte Unternehmen am Markt dann sogleich weitere technische Anwendungen feil. Die unheilige Allianz der Institutionen sorgt so dafür, dass sich das Individuum an keinem Ort vor fremden Blicken mehr sicher fühlen kann (vgl. *Wolfgang Sofsky*, Verteidigung des Privaten, München 2007, S. 120).

Wissen *ist* Macht (nach dem englischen Philosophen *Francis Bacon*, 1561-1626). Die Einheit der Erkenntnis, ohne welche alles Wissen nur Stückwerk ist, *verlangte* die Aufklärung (nach dem deutschen Philosophen *Immanuel Kant*, 1724-1804). Mehr Wissen *bedeutet* folglich mehr Macht, *beansprucht* aber auch mehr Aufklärung. So bezeichnet man eine von

Rationalismus und Fortschrittsglauben bestimmte europäische geistige Strömung, die sich gegen Aberglauben, Vorurteile und Autoritätsdenken wendet:

*„Aufklärung ist der Ausgang des Menschen aus seiner selbstverschuldeten Unmündigkeit. Unmündigkeit ist das Unvermögen sich seines Verstandes ohne Leitung eines anderen zu bedienen. Selbstverschuldet ist diese Unmündigkeit, wenn die Ursache derselben nicht am Mangel des Verstandes, sondern der EntschlieÙung und des Mutes liegt, sich seiner ohne Leitung eines anderen zu bedienen. Sapere aude! Habe Mut dich deines eigenen Verstandes zu bedienen!“* (vgl. Immanuel Kant, Was ist Aufklärung?, Göttingen 1967, S. 55).

Das humanistische Ideal der Aufklärung ist ein vornehmes Werturteil, kein dahinreichendes Wirklichkeitsurteil. Geheimdienstliche Aufklärung liegt der wirtschaftlichen und politischen Macht deutlich näher. Tatsächlich am meisten davon hat, wer über heimliches Wissen verfügt. Und ebenso „klandestin“ - wie vorbezeichnete Rechtsprechung dies eindrucksvoll belegt – entzieht sich die Exekutivgewalt der öffentlichen Kontrolle:

*„Die traditionelle Macht ist diejenige, die sich sehen lässt, die sich zeigt, die sich kundtut und die die Quelle ihrer Kraft gerade in der Bewegung ihrer ÄuÙerung findet... Ganz anders die Disziplinarmacht: sie setzt sich durch, indem sie sich unsichtbar macht, während sie den von ihr Unterworfenen die Sichtbarkeit aufzwingt. In der Disziplin sind es die Untertanen, die gesehen werden müssen, die im Scheinwerferlicht stehen, damit der Zugriff der Macht gesichert bleibt. Es ist gerade das ununterbrochene Gesehenwerden, das ständige Gesehenwerdenkönnen,... was das Disziplinarindividuum in seiner Unterwerfung festhält... in einem Objektivierungsmechanismus einfängt“* (vgl. Michel Foucault, Überwachen und Strafen, 1. Aufl., Frankfurt a. M. 1994, S. 241). Mit anderen Worten:

*„Von allen jenen Gewalten aber, welche das individuelle Handeln zurückdrängen, ist die unwiderstehlichste... die rationale „Disziplin“. Sie ist inhaltlich nichts anderes als die konsequent rationalisierte, d.h. planvoll eingeschulte, präzise, alle eigene Kritik bedingungslos zurückstellende, Ausführung des empfangenen Befehls, und die unablässige innere Eingestelltheit ausschließlich auf diesen Zweck... Die „Disziplin“... ist etwas „Sachliches“ und stellt sich in unbeirrter „Sachlichkeit“... jeder Macht zur Verfügung, welche auf ihren Dienst reflektiert und sie zu schaffen weiß“* (vgl. Max Weber, Wirtschaft und Gesellschaft, 5. Aufl., Tübingen 1976, 2. Halbband, S. 681 f.).

„Sichtbarkeit“, das „ständige Gesehenwerdenkönnen“ und die „Disziplin“ müssen in der Entwicklung beurteilt werden, die die Erfassung von Fingerabdrücken nahm und nehmen „soll“.

## 1.1 Erste Entwicklungen

Die Erfassung von Fingerabdrücken in Pass- und Personalausweisdokumenten weist zurück auf die Erfindung der Daktyloskopie (griechisch: *Daktylos* = Finger, *skopein* = schauen). Englische Kolonialbeamte hatten sie als Mittel der sozialen Kontrolle entwickelt. Um die Auszahlung von Pensionen zu kontrollieren und Identitätsschwindeleien zu unterbinden, ließ *William James Herschel*, der von 1853 bis 1878 im Distrikt Hooghly (Bengalen) arbeitete, die Zahlungsempfänger mit ihrem Fingerabdruck registrieren und den Erhalt der Pension mit ihrem Abdruck quittieren. Später führte er die Daktyloskopie auch im Gefängnis seines Distrikts ein, um Verwechslungen zu vermeiden. Die koloniale Rechts- und Herrschaftsordnung ging von der Ungleichheit der Kolonisierten und Kolonisten aus. An den beengenden Rahmen der heimischen Rechtsordnungen mit ihren rechtsstaatlichen Sicherungen war sie nicht gebunden. Die Beamten konnten in diesem Labor der europäischen Moderne wechselnde Methoden der Disziplinierung und Ausweitung staatlicher Macht erproben und versuchten, Wünsche nach lückenloser Erfassung und Kontrolle durchzusetzen. Gelegentlich brachte die Kolonialbürokratie dabei Innovationen hervor, die sich in ihrer Effektivität auch für das Mutterland empfahlen; so auch den Fingerabdruck (vgl. *Miloš Vec*, *Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933)*, 1. Aufl., Baden-Baden 2002, S. 48 ff., m. w. N.).

Die Kriminalisten griffen die Fingerschau auf und verbreiteten sie innerhalb weniger Jahre weltweit. Bemerkenswert an dieser Erfolgsgeschichte war die Eigendynamik, die die neuen Techniken entfalteten. Die bloße Existenz der modernen Verfahren genügte in Verbindung mit dem Versprechen der Effektivität für den Beginn ihrer kriminalistischen Karriere in den staatlichen Institutionen. Es ging den Kriminalisten darum, ihre Kontrollkapazität zu steigern. Die Anwendungsfelder standen also nicht von vorneherein fest, sondern wurden erst nach und nach erschlossen. Die Kriminalisten fokussierten auf die Eigentums- und Gewaltkriminalität in der Großstadt, und sie betrieben von hier aus ihre Selbstlegitimierung mittels von ihnen entworfener Bedrohungsszenarien. Es war ein vages Versprechen von verbesserter Überwachung und sozialer Kontrolle, das ihren Erfindungsreichtum bezüglich der neuen

Techniken antrieb. Die Kriminalisten gerierten sich als Techniker, die das soziale Problem der Kriminalität mit den staunenswerten neuen Verfahren technisch in den Griff bekommen wollten (vgl. *Miloš Vec*, *Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933)*, 1. Aufl., Baden-Baden 2002, S. 65 ff., m. w. N.).

Dass der Apparat und seine Funktionäre auch subjektive Interessen haben könnten, kam in diesen Diskursen mit ihrem selbstsicheren Wahrheitsethos nicht vor. Die Individualität der ermittelnden Kriminalisten und der beweismäßigenden Richter wurde ausgeblendet. Die Idealvorstellung von der „objektiven“ Technik ließ jene Personen verschwinden, die sie bedienten und von ihr profitierten. Das wurde aber keineswegs als Nachteil begriffen, im Gegenteil. Noch jedes Versprechen technologisch garantierter Wahrheitsfindung im Prozess begrüßte und begrüßt diese Entpersonalisierung:

*„Ich erstrebe einen Strafprozess, der – lassen sie es mich extrem formulieren – frei ist von Zeugen und Sachverständigen. Der sich ausschließlich gründet auf dem wissenschaftlich nachprüfbar, messbaren Sachbeweis. Nach meiner Theorie wäre, so schrecklich das klingt, auch der Richter entbehrlich“* (vgl. *Horst Herold*, der frühere Präsident des Bundeskriminalamts, zit. nach: *Miloš Vec*, *Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933)*, 1. Aufl., Baden-Baden 2002, S. 79, m. w. N.).

Das Versprechen der Wissenschaftlichkeit aktualisiert sich mit jeder neuen Erfindung. Durch Multiplikation der neuen Techniken vervielfacht sich das kriminalistische Selbstbewusstsein:

*„In der Praxis erlebe ich häufig, dass Richter dem Gutachter folgen. Wenn man das weiterdenkt, könnte herauskommen, dass man das Gericht eigentlich nicht mehr braucht. Gutachter würden auch reichen... Ich selbst habe als Gutachter in einem Mordfall mit funktioneller Bildgebung die Glaubwürdigkeit einer Zeugin belegt“* (vgl. *Hans Markowitsch*, in: *DER SPIEGEL* Nr. 31 vom 30. Juli 2007, S. 122 f.).

Auch im späten 19. Jh. erschlossen sich erst nach und nach die neuen Anwendungsfelder. Wenn die Kriminalisten findig waren, konnten sie ihre Sicherheitsversprechungen gegenüber der Politik und der Gesellschaft steigern. Dem einzelnen Kriminalbeamten bot die Werbung für neue technische Methoden der Personenidentifikation Karrierechancen. Er konnte sich in der Polizei hervortun und Führungspositionen beanspruchen, wenn er den Erkennungsdienst

erfolgreich modernisiert hatte. Aber auch als Gruppe profilierten sich die Kriminalisten durch die neuen Kontrollmöglichkeiten, die ihre Bedeutung unterstrichen und zu einem höheren sozialen Status führen konnten. Das Ziel war eine kollektive Selbstaufwertung der Kriminalbeamten (vgl. *Miloš Vec*, Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933), 1. Aufl., Baden-Baden 2002, S. 79 f., m. w. N.).

Die „Volksdaktyloskopie“, dass also die gesamte Menschheit amtlich daktyloskopiert werde, darauf wollten die Protagonisten unter den Kriminalisten schon vor nunmehr rund einhundert Jahren hinaus: eine internationale Passreform und die Verwendung der Fingerabdrücke in den Legitimationspapieren aller Menschen (vgl. *Robert Heindl*, Passreform, in: Archiv für Kriminal-Anthropologie und Kriminalistik 32 (1908), S. 162 ff.; ebenso: *Luigi Tomellini*, Des modifications a introduire dans les passpotes, in: Archives D'Anthropologie Criminelle 23 (1908), S. 508 ff.).

Mit diesem „Totalitätsanspruch“ gingen die Kriminalisten dann propagandistisch hausieren: Sie entwarfen Bedrohungsszenarien, die den Einsatz aller kriminalistischen Mittel rechtfertigen sollten. Sie schilderten die Vorteile des daktyloskopischen Verfahrens auch jenseits des konkreten Tatverdachts oder der konkreten Kriminalprävention. Sie priesen die Einfachheit und Sicherheit des Verfahrens, das Transfers in andere Bereiche scheinbar zwingend nahe legte. Sie argumentierten mit den Sicherheitszuwächsen, von denen nicht nur der Staat, sondern die ganze Gesellschaft und Privatunternehmen profitieren könnten. Denn nicht nur Polizei und Justiz, auch der moderne Sozial- und Wohlfahrtsstaat, auch die Wirtschaft könnte zur Erfüllung ihrer Aufgaben funktionierende Identifikationstechniken gebrauchen. Ebenso wünschten sich vielleicht die Bürger individuell die Möglichkeit ihrer zuverlässigen Identifikation, etwa nach Katastrophen und Unglücksfällen... Jedenfalls war das Potential der Daktyloskopie bei weitem noch nicht ausgeschöpft: Kontrollmöglichkeiten und Sicherheitsgewinne allenthalben! (vgl. *Miloš Vec*, Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933), 1. Aufl., Baden-Baden 2002, S. 106 ff., m. w. N.).

Eine Reform des Passwesens wäre daher gleichbedeutend mit der Erschließung des größtmöglichen Anwendungsfelds für dieses kriminalistische Identifizierungsverfahren gewesen. Als Vorbilder galten den Kriminalisten international Portugal, das 1912 den Fingerabdruck des Inhabers in den Pass aufgenommen hatte, und Brasilien. In Deutschland schrieben nur die Länder Sachsen und Bayern den Abdruck des rechten Zeigefingers vor. Die Kriminalisten for-

dernten vehement eine Ausweitung auf Reichsebene durch eine reichsrechtliche Regelung. Die fakultative, d.h. freigestellte Aufnahme von Fingerabdrücken in den Pass durch die Bekanntmachung des Reichskanzlers vom 24. Juni 1916 (vgl. Reichsgesetzblatt 1916, Nr. 143, S. 601 ff. [609]), eine juristische Technikermöglichkeit auf halber Strecke, genügte ihnen nicht (vgl. *Miloš Vec*, Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933), 1. Aufl., Baden-Baden 2002, S. 110 ff., m. w. N.). Ihr Hochmut kam vor dem Fall:

In Argentinien hatte *Juan Vucetich* 1916 mit seinem Vorstoß, die ganze Bevölkerung daktyloskopisch zu erfassen, eine wahre Revolution an Ablehnung ausgelöst. Das Projekt wurde für verfassungswidrig erklärt, die bereits gesammelten Daten vernichtet. *Vucetich* verglich das Scheitern seines Projekts pathetisch mit der Zerstörung der Bibliothek von Alexandria (vgl. *Miloš Vec*, Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933), 1. Aufl., Baden-Baden 2002, S. 111, m. w. N.).

Es blieb bei der Daktyloskopierung von Kriminellen, Tatverdächtigen und gesellschaftlichen Randgruppen (etwa den ausländischen landwirtschaftlichen Arbeitern). Die Hoffnungen, die Datenbasis zu erweitern, waren zu sehr auf die Kreise der Kriminalisten beschränkt, um eine Ausweitung des Fundus auf andere gesellschaftliche Gruppen oder gar die Allgemeinheit zu erwirken. Die von den Kriminalisten geforderte technisch induzierte Erfassung der Individuen zu Präventionszwecken blieb gesellschaftlich unerwünscht. Die damit verknüpften Sicherheitsversprechen überzeugten nicht (vgl. *Miloš Vec*, Die Spur des Täters - Methoden der Identifikation in der Kriminalistik (1879-1933), 1. Aufl., Baden-Baden 2002, S. 111 f., m. w. N.).

Auch die erstmalige gesetzliche Normierung der Daktyloskopie in Deutschland schrieb 1933 nur das fest, was ohnehin schon seit langem praktische Übung war, und auch heute noch gilt:

*„Soweit es für die Zwecke der Durchführung des Strafverfahrens oder für die Zwecke des Erkennungsdienstes notwendig ist, dürfen Lichtbilder und Fingerabdrücke des Beschuldigten auch gegen seinen Willen aufgenommen und Messungen oder (n.F.: „und“) ähnliche Maßnahmen an ihm vorgenommen werden“* (vgl. Reichsgesetzblatt 1933, Teil I, S. 995 ff. [1000]; § 81 b StPO).

In Deutschland hatten dann nur noch einmal die Nationalsozialisten in der „Verordnung über Kennkarten vom 22. Juli 1938“ (vgl. Reichsgesetzblatt, Jahrgang 1938, Teil I, S. 913 ff.) in Verbindung mit der ersten und dritten „Bekanntmachung über den Kennkartenzwang vom 23. Juli 1938“ (vgl. Reichsgesetzblatt, Jahrgang 1938, Teil I, S. 921 f.) zur Personenkennzeichnung bestimmt, dass volljährige „männliche deutsche Staatsangehörige“ und „Juden, die deutsche Staatsangehörige sind“, „Fingerabdrücke von sich nehmen zu lassen“ haben.

Die „Verordnung über die Reisepässe von Juden vom 5. Oktober 1938“ (vgl. Reichsgesetzblatt 1938, Teil I, S. 1342) führte dann das »J« im Pass als Personengruppenkennzeichen ein...

## 1.2 Weitere Entwicklungen

Erst Zug um Zug enthüllte sich die Tatsache, dass Totalitarismus nie positive Ordnung im Sinne allgemeiner Sicherheit sein kann, weil er wesensmäßig jede wirksame Kontrolle ausschließt und unter Ordnung nur die bedingungslose Durchsetzung des eigenen Willens versteht. Der Nationalsozialismus, welcher die kriminalistische „Volksdaktyloskopie“ einfach vereinnahmt und in seinem Sinne verknüpft hatte, machte für die Nachwelt noch einmal unmissverständlich klar, dass *„identifiziert werden kann eine Person immer auf zwei unterschiedliche Weisen: zum einen als Einzelperson im polizeilichen Sinn; zum anderen als Rechtssubjekt, das durch kollektiv zugeteilte Zugangs- oder Ausschlusskriterien definiert ist. Kurz, Personen werden durch Dokumente identifiziert, deren Inhalt und Gebrauch sie selbst nicht bestimmen können“* (vgl. Valentin Groebner, Der Schein der Person – Steckbrief, Ausweis und Kontrolle im Europa des Mittelalters, München 2004, S. 176 ff. [179]).

Beim Einsatz biometrischer Verfahren ist ferner zu bedenken, dass die Verknüpfung biometrischer Daten (z. B. der Fingerabdrücke) mit einer natürlichen Person eine Verknüpfung darstellt, die über den eigentlichen Einsatzzweck (z. B. die Authentifizierung gegenüber einer Smartcard) hinaus besteht und technisch - im Gegensatz zu Benutzernamen und Passwörtern oder PIN's - auch in anderen Zusammenhängen verwendet werden kann: *„Jede Instanz, die sich in den Besitz der Verknüpfung gegebener biometrischer Daten mit einer natürlichen Person bringt, kann diese in einem neuen Sinne verwenden“* (vgl. Peter Biltzinger, Biometrie und Datenschutz, in: DuD 29 (2005), 726 ff. [731]).

Im „Gesetz über Personalausweise vom 19. Dezember 1950“ (vgl. Bundesgesetzblatt, S. 807) zog der Bundesgesetzgeber die bereichsspezifischen Konsequenzen aus der NS-Zeit wie folgt:

*„Raum für einen Fingerabdruck darf nicht vorgesehen werden“*, vgl. § 2 Abs. 2 Satz 2 PAuswG 1950.

*„Gleichzeitig treten die auf das Ausweiswesen bezüglichen Vorschriften des Gesetzes über das Pass-, das Ausländerpolizei- und das Meldewesen sowie das Ausweiswesen vom 11. Mai 1937 (Reichsgesetzbl. I S. 589) sowie die auf Grund dieses Gesetzes erlassenen Verordnungen, soweit sie Bestimmungen über Ausweise (Kennkarten) enthalten, außer Kraft“*, vgl. § 5 Abs. 2 PAuswG 1950.

Unter Berücksichtigung des Grundrechts auf informationelle Selbstbestimmung nach dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 (vgl. *BVerfG*, NJW 1984, S. 419 ff.) wurde der bereichsspezifisch gebotene Datenschutz im „Passgesetz vom 19. April 1986“ (vgl. Bundesgesetzblatt I, S. 537 ff.) und ebenso im „Gesetz über Personalausweise vom 19. April 1986“ (vgl. Bundesgesetzblatt I, S. 545 ff.) inhaltlich verstärkt, u.a. wie folgt:

*„Der Pass darf weder Fingerabdrücke noch verschlüsselte Angaben über die Person des Inhabers enthalten. Die Seriennummer und die Prüfziffern dürfen keine Daten über die Person des Passinhabers oder Hinweise auf solche Daten enthalten. Jeder Pass erhält eine neue Seriennummer“*, vgl. § 16 Abs. 1 PassG 1986 (vgl. § 3 Abs. 1 PAuswG 1986).

Ein wichtiges Anliegen der Bestimmung war es, sowohl verschlüsselte Angaben über die Person des Passinhabers zu verhindern, wozu auch Fingerabdrücke zählen, als auch die an sich zugelassenen Seriennummern und Prüfziffern datenschutzfest zu gestalten (vgl. *Hans-Joachim Ordemann*, Passrecht, Ausweisrecht, Melderecht des Bundes, München 1988, § 16). Mit dem Verbot der Aufnahme von verschlüsselten Angaben über die Person des Inhabers wurde verdeutlicht, dass der Pass *„keinerlei Informationen enthalten darf, die nicht für jeden Inhaber lesbar und verständlich sind“* (vgl. Bericht des BT-Innenausschusses zu der entsprechenden Vorschrift im Entwurf des PAuswG, in: BT-Drucks. 8/3498, S. 9).

In der Begründung des Regierungsentwurfs wurde weiter ausgeführt wie folgt: *„Durch das Verbot der Aufnahme personenbezogener Daten in die Seriennummer oder die Prüfziffern*

*soll verhindert werden, dass die Seriennummer oder die Prüfziffer die Funktion eines Personenkennzeichens übernehmen kann... Die Normierung der Pflicht, bei Neuausstellung eines Passes auch eine neue Seriennummer zu bestimmen, dient dem Persönlichkeitsschutz. Hierdurch wird verhindert, dass die Seriennummer des Passes ihren Inhaber lebenslang begleitet und dadurch als Surrogat eines Personenkennzeichens verwendet werden könnte“ (vgl. BT-Drucks. 10/3303, S. 15; zit. nach: Klaus M. Medert/ Werner Süßmuth, Pass- und Personalausweisrecht: Kommentar, Bd. 2, Passrecht, 2. Aufl., Köln 1992, § 16 Rdnr.4).*

Der menschliche Fingerabdruck ist ein einmaliges, klassifizierbares und nahezu unveränderliches Personenkennzeichen, das sich selbst bei schweren Verbrennungen wieder regeneriert (vgl. *Friedrich Geerds*, in: *Hans Groß/ Friedrich Geerds*, Handbuch der Kriminalistik, 10. Aufl., Berlin 1977, Band I, S. 450 ff., S. 568 ff.).

Als Fingerabdruck wird der Abdruck der Fingerbeere auf Gegenständen bezeichnet. Dieser Abdruck stellt das Hautleistenrelief des entsprechenden Fingers dar, die charakteristischen Täler und Erhebungen der Fingerkuppe. Voraussetzung dieses Abdrucks ist ein gewisses Quantum Emulsion (Schweiß oder Talg), das ständig von den Hautleisten abgesondert wird. Das Muster dieser schleifen-, wirbel- und bogenförmig angeordneten Hautleisten, die auch als Papillarlinien bezeichnet werden, ist einzigartig. Entgegen vielen anderen morphologischen Kennzeichen des Menschen ist deren Anordnung nicht vererbbar und bildet sich im Embryostadium aus. Der Fingerabdruck verändert sich nur bei Unfall, Krankheit, Verbrennungen oder anderen Verletzungen. Das Hautleistenrelief ist nach bestimmten Grundprinzipien, wie z. B. der Lage und den Richtungen der Schleifen oder der Position spezieller Verzweigungs- und Endpunkte von Hautleisten, den Minuzien, klassifizierbar (vgl. *Marco Breitenstein*, in: *Veronika Nolde/ Lothar Leger* (Hrsg.), Biometrische Verfahren, Köln 2002, S. 35).

Seit Ende 1992 arbeitet das Bundeskriminalamt (BKA) mit einem Automatisierten-Fingerabdruck-Identifikations-System. AFIS ist eine Datenbank mit Fingerbilddateien aus Straf- und Asylverfahren. Bei der Strafverfolgung werden am Tatort gefundene Fingerabdrücke mit den in AFIS gespeicherten Abdrücken verglichen. Im Asylverfahren wird festgestellt, ob die betreffende Person bereits einen Asylantrag gestellt hat. AFIS enthält Datenbestände mit Angaben zu allen zehn Fingern sowie einen Spurentatbestand mit nicht persönlich zugeordneten Fingerabdrücken (vgl. *Alexander Gruner*, Biometrie und informationelle Selbstbestimmung, Dresden 2005, S. 42).

Bei dem System werden Fingerabdrücke digital in das Computersystem eingelesen, automatisch klassifiziert und im Datenbestand recherchiert. Das neue Verfahren verkürzt die Eingabezeit von bisher 90 Minuten pro Person auf drei Minuten und erhöht die Trefferwahrscheinlichkeit auf 99%. Somit können zeitschnell Fingerabdrücke von Tatverdächtigen vollautomatisch mit dem Datenbestand des BKA verglichen werden, um Personen zu identifizieren. Da auch Tatortspuren eingegeben werden, kann festgestellt werden, ob eine bekannte Person als Spurenleger in Frage kommt. Hierbei beträgt die Trefferwahrscheinlichkeit 60%. Darüber hinaus ist es auch möglich, Tatortspuren untereinander zu vergleichen, um so Tatserien festzustellen, ohne den modus operandi zugrunde legen zu müssen und ohne den Täter zu kennen. Die Tatortfingerspuren zeigen dann, ob sie von ein und demselben Spurenleger stammen (vgl. *Robert Weihmann*, *Kriminalistik*, 6. Aufl., Hilden 2002, S. 91).

Die Abnahme von Fingerabdrücken bei Personen geschieht durch Einschwärzen mit Druckerfarbe und Abrollen der Finger auf Papier oder Karton. Seit Mitte 2000 werden Finger- und Handflächenabdrücke auch mit optoelektrischen Geräten, so genanntem „Life-Scan“, unmittelbar von der Haut digital eingelesen und mit PC-Druckern auf Papier gedruckt. Tatortfingerspuren können mit Kontrastmitteln oder mittels Schräglicht durch Fotografie gesichert werden. Die Haltbarkeit dieser Spuren ist sehr groß (vgl. *Robert Weihmann*, *Kriminalistik*, 6. Aufl., Hilden 2002, S. 92).

Im Erfassungsvorgang werden die Fingerabdrücke an der Erfassungsstation nach Einlegen des Fingerabdruckblattes automatisch eingelesen, digitalisiert, umfassend analysiert, codiert und zuletzt digital gespeichert. Jeder Erfassungsvorgang stößt automatisch einen Rechercheprozess im AFIS-Bestand an. Bei einem Treffer werden die gespeicherten Daten aus dem Bestand abgerufen und auf dem Bildschirm dem Daktyloskopen zum visuellen Vergleich der Fingerabdrücke angeboten. Die Entscheidung, ob zwischen den zum Vergleich anstehenden Fingerabdrücken Identität besteht, trifft ein Daktyloskop nach daktyloskopischen Regeln. Werden im Bestand keine identischen Fingerabdrücke vorgefunden, wird der Erfassungsvorgang mit der Speicherung der zugehenden Fingerabdrücke beendet (vgl. *Heiko Loesing*, in: *Bundeskriminalamt (Hrsg.), Aktuelle Methoden der Kriminaltechnik und Kriminalistik*, Wiesbaden 1995, S. 221 ff.).

AFIS führte zu einer höheren Effizienz des Erkennungsdienstes. Die kriminalistischen Erfolgsmeldungen ließen nicht lange auf sich warten. Doch die besten Fingerabdrücke nutzten nur etwas, wenn sie sich potenziell einordnen ließen. Wenn man denn nur genug Vergleichsmaterial hätte... In den USA begann das FBI bereits in der Zwischenkriegszeit mit der Registrierung und Klassifizierung der Fingerabdrücke von Personen, die nicht mit dem Gesetz in Konflikt geraten waren (vgl. *John Edgar Hoover*, Die Daktyloskopie der Unvorbestraften in USA, in: Archiv für Kriminologie 104 (1939), S. 29 f.). Es handelte sich dabei um die Inanspruchnahme der Bundespolizei durch Privatpersonen, die einen sicheren Zugriff auf ihre Identität im Fall eines Gedächtnisverlusts sicherstellen wollten. Hinzu kamen die Fingerabdrücke von Staatsangestellten. Das Militär registrierte ebenfalls seine Rekruten. Heute verwaltet die *Criminal Justice Information Services Division* des FBI mit vierzig Millionen Abdrücken von Nicht-Kriminellen eine ebenso große Datenmenge zu diesem Personenkreis wie zu den Kriminellen (vgl. *Peter Becker*, Dem Täter auf der Spur – Eine Geschichte der Kriminalistik, Darmstadt 2005, S. 133).

### **1.3 Letzte Entwicklungen**

Vor einigen Jahren erschien in zahlreichen Tageszeitungen eine auffällige ganzseitige Anzeige. Sie zeigte, wie das bei Anzeigen so üblich ist, lachende Menschen. Man sah eine Frau mit zwei Kindern, die von einem Mann mit Kamera abgelichtet wurden. Das meiste an dieser Anzeige war freilich unüblich. Es wurde für kein Produkt geworben. Die Anzeige geschaltet hatte keine Firma. Es war vielmehr das amerikanische Heimatschutzministerium, das mit riesigen Lettern in Deutschland für eine neue Identifizierungsprozedur warb: „*Der Flug nach Amerika dauert acht Stunden. Ihren Besuch sicherer zu gestalten, dauert nur einige Sekunden.*“ – Geworben wurde dafür, sich in das Unvermeidliche zu fügen und hinzugeben, was der amerikanische Staat gerne von uns ergreifen wollte: Eine digitale Aufnahme der Fingerabdrücke (vgl. *Miloš Vec*, Freiheit unter Verdacht, in: Blätter für deutsche und inter-nationale Politik 8/2007, S. 957).

Mit dem „Enhanced Border Security and Visa Entry Reform Act of 2001“ hat der US-Senat in Folge der Anschläge vom 11. September 2001 das Visa-Recht der USA verschärft (vgl. 107<sup>th</sup> Congress, 1<sup>st</sup> Session, H.R. 3525). Das Gesetz verlangt beispielsweise in Title II, Sec. 202 i.V.m. Title III, Sec. 303, dass ein neues interoperables elektronisches Strafverfolgungs- und Aufklärungssystem einen angemessenen biometrischen Identifikationsstandard

benutzt. Ausländer sollen nur noch mit maschinenlesbaren und fälschungssicheren Visa und Reisedokumenten mit biometrischen Merkmalen einreisen dürfen und alle Einreisepunkte der USA entsprechend mit Hard- und Software ausgestattet sein (vgl. *Alexander Gruner*, *Biometrie und informationelle Selbstbestimmung*, Dresden 2005, S. 60 f.).

Auf der Jahrestagung des Bundeskriminalamts vom 13. bis 15. November 2001 nahm der damalige Bundesinnenminister *Otto Schily* die Gelegenheit wahr, sich für die Annahme von biometrischen Merkmalen, insbesondere auch Fingerabdrücken, in Personalausweise und Visaanträge auszusprechen. Den Widerstand gegen die Aufnahme von Fingerabdrücken in Personalausweise hielt *Schily* für verfehlt. Im übrigen maß er der Prävention eine vorrangige Bedeutung bei (vgl. *Konrad Händel*, *Jahrestagung des Bundeskriminalamts (Mitteilung)*, in: *NJW* 2002, 277 [278]).

Und so apodiktisch weissagte das „Gesetz zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002“ (TBG) die „Volksdaktyloskopie“ ins 21. Jahrhundert:

*„Der Pass darf neben dem Lichtbild und der Unterschrift weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Passinhabers enthalten. Das Lichtbild, die Unterschrift und die weiteren biometrischen Merkmale dürfen auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden. Auch die in Absatz 1 Satz 2 aufgeführten Angaben über die Person (scil.: Familienname und ggf. Geburtsname, Vornamen, Doktorgrad, Ordensname/ Künstlername, Tag und Ort der Geburt, Geschlecht, Größe, Farbe der Augen, Wohnort, Staatsangehörigkeit) dürfen in mit Sicherheitsverfahren verschlüsselter Form in den Pass eingebracht werden“*, vgl. § 4 Abs. 3 PassG 2002/ Art. 7 Nr. 1 b) (3) TBG (vgl. § 1 Abs. 4 PAuswG 2002/ Art. 8 Nr. 1 a) (4) TBG).

*„Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form nach Abs. 3 sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt. Eine bundesweite Datei wird nicht eingerichtet“*, vgl. § 4 Abs. 4 PassG 2002/ Art. 7 Nr. 1 b) (4) TBG (vgl. § 1 Abs. 5 PAuswG 2002/ Art. 8 Nr. 1 a) (5) TBG).

*„Im Pass enthaltene verschlüsselte Merkmale und Angaben dürfen nur zur Überprüfung der Echtheit des Dokumentes und zur Identitätsprüfung des Passinhabers ausgelesen werden. Auf*

*Verlangen hat die Passbehörde dem Passinhaber Auskunft über den Inhalt der verschlüsselten Merkmale und Angaben zu erteilen“*, vgl. § 16 Abs. 6 PassG 2002/ Art. 7 Nr. 2 b) (6) TBG (vgl. § 3 Abs. 5 PAuswG 2002/ Art. 8 Nr. 2 b) (5) TBG).

Bereits die Kürze des Gesetzgebungsverfahrens ließ Zweifel aufkommen, dass der Bundestag seinem Auftrag, Gesetze nur mit Sorgfalt und am Gemeinwohl orientiert zu konzipieren, nachgekommen ist (vgl. *Martin Nolte*, Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, in: DVBl. 2002, S. 573 ff. [574], m. w. N.) – Am 7. November 2001 erfolgte im Bundestag die Befragung der Bundesregierung zu deren am gleichen Tag beschlossenen „Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus“. Allein der Regierungsentwurf umfasste 80 Seiten und erfasste unterschiedlichste Gesetze. Trotzdem erfolgte bereits am 15. November 2001 die erste Lesung im Bundestag. Für die Aussprache waren nur eineinviertel Stunden vorgesehen und insgesamt 25 andere Tagesordnungspunkte zu bearbeiten. Die Debatte wurde sehr emotional und weit entfernt von der juristischen Abwägungslehre geführt. Am 14. Dezember 2001 - nach zweiter und dritter Lesung nebst neun anderen Tagesordnungspunkten - erfolgte die Gesetzesannahme durch den Bundestag.

Insbesondere die fehlende ausführliche Abwägung der Freiheits- und Sicherheitsbelange in den Lesungen des Bundestages zu Art. 7 und Art. 8 des Terrorismusbekämpfungsgesetzes lies diese Regelungen „*von einer politisch demokratischen Legitimation weit entfernt*“ erscheinen (vgl. *Cordelia Koch*, Freiheitsbeschränkung in Raten?, in: Hessische Stiftung Friedens- und Konfliktforschung (Hrsg.), HSFK Report, Frankfurt/M 2002, S. 33 f.). Im Gesetzgebungsverfahren müssen Freiheits- und Sicherheitsbedürfnisse stets neu artikuliert und abgewogen werden:

*„Diese Aufgabe verträgt sich schwerlich mit einer Gesetzgebungstechnik, welche eine Vielzahl von Schubladenentwürfen in umfangreichen „Sicherheitspaketen“ zusammenfasst und bei gegebenen Anlässen ins Parlament einbringt, um sie sodann unter größtem Zeitdruck durch Ausschüsse, Sachverständigenanhörungen und Plenum zu „peitschen““* ( vgl. *Christoph Gusy*, Geheimdienstliche Aufklärung und Grundrechtsschutz, in: APuZ B 44/2004, S. 14 ff. [18]) - unter der Devise: *„Jetzt weht der Wind, jetzt gehen wir segeln“* (vgl. *Hansjürgen Garstka*, in: Öffentliche Anhörung zum Thema Terrorismusbekämpfungsgesetz, 78. Sitzung des Innenausschusses am 30. November 2001, Protokoll Nr. 78, S. 19, m. w. N.).

Der Verweis, dass fundamentalistisch-islamische Terroristen nicht mit deutschen Personalausweisen einzureisen pflegen (vgl. *Martin Kutscha*, in: Stellungnahme zum Entwurf des Terrorismusbekämpfungsgesetzes, BT-Drs. 14/7396, ad 2), so dass man einen fehlenden Zusammenhang zwischen den gesetzlichen Maßnahmen und der Terrorismusbekämpfung monieren kann (vgl. *Martin Nolte*, Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, in: DVBl. 2002, S. 573 ff. [574]), die begründete Warnung vor einem „Überwachungsstaat eines Ausmaßes, den wir uns heute noch nicht vorstellen können“ (vgl. *Stefan König*, in: Öffentliche Anhörung zum Thema Terrorismusbekämpfungsgesetz, 78. Sitzung des Innenausschusses am 30. November 2001, Protokoll Nr. 78, S. 19), u. v. a. m. - es war wohl egal:

*„Jede Kritik an der Effizienz, jeder Zweifel an der Rechtsstaatlichkeit dieser Maßnahmen perlt an dem apodiktischen Schutzpanzer der Präventionsrhetorik ab. Mit ihr lässt sich zuweilen sogar die apokalyptische Vision einer Gesellschaft, die in wuchernder Kriminalität erstickt, an die bürgerliche Fassade malen. Sie dient als Vorlage für jene Argumentation, dass die Präventionsanstrengungen weiter verstärkt und verschärft werden müssen, weil sie nicht mehr ausreichen. So kommt es, dass der öffentliche Begründungsaufwand für neue Präventionsmaßnahmen verschwindend gering ist und die dahinter stehende Präventionslogik nicht mehr Gegenstand kritischer Diskussionen ist“* (vgl. *Hermann Strasser/ Henning van den Brink*, Auf dem Weg in die Präventionsgesellschaft?, in: APuZ 46/2005, S. 3 ff. [4]). So werde die Abwehrmaßnahme gegen die Gefahr zu einem Beweis für die Gefahr, wie der Schriftsteller *Peter Schneider* beklagt (vgl. *Peter Schneider*, Kultur der Angst, in: Die Zeit vom 24. Februar 2005, S. 47).

Dazu ist bemerkenswert, „dass der Entwurf des Terrorismusbekämpfungsgesetzes auf dem Vorblatt und im Text der ausführlichen Allgemeinen Begründung das Wort »Sicherheit« 37 mal, das Wort »Freiheit« jedoch nicht ein einziges mal verwendet“ (vgl. *Erhard Denninger*, Freiheit durch Sicherheit?, in: StV 2/2002, S. 96 ff. [101]).

Dass die pass- und ausweisrechtlichen Änderungen nach dem Terrorismusbekämpfungsgesetz noch keine Eingriffsregelungen waren, weil die Konkretisierungen fehlten und späteren Bundesgesetzen vorbehalten wurden (vgl. § 4 Abs. 4 PassG 2002, § 1 Abs. 5 PAuswG 2002), das erschien: „gesetzgebungstechnisch merkwürdig“ (vgl. *Martin Nolte*, Die Anti-Terror-Pakete im Lichte des Verfassungsrechts, in: DVBl. 2002, S. 573 ff. [576], m. w. N.). Bloß, dass „Regierungen, die entsprechende Einschränkungen und Vorgaben nicht auf nationaler

*Ebene durchsetzen konnten, nutzen den Umweg über Europa...*“ (vgl. Peter Schaar, Datenschutz im Spannungsfeld von Privatsphärenschutz, Sicherheit und Informationsfreiheit, in: RDV 2006, S. 1 ff. [2]).

Der Europäische Rat bekräftigte auf seiner Tagung vom 19. und 20. Juni 2003 in Thessaloniki, dass in der Europäischen Union ein kohärenter Ansatz in Bezug auf biometrische Identifikatoren oder biometrische Daten für Dokumente für Drittstaatsangehörige, Pässe für Bürger der Europäischen Union und Informationssysteme (VIS und SIS II) verfolgt werden muss. Entsprechend den Schlussfolgerungen des Europäischen Rates machte die Kommission der Europäischen Gemeinschaften am 18. Februar 2004 den „Vorschlag für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger“ (vgl. KOM(2004) 116, in: ABLEU Nr. C 98 vom 23. April 2004, S. 39). Der Vorschlag der Kommission beschränkte sich auf die Verpflichtung zur Aufnahme von Gesichtsdaten und stellte die zusätzliche Speicherung von Fingerabdrücken in das Ermessen der Mitgliedstaaten:

*„Es können Fingerabdrücke in interoperabler Form hinzugefügt werden“*, vgl. Artikel 1 Absatz 2 Satz 2 ebenda.

Danach erschien es einmal mehr: *„bemerkenswert, dass dem Europäischen Parlament zunächst der erste Verordnungsentwurf, der noch die fakultative Aufnahme der Fingerabdrücke vorsah, vorgelegt wurde und dem Europäischen Parlament erst wenige Tage vor seiner Stellungnahme der – ohne Begründung geänderte – neue Entwurf übermittelt wurde, der nunmehr die obligatorische Aufnahme digitalisierter Fingerabdrücke vorsah. Seine Stellungnahme hat das Europäische Parlament bezeichnenderweise zu dem „alten“ Entwurf abgegeben, der nur eine fakultative Aufnahme der Fingerabdrücke vorsah“* (vgl. Peter Schaar, Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Novellierung des Passgesetzes für die Anhörung im Innenausschuss des Deutschen Bundestages am 23. April 2007, in: Ausschussdrucksache 16(4)192 E, S. 1).

So erließ der Europäische Rat die „Verordnung (EG) Nr. 2252/2004 vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten“ (vgl. ABl. L 385 vom 29. Dezember 2004, S. 1) -

„auf Vorschlag der Kommission <sup>(1)</sup>, nach Stellungnahme des Europäischen Parlaments <sup>(2)</sup>“:

„Die Pässe und Reisedokumente sind mit einem Speichermedium versehen, das ein Gesichtsbild enthält. Die Mitgliedstaaten fügen auch Fingerabdrücke in interoperablen Formaten hinzu“, vgl. Artikel 1 Absatz 2 Sätze 1 und 2 ebenda.

Damit wurde dem Deutschen Bundestag – unter Mitwirkung der Bundesregierung bei Missachtung des Gesetzesvorbehalts aus § 4 Abs. 4 PassG 2002/ Art. 7 Nr. 1 b) (4) TBG – die Entscheidung darüber entzogen, ob Fingerabdrücke überhaupt in die Pässe deutscher Staatsangehöriger aufgenommen werden sollten. Aber auch das Europäische Parlament hatte keine Möglichkeiten, die Entscheidung effektiv zu beeinflussen, denn der Rat hat die Verordnung im Rahmen der sog. „Dritten Säule“ der Europäischen Union beschlossen. Die weitreichende Maßnahme, Fingerabdrücke in die Pässe aller EU-Bürgerinnen und Bürger aufzunehmen, ist also allein durch die Regierungen und nicht durch die Parlamente entschieden worden, obwohl dies erhebliche Konsequenzen für die Grundrechte hat (vgl. *Peter Schaar*, Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Novellierung des Passgesetzes für die Anhörung im Innenausschuss des Deutschen Bundestages am 23. April 2007, in: Ausschussdrucksache 16(4)192 E, S. 1). Einmal mehr zeigte sich darin: „ein erschreckendes Demokratiedefizit in der Europäischen Union, welches in der Praxis nicht durch die nationalen Parlamente ausgeglichen werden kann“ (vgl. *Sönke Hilbrans*, Stellungnahme der Deutschen Vereinigung für Datenschutz e.V. zur Novellierung des Passgesetzes für die Anhörung im Innenausschuss des Deutschen Bundestags am 23. April 2007, in: Ausschussdrucks. 16(4)192 F, S. 1) und „inakzeptabel ist“ (vgl. *Entschließungsantrag der FDP-Fraktion*, in: Innenausschuss-Drucks. 16(4)215, in: Bundestags-Drucks. 16/5445 vom 23. Mai.2007, S.17 ff. [18]).

Allseits eilfertig eingeübtes „Demokratiedefizit“ - erst beim Terrorismusbekämpfungsgesetz vom 9. Januar 2002 und dann bei der Verordnung (EG) Nr. 2252 des Rates vom 13. Dezember 2004, dem ersten und zweiten Akt zur Einführung der „Volksdaktyloskopie“ also -, es setzte sich in der Bundesrepublik Deutschland in einem dritten Akt fort. Denn nachdem der Gesetzesvorbehalt des Deutschen Bundestages aus § 4 Abs. 4 PassG 2002/ Art. 7 Nr. 1 b) (4) des Terrorismusbekämpfungsgesetzes von der Bundesregierung eigenmächtig „ad acta“ gelegt und das Recht zur Stellungnahme des Europäischen Parlaments vom Europäischen Rat

---

<sup>1</sup>,<sup>(1)</sup> ABl. C 98 vom 23.4.2004, S. 39.“

<sup>2</sup>,<sup>(2)</sup> Stellungnahme vom 2.12.2004 (noch nicht im Amtsblatt veröffentlicht.)“

gemeinschaftlich „ad absurdum“ geführt worden war, so sollte nun unwiderstehlich werden: „die konsequent rationalisierte, d.h. planvoll eingeschulte, präzise, alle eigene Kritik bedingungslos zurückstellende, Ausführung des empfangenen Befehls“ (vgl. Max Weber, *Wirtschaft und Gesellschaft*, 5. Aufl., Tübingen 1976, 2. Halbband, S. 681 f.), d. h. schlicht:

*„Der Rat der Europäischen Union hat die Aufnahme des Gesichtsbildes sowie von Fingerabdrücken in elektronischer Form in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten verbindlich vorgeschrieben... Deshalb sind im deutschen Passgesetz die für die Abnahme der Fingerabdrücke und für die Kontrolle der biometrischen Daten erforderlichen Rechtsgrundlagen zu schaffen“* (vgl. Entwurf der Bundesregierung zur Änderung des Passgesetzes und weiterer Vorschriften vom 29. Januar 2007, in: BT-Drs. 16/4138).

Am 24. Mai 2007 – in zweiter und dritter Lesung des von der Bundesregierung eingebrachten Gesetzesentwurfs nebst Beschlussempfehlung und Bericht des Innenausschusses (vgl. BT-Drs. 16/5445) sowie weiterer Anträge (vgl. BT-Drs. 16/854, 16/3046, 16/4159, 16/5445) – war denn auch bemerkenswert „diszipliniert“, wie der Abgeordnete *Frank Hofmann*, Kriminaloberrat a. D. (BKA), die Freiheit aller Mitglieder des Deutschen Bundestages – „*Sie sind Vertreter des ganzen Volkes, an Aufträge und Weisungen nicht gebunden und nur ihrem Gewissen unterworfen*“, vgl. Art. 38 Abs. 1 Satz 2 GG – verleugnete:

*„Ich will in diesem Zusammenhang daran erinnern, dass wir die Pflicht haben, die EU-Richtlinie in nationales Recht umzusetzen“* (vgl. *Frank Hofmann*, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10241). Der Abgeordnete *Clemens Binninger*, auch ein gelernter Polizist, er war dabei noch patriotisch: „*Gleichzeitig – das ist ein Aspekt, den man sicherlich nennen darf – ist die Biometrie ein Standortfaktor für unser Land*“ (vgl. *Clemens Binninger*, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10238).

Das wusste sicher auch der Abgeordnete *Otto Schily* zu schätzen. Denn nachdem er sich als Innenminister schon beim „Gesetz zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002“ für biometrische Ausweise stark gemacht hatte, wurde er Aufsichtsrat bei Safe ID Solutions und Byometric Systems AG (vgl. <http://www.bundestag.de/mdb/bio/S/schilotO>) - zwei Firmen, die Lösungen für biometrische Anwendungen herstellen. Safe ID produziert Hard- und Softwarelösungen für die Herstellung modernster Ausweispapiere. Byometric

Systems entwickelt Technik zur Personenidentifizierung anhand der Irisstruktur. Dazu zitierte ZEIT online *Otto Schily* mit den Worten:

*„Ich sehe keinerlei Probleme darin, zwei junge Unternehmen, die moderne Sicherheitstechnik entwickeln, insbesondere bei ihren Exportbemühungen zu unterstützen.“* Und auch das ist wohl wahr: *„Interessen-Kollisionen mit meiner früheren Tätigkeit als Bundesminister bestehen nicht“* (vgl. <http://images.zeit.de/text/online/2006/33/schily-biometrie>).

So gesehen war der 11. September nur Auslöser und ganz zu unrecht vielfach in Anspruch genommener Legitimationstopos für die Einführung der „Volksdaktyloskopie“:

*„Lieber Kollege Wieland, sind Sie in der Lage, zu begreifen, dass es bei der Einführung dieses wunderbaren neuen Passes nicht um Terrorismus oder Fälschungsfragen geht, sondern darum, dass man an der Grenze, wenn Sie einen solchen Pass eines Tages haben, blitzschnell feststellen kann: „Wieland ist derjenige, der in dem Pass steht, und umgekehrt.“? Das ging bislang nicht. Das ist der geniale Fortschritt. Sind Sie nicht der Meinung, dass dieses Hightechinstrument, dieser Pass, den es weltweit nur in Europa gibt, das wert ist, weil er den Bürgern in der Tat mehr Sicherheit verschafft? Mit Terrorismus hat das alles nichts zu tun, lieber Herr Wieland“* (vgl. *Dieter Wiefelspütz*, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10245).

Das „Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften vom 20. Juni 2007“ (vgl. Bundesgesetzblatt vom 27. Juli 2007, Teil I, S. 1566 ff.), es schreibt u.a. folgendes vor:

*„Auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedsstaaten ausgestellten Pässen und Reisedokumenten (ABl. EU Nr. L 385 S. 1) sind der Reisepass, der Dienstpass und der Diplomatenpass mit einem elektronischen Speichermedium zu versehen, auf dem das Lichtbild, Fingerabdrücke, die Bezeichnung der erfassten Finger, die Angaben zur Qualität der Abdrücke und die in Abs. 2 S. 2 genannten Angaben gespeichert werden. Die gespeicherten Daten sind gegen unbefugtes Auslesen, Verändern und Löschen zu sichern. Eine bundesweite Datenbank nach Satz 1 wird nicht errichtet“, vgl. § 4 Abs. 3 PassG 2007.*

*„Die Fingerabdrücke werden in Form des flachen Abdrucks des linken und rechten Zeigefingers des Passbewerbers im elektronischen Speichermedium des Passes gespeichert. Bei Fehlen eines Zeigefingers, ungenügender Qualität des Fingerabdrucks oder Verletzungen der Fingerkuppe wird ersatzweise der flache Abdruck entweder des Daumens, des Mittelfingers oder des Ringfingers gespeichert. Fingerabdrücke sind nicht zu speichern, wenn die Abnahme der Fingerabdrücke aus medizinischen Gründen, die nicht nur vorübergehender Art sind, unmöglich ist“, vgl. § 4 Abs. 4 PassG 2007.*

*„Soweit in den Pass Fingerabdrücke aufzunehmen sind, sind diese dem Passbewerber abzunehmen und nach Maßgabe des § 4 Abs. 4 zu erfassen; der Passbewerber hat bei der Abnahme der Fingerabdrücke mitzuwirken“, vgl. § 6 Abs. 2 Satz 3 PassG 2007.*

*„Es bleibt dabei: Die Fingerabdrücke werden nur im Pass gespeichert“, so hatte sich der Abgeordnete Frank Hofmann - beim BKA a. D. - „mit dem Erreichten sehr zufrieden gegeben“ (vgl. Frank Hofmann, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10241). Das könnte wohl auch noch gut möglich sein, wenn der Abgeordnete Clemens Binninger recht behielte: „Sicherlich werden wir in einigen Jahren, vielleicht auch früher, noch einmal über unsere Forderung diskutieren, eine Kopie der Fingerabdrücke zu hinterlegen“ (vgl. Clemens Binninger, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10238). Schließlich wissen beide Mitglieder des Innenausschusses längst, dass zum nächsten Akt der „Volksdaktyloskopie“ auch noch das „Demokratiedefizit“ der Europäischen Union wegweist:*

*„Diese Verordnung, die den rechtlichen Rahmen für die Harmonisierung der Sicherheitsmerkmale der Pässe und die Einführung biometrischer Identifikatoren festlegt, stellt einen ersten Schritt da. Ein zweiter Schritt wird längerfristig mit der Einrichtung eines Europäischen Passregisters erfolgen... In diesem Fall muss der Fingerabdruck abgenommen und gespeichert werden, um die Abfrage zu ermöglichen („one-to-many-Verfahren“, 1:n Vergleich)“ (vgl. Kommission der Europäischen Gemeinschaften, in: ABl.EU Nr. C 98 vom 23. April 2004, S. 39; KOM(2004) 116, S. 7 f.). Mit anderen Worten:*

Die obligatorische Erfassung von Fingerabdrücken „intendiert“ bereits die Entstehung eines AFIS mit mehreren 100 Millionen Fingerbilddateien, und zwar: „unabweisbar“. Und,

„unbestreitbar“, die kriminalistische Funktionalität so umfassender Datenbestände zum Vergleich mit zahllosen Tatortspuren wäre groß. So groß, dass ein Mord in der Münchener Schickleria oder irgendetwas irgendwo – falls die Kriminalisten dann keine Fingerabdrücke finden - mit dem gleichen „obligatorischen Zwang“ auch dazu führen würde, dass in eine Datenbank „*jeder Bürger und jeder Einreisende sein Genmaterial vorsorglich „einzuzahlen“ hätte*“ (vgl. Miloš Vec, Freiheit unter Verdacht, in: Blätter für deutsche und internationale Politik 8/2007, S. 957 [964]). Diese „sicherheitstechnische Eigendynamik“ würde mit der obligatorischen Erfassung von Fingerabdrücken mit „sicherheitsgesetzlichem Zwang“ in Gang gesetzt werden. In dem weiteren Vorgang würde das Recht seines verfassten gesellschaftlichen Steuerungsanspruchs allmählich enthoben. Darin inbegriffen wäre, dass die freiheitlich demokratische Grundordnung einem strengen elitären Sicherheitsregime erlänge:

*„Es scheint, dass bei der Suche nach dem Einsatz immer effizienterer Mittel, die die Technik feilbietet, und bei dem Wunsch, Gefahren so früh wie möglich zu erkennen, das Augenmaß für das notwendige Balancieren von Freiheit und Sicherheit allmählich abhanden kommt. Immer abstrakter werden die Gefahren in Recht gefasst, gegen die man zu Felde ziehen will, immer potenzieller werden die Täter, die man fassen will. Der Traum eines jeden Polizisten, von dem Horst Herold als damaliger BKA-Chef erzählte, eher am Tatort zu sein als der Täter, soll so Wirklichkeit werden. Aber wenn gesetzlich nicht mehr klar umschrieben wird, gegen was konkret vorgegangen werden soll... dann ist am Ende jeder verdächtig und den Verfolgungsbehörden alles erlaubt. So droht der Mensch vom Schutzsubjekt zur Erkenntnisquelle zu pervertieren, die umfassend abgeschöpft wird – ein Ergebnis das unserem Grundgesetz widerspricht“* (vgl. Christine Hohmann-Dennhardt, Freiräume – Zum Schutz der Privatheit, in: NJW 2006, S. 545 [548], m. w. N.).

So sieht der am 4. Juli 2006 unterzeichnete Vertrag von Prüm bereits vor, dass sich die beteiligten Staaten – zunächst Belgien, Deutschland, Frankreich, Luxemburg, Niederlande, Österreich und Spanien – untereinander bestimmte Zugriffsrechte auf DNA- und Fingerabdruckdateien sowohl zur Verfolgung als auch zur Verhinderung von Straftaten gewähren (vgl. Peter Schaar, Datenaustausch und Datenschutz im Vertrag von Prüm, in: DuD 30 (2006), S. 691 ff., m. w. N.). Dazu „passt“:

*„Wie die Staaten, die eine Leseberechtigung für die gespeicherten biometrischen Daten haben, mit den Daten umgehen, entzieht sich der Kontroll- und Einflussmöglichkeit deutscher*

*Stellen. Diese Daten könnten also in Personendatenbanken einfließen“ (vgl. Peter Schaar, Stellungnahme des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zur Novellierung des Passgesetzes für die Anhörung im Innenausschuss des Deutschen Bundestages am 23. April 2007, in: Ausschussdrucksache 16(4)192 E, S. 2). Dito, das ist die Absicht:*

*„Schauen wir einmal, wie es in den anderen Ländern Europas gemacht wird, in denen biometrische Pässe eingeführt werden: Frankreich sieht eine zentrale Speicherung der Fingerabdrücke vor; wir vernichten sie. Holland sieht eine zentrale Speicherung der Fingerabdrücke vor; wir vernichten sie. Österreich sieht eine zentrale Speicherung der Fingerabdrücke vor; wir vernichten sie. Ich halte das nicht für den richtigen Weg...“ (vgl. Clemens Binninger, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10239).*

Ebenso würde auch der Bundesrat die obligatorische Erfassung von Fingerabdrücken *„für einen automatisierten Abgleich mit erkennungsdienstlichen Dateien der Polizeivollzugsbehörden verwenden“*. Dabei würde *„insbesondere an das beim Bundeskriminalamt geführte automatische Fingerabdruck Identifizierungssystem (AFIS) zu denken sein“* (vgl. Stellungnahme des Bundesrates vom 28. Februar 2007 zum „Entwurf eines Gesetzes zur Änderung des Passgesetzes und weiterer Vorschriften“, in: Bundestags-Drs. 16/4456, S. 2 f.).

Mit der obligatorischen Erfassung von Fingerabdrücken kämen noch weitere Risiken hinzu, die sich aus der RFID-Implementierung des elektronischen Passes, auch in Kombination mit der Biometrie ergeben, insbesondere Tracking. Denn die Einführung von Biometrie und RFID-Technik macht den elektronischen Pass zur Komponente eines IT-Systems (vgl. *Martin Meints, Implementierung großer biometrischer Systeme, in: DuD 31/2007, S. 189 ff.*).

Die Verbreitung von Computern wie auch des Mobilfunks hat deutlich gemacht, dass sowohl immer weitergehende technische Möglichkeiten, als auch die zunehmende Speicherung von Daten für (repressive und präventive) Überwachung nutzbar gemacht werden. Dies zeigt sich nicht nur im originären Einsatz entsprechender Technologie durch staatliche Behörden, sondern auch in der Nutzung der sich aus der allgemeinen Verwendung solcher Technik ergebenden Datenquellen. Wohin diese sich insoweit verselbständigende Entwicklung führen könnte, lässt sich an der Technik der Radio Frequenz Identifikation (RFID) exemplifizieren:

*„RFID ist eine Erkennungstechnologie basierend auf Datenübermittlung mittels Funksignalen. Dabei werden auf kleinen Transponderchips gespeicherte Daten mittels Lese-/Schreibgerät ausgelesen bzw. verändert, ohne dass hierfür eine Sicht- oder sonstige direkte Verbindung erforderlich wäre. Die Technik arbeitet somit unabhängig von örtlichen Gegebenheiten – beispielsweise Sichtbarrieren wie Wänden, Taschen, Kleidungsstücken – und gegebenenfalls auch ohne Kenntnisnahme des Betroffenen... Neben der Nutzung durch Private... kommt der Einsatz der RFID-Technologie insbesondere auch für den Bereich staatlicher Ausforschung und Kontrolle, unter anderem im Bereich der Strafverfolgung in Betracht. Dabei ist an eine mittelbare Nutzung in Form des bloßen Auslesens bereits auf einem Chip vorhandener Daten ebenso zu denken, wie an einen originären Einsatz der Chips durch staatliche Stellen, beispielsweise zu Zwecken der Observation. Während letzteres vor allem eine Vereinfachung sowie Automatisierung bereits vorhandener Möglichkeiten und somit im Hinblick auf Ressourcen auch eine Ausweitung von Datenerhebung mit sich bringen dürfte, eröffnet die erstgenannte Variante per se nahezu totale Möglichkeiten der Ausforschung... Dementsprechend ist im mittelbaren Bereich die Nutzung existierender Chips zur Erstellung von Bewegungsprofilen bzw. zur Überwachung so genannter „hot spots“ möglich. Hierfür käme ein Anbringen von Lese- und Schreibeinheiten an ausgewählten Orten in Betracht... Die technische Möglichkeit der Veränderung der Daten im Transponder gekoppelt beispielsweise mit einem Videoaufnahmegerät ermöglicht die Anfertigung von Überwachungsbildern bezogen auf ein gehäuftes Auftreten einer bestimmten Kennung und einer entsprechenden Zuschreibung zu einer bestimmten Person. Zudem ist ein Einsatz auch zur weitergehenden Datensammlung zwecks Erstellung eines Persönlichkeitsmusters denkbar... Der direkte staatlich bewirkte Einsatz der Transponder – unmittelbar als Überwachungschip, aber auch in Pässen...– könnte etwa für längerfristige Observationen oder zur Zutrittsbegrenzung im Sinne einer ort-spezifischen Prävention in Betracht kommen“ (vgl. Ulrich Eisenberg/ Jens Puschke/ Tobias Singelstein, Überwachung mittels RFID-Technologie, in: ZRP 1/2005 S. 9 ff., m. w. N.).*

## 2 Rechtswidrigkeit

Die obligatorische Erfassung von Fingerabdrücken bzw. die Nichterteilung von Reisepässen ist formell und materiell verfassungs- und gemeinschaftsrechtswidrig. Der Maßnahme fehlt schon die Rechtsgrundlage. Zudem waren die Verfahren parlamentarisch nicht demokratisch. So wurde das Europäische Parlament nicht ordnungsgemäß gehört und der Gesetzesvorbehalt des Deutschen Bundestages wurde missachtet. In der Sache aber verletzt die obligatorische Erfassung von Fingerabdrücken das allgemeine Persönlichkeitsrecht auf informationelle Selbstbestimmung bzw. das Recht auf Freizügigkeit der Person.

Systematisch wird hier zunächst die formelle Rechtswidrigkeit der beklagten Maßnahme nach der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 und anschließend ebenso nach dem Passgesetz vom 20. Juli 2007 festgestellt (2.1). Sodann wird die materielle Rechtswidrigkeit der obligatorischen Erfassung von Fingerabdrücken nach dem Grundsatz der Verhältnismäßigkeit für das Gemeinschafts- und Verfassungsrecht einheitlich begründet (2.2).

### 2.1 Formelle Rechtswidrigkeit der obligatorischen Erfassung von Fingerabdrücken

Die Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 ist schon mangels Rechtsgrundlage nichtig. Die EG verfügte über keine Kompetenz zum Erlass der Passverordnung. Diese wurde zu Unrecht gestützt auf den Vertrag zur Gründung der Europäischen Gemeinschaft, insbesondere Artikel 62 Absatz 2 Buchstabe a). Dort ist zwar vorgesehen, dass „*Maßnahmen bezüglich des Überschreitens der Außengrenzen der Mitgliedsstaaten*“ beschlossen werden, „*mit denen folgendes festgelegt wird: Normen und Verfahren, die von den Mitgliedsstaaten bei der Durchführung der Personenkontrollen an diesen Grenzen einzuhalten sind*“, vgl. Artikel 62 Absatz 2 Buchstabe a) EGV. Die EG-Passverordnung enthält aber noch vielmehr: „*Allgemeine Maßnahmen zur Verhütung und Bekämpfung der Kriminalität*“, vgl. Art. 29 EUV. Denn die obligatorische Erfassung von Fingerabdrücken zielt auf eine Datenverarbeitung, die nicht zur Durchführung von Personenkontrollen an den Außengrenzen erforderlich ist, aber zum Schutz der öffentlichen Sicherheit und zu Strafverfolgungszwecken als erforderlich angesehen wird. Die Kompetenzvorschriften des Europarechts erlauben allerdings keine freie Wahl der Rechtsgrundlage nach Opportunitäts Gesichtspunkten (vgl. *Patrick Breyer*, Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, StV 4/2007, S. 217 ff. [215]).

Die Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 nimmt in den Erwägungsgründen unter (2) und (3) – ebenda: „*einheitliche Sicherheitsstandards für Pässe und Reisedokumente zum Schutz vor Fälschungen festzulegen*“ sowie „*eine verlässlichere Verbindung zwischen dem Inhaber und dem Pass oder dem Reisedokument her[zu]stellen und damit erheblich zum Schutz vor einer betrügerischen Verwendung von Pässen und Reisedokumenten bei[zu]tragen*“ – eindeutigen Bezug auf strafrechtliche Bestimmungen, insbesondere beispielsweise auf die „Urkundenfälschung“ gem. 267 StGB, das „Verändern von amtlichen Ausweisen“ gem. § 273 StGB, das „Verschaffen von falschen amtlichen Ausweisen“ gem. 276 StGB und den „Missbrauch von Ausweispapieren“ gem. § 281 StGB.

Darüber hinaus wurde die EG-Passverordnung auch noch in einem weiteren Zusammenhang des Art. 29 EUV – ebd.: der „*Verhütung und Bekämpfung... insbesondere des Terrorismus*“ - gesehen: „*Nach den tragischen Ereignissen vom 11. September 2001 bestand der Wunsch nach raschen Maßnahmen zur Verbesserung der Dokumentensicherheit*“ (vgl. *Kommission der Europäischen Gemeinschaften*, Vorschlag für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger, in: KOM (2004) 116, S. 2).

Schließlich hat der Rat der Europäischen Union mit seiner Festlegung auf Fingerabdrücke ohne ersichtliche Abwägung aber ausgerechnet denjenigen biometrischen Identifikator in die Pässe und Reisedokumente der EU-Bürger aufzunehmen bestimmt, der von Seiten der kriminalistischen „Volksdaktyloskopie“ schon seit rund einhundert Jahren eingefordert wird (vgl. *Robert Heindl*, Passreform, in: *Archiv für Kriminal-Anthropologie und Kriminalistik* 32 (1908), S. 162 ff.; ebenso: *Luigi Tomellini*, Des modifications a introduire dans les passpotes, in: *Archives D`Anthropologie Criminelle* 23 (1908), S. 508 ff.).

Nach allem lässt sich die Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 zwar unter die generalklauselartige Kategorie des Art. 62 Nr. 2 a) EGV – ebenda: „*Normen und Verfahren bezüglich des Überschreitens der Außengrenzen der Mitgliedsstaaten*“ – subsumieren. Der „Anlass“ von Personenkontrollen reicht zur „Begründung“ der Erfassung von Fingerabdrücken aber nicht hin. Dafür gelten allenfalls die Bestimmungen der polizeilichen und justitiellen Zusammenarbeit in Strafsachen gemäß Titel VI. Art. 29 ff. EUV.

Es gilt der Grundsatz: „*Lex specialis derogat legi generali*“: das besondere Gesetz geht dem allgemeinen vor. So hat die Passverordnung die falsche, mithin: keine Rechtsgrundlage mehr.

Darüber hinaus ist die Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 auch nicht verfahrensordnungsgemäß erlassen worden. Zwar besaß das Europäische Parlament insoweit keine Mitentscheidungsmöglichkeit. Gerade in diesem Fall hätte jedoch das Recht auf Anhörung bzw. Stellungnahme des Europäischen Parlaments strikt gewahrt werden müssen. Das war so nicht der Fall, weil *„die Vorlage an das Parlament lediglich die fakultative Aufnahme von Fingerabdrücken vorsah und die entsprechende Verpflichtung erst nach der Stellungnahme des Parlaments am 2. Dezember 2004 durch den Rat eingefügt wurde, ohne dass die EG-PassVO diesem zur erneuten Stellungnahme vorgelegt wurde“* (vgl. Alexander Roßnagel/ Gerrit Hornung, Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck, in: DÖV 2005, 983 [984]) - oder *„dem Europäischen Parlament zunächst der erste Verordnungsentwurf, der noch die fakultative Aufnahme der Fingerabdrücke vorsah, vorgelegt wurde und der neue Entwurf, in dem die Aufnahme digitalisierter Fingerabdrücke obligatorisch ausgestaltet war, ohne dass dies näher begründet worden wäre, dem Europäischen Parlament so spät übermittelt wurde, dass er in dessen Stellungnahme nicht mehr einbezogen werden konnte“* (vgl. Entschließungsantrag der FDP-Fraktion, in: Innenausschuss-Drucks. 16(4)215, in: BT-Drucks. 16/5445 vom 23. Mai. 2007, S. 17 f. ). Als die Verordnung (EG) Nr. 2252/2004 vom 13. Dezember 2004 dann im Amtsblatt der Europäischen Union am 29. Dezember 2004 veröffentlicht wurde, da war denn auch die Stellungnahme des Europäischen Parlaments vom 2. Dezember 2004 bezeichnenderweise: *„noch nicht im Amtsblatt veröffentlicht“* (vgl. Klammerzusatz zu Fußnote <sup>(2)</sup> der EG-PassVO, in: ABl.EU Nr. L 385 v. 29.12.2004, S. 1).

Der Europäische Gerichtshof sieht in den Anhörungsrechten ein wichtiges Mittel, das dem Parlament eine wirksame Beteiligung am Gesetzgebungsverfahren der Gemeinschaft ermöglicht. Die Anhörung erfolgt durch den Rat auf der Grundlage des Vorschlags der Kommission. Weicht die endgültige Fassung substantiell von dem Text ab, zu dem das Europäische Parlament gehört worden ist, so ist eine erneute Anhörung des Europäischen Parlaments erforderlich. Der Anhörung ist nicht bereits dadurch genügt, dass der Rat das Europäische Parlament um eine Stellungnahme ersucht. Das Parlament muss vielmehr seiner Auffassung tatsächlich Ausdruck verleihen. Um dies zu erreichen muss der Rat seine Möglichkeiten ausschöpfen. Die ordnungsgemäße Anhörung des Parlaments stellt somit eine wesentliche Formvorschrift dar, deren Missachtung die Nichtigkeit der betroffenen Handlung zur Folge hat (vgl. *EuGH*, Slg. 1980, 3333 – „Roquette Frères-Isoglucose“). Damit ist die EG-PassVO vom 13. Dezember 2004 aus kompetenz- und verfahrensrechtlichen Gründen nichtig.

Die Nichtigkeit der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 bedeutet, dass das Bundesverfassungsgericht die Verfassungswidrigkeit der obligatorischen Erfassung von Fingerabdrücken feststellen und mithin das Passgesetz vom 20. Juli 2007 für nichtig erklären kann, ohne den Vorrang des Gemeinschaftsrechts beachten zu müssen. Denn Normen des sekundären Gemeinschaftsrechts, die gegen Regelungen des EG-Vertrages und des sonstigen primären Gemeinschaftsrechts einschließlich der Gemeinschaftsgrundrechte verstoßen und deswegen nichtig sind, sind vom deutschen Zustimmungsgesetz nicht gedeckt. Die mit der Umsetzung befassten Staatsorgane sind aus verfassungsrechtlichen Gründen gehindert, diese Rechtsakte in Deutschland anzuwenden (vgl. BVerfGE 89, 155 [188]). In der Übergangszeit bis zur Nichtigkeitsklärung der Verordnung (EG) Nr. 2252/2004 hat Deutschland von Verfassungswegen ein Vertragsverletzungsverfahren in Kauf zu nehmen (vgl. *Patrick Breyer*; Rechtsprobleme der Richtlinie 2006/24/EG zur Vorratsdatenspeicherung und ihrer Umsetzung in Deutschland, StV 4/2007, 214 [216]).

Das Passgesetz vom 20. Juli 2007 ist formell verfassungswidrig. Denn die obligatorische Erfassung von Fingerabdrücken erfolgte gemäß § 4 Abs. 3 S. 1 des Passgesetzes vom 20. Juli 2007 „auf Grund der Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004“. Diese „Rechtsgrundlage“ entfällt mit ihrer Nichtigkeit „ex tunc“, das heißt: „von damals an“. Folglich gilt zunächst wieder diejenige Rechtslage, die vor Erlass der EG-PassVO bestand. Das führt noch einmal auf die Änderung des Passgesetzes gemäß Artikel 7 des Gesetzes zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002 zurück. Es sah vor: „Die Arten der biometrischen Merkmale, ihre Einzelheiten und die Einbringung von Merkmalen und Angaben in verschlüsselter Form... sowie die Art ihrer Speicherung, ihrer sonstigen Verarbeitung und ihrer Nutzung werden durch Bundesgesetz geregelt“, vgl. § 4 Abs. 4 S. 1 PassG 2002/ Art. 7 Nr. 1 b) (4) TBG. Darin kommt die verfassungsrechtlich gebotene Verantwortlichkeit des Parlaments zum Ausdruck. Dazu sind die Abgeordneten des Deutschen Bundestages „an Aufträge und Weisungen nicht gebunden“, vgl. Artikel 38 Abs. 1 S. 2 GG.

Dem widerspricht, dass Abgeordnete des Deutschen Bundestages der obligatorischen Erfassung von Fingerabdrücken in der Annahme zustimmten, „dass wir die Pflicht [dazu] haben“ (vgl. *Frank Hofmann*, in: Deutscher Bundestag, Protokoll, 16. Wahlperiode, 100. Sitzung, Berlin, Donnerstag, 24. Mai 2007, S. 10241), obwohl Art. 38 Abs. 1 S. 2 GG jedes imperative Mandat verbietet. Ohne Freiheit des Mandats gibt es keine Verantwortlichkeit des Parlaments. So erscheint das Passgesetz vom 20. Juli 2007 am Ende wie die obligatorische Erfassung von Fingerabdrücken von Anfang an: „oktroziert“, d.h. formell verfassungswidrig.

## 2.2 Materielle Rechtswidrigkeit der obligatorischen Erfassung von Fingerabdrücken

Die Erfassung von Fingerabdrücken verletzt das Recht auf informationelle Selbstbestimmung.

Im Sinne des obersten Konstitutionsprinzips der ‚*Würde des Menschen*‘ entwickelte das Bundesverfassungsgericht im sog. Volkszählungsurteil vom 15. Dezember 1983 ein „*Recht auf informationelle Selbstbestimmung*“ (vgl. *BVerfG*, NJW 1984, S. 419 ff.). Seitdem ist u. a. folgendes in ständiger Rechtsprechung und allgemein anerkannt: „*Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung persönlicher Daten zu bestimmen*“ (vgl. *BVerfGE* 65, 1 [43]; 78, 77 [84]; 80, 367 [373]; 84, 192 [194]; 92, 191 [197]; 96, 171 [181]; 101, 106 [121]; *BVerfG*, NJW 2006, 976 [979])).

Im Interesse des Einzelnen ist das Recht auf informationelle Selbstbestimmung eine Voraussetzung für die Ausübung weiterer Grundrechte: „*Das Grundrecht dient dabei auch dem Schutz vor einem Einschüchterungseffekt, der entstehen und zu Beeinträchtigungen bei der Ausübung anderer Grundrechte führen kann, wenn für den Einzelnen nicht mehr erkennbar ist, wer was wann und bei welcher Gelegenheit über ihn weiß. Die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen und zu entscheiden, kann dadurch wesentlich gehemmt werden... Wer damit rechnet das etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und das ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten*“ (vgl. *BVerfGE* 65, 1 [42 f.]).

Im Interesse des Gemeinwohls ist das Recht auf informationelle Selbstbestimmung eine Voraussetzung für eine freiheitlich demokratische Grundordnung: „*Ein von der Grundrechtsausübung abschreckender Effekt fremden Geheimwissens muss nicht nur im Interesse der betroffenen Einzelnen vermieden werden. Auch das Gemeinwohl wird hierdurch beeinträchtigt, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger gegründeten freiheitlichen demokratischen Gemeinwesens ist*“ (vgl. *BVerfGE* 65, 1 [43]; *BVerfG*, NJW 2006, 976 [979])).

Der Grundrechtsstandard auf europäischer Ebene ist dem Grundrechtsstandard des Grundgesetzes „*im Wesentlichen gleich zu achten*“ (vgl. *BVerfG*, NJW 2000, 3124 ff. [3124]):

Der Europäische Gerichtshof hat bereits im Jahre 1969 die Grundrechtsqualität des Datenschutzes anerkannt und in der Folge bestätigt und ausgebaut. Er rekurriert dabei auf die gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten und maßgeblich auf internationale und europäische Abkommen über Menschenrechte, an denen die Mitgliedstaaten beteiligt sind. Das betrifft im vorliegenden Fall insbesondere Art. 8 der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK). Die Sammlung und Speicherung personenbezogener Daten greift in die dort gewährleisteten Rechte ein und bedarf einer Rechtfertigung, die ihrerseits den Anforderungen aus Art. 8 Abs. 2 EMRK genügen muss. Es ist eine gesetzliche Grundlage erforderlich, die ausreichend deutlich und genau sein muss. Außerdem muss das Verhältnismäßigkeitsprinzip beachtet werden (vgl. *Alexander Roßnagel/Gerrit Hornung*, Reisepässe mit elektronischem Gesichtsbild und Fingerabdruck, in: DÖV 2005, S. 983 ff. [986] m. w. N.).

Ein Grundrechtskatalog, vergleichbar dem des Grundgesetzes oder der EMRK, existiert auf Ebene der Europäischen Union bisher nur in Form der nicht rechtsverbindlichen Europäischen Grundrechtscharta (EGC). In Art. 8/68 EGC ist der Schutz personenbezogener Daten geregelt. Das Präsidium des Europäischen Konvents hat den Schutz personenbezogener Daten in Art. 8/68 EGC auf folgende Regelungen gestützt: auf den Schutz personenbezogener Daten in Art. 286 EGV, auf die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, auf Art. 8 EMRK und auf das Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (vgl. *Hans D. Jarass*, EU-Grundrechte, München 2005, § 13 Rn. 1, m. w. N.). Auf die Europäische Grundrechtscharta hat der Europäische Gerichtshof, entgegen dem Gericht erster Instanz und den Generalanwälten, bislang noch nicht ausdrücklich Bezug genommen. Da die oben genannten Quellen aber lediglich als Rechts-erkenntnisquellen angesehen werden, hat der Europäische Gerichtshof einen erheblichen Gestaltungsspielraum. Es soll gelten, „*was sich bei einer kritischen Analyse der Lösungen, die sich nach der rechtsvergleichenden Umschau ergeben, als die beste Lösung darstellt*“ (vgl. *Benjamin Rusteberg*, Die EG-Richtlinie zur Vorratsdatenspeicherung von Verkehrsdaten im System des europäischen Grund- und Menschenrechtsschutzes, in: VB/BW 5/2007, S. 171 ff. [176] m. w. N.). Diese muss verhältnismäßig, also wert- und zweckrational bestimmt werden.

Die obligatorische Erfassung von Fingerabdrücken verletzt den Grundsatz der „Verhältnismäßigkeit“ („proportionality“/ „proportionalité“). Zwar können mit beklagter Maßnahme angeblich verfolgte Zwecke als durchaus „legitim“ angesehen werden. Den gesetzten Zwecken kann die obligatorische Erfassung von Fingerabdrücken aber nicht „entsprechen“ („genuinely meet“/ „répondent effectivement“), sie ist also nicht „geeignet“. Darüber hinaus ist die beklagte Maßnahme nicht „erforderlich“ („necessary“/ „nécessaires“), um die gesetzten Ziele zu erreichen. Schließlich ist die obligatorische Erfassung von Fingerabdrücken auch „unangemessen“ („disproportionate“/ „démessuré“). Damit ist die beklagte Maßnahme letztlich auch davon fernab:

*„Zweckrational handelt, wer sein Handeln nach Zweck, Mitteln und Nebenfolgen orientiert und dabei sowohl die Mittel gegen die Zwecke, wie die Zwecke gegen die Nebenfolgen, wie endlich auch die verschiedenen möglichen Zwecke gegeneinander rational abwägt“ (vgl. Max Weber, Wirtschaft und Gesellschaft, 5. Aufl., Tübingen 1976, 1. Halbband, S. 13).*

Die obligatorische Erfassung von Fingerabdrücken ist „Mittel“ zum „Zweck“. Die EG-PassVO vom 13. Dezember 2004 gibt in den Erwägungsgründen (2) und (3) insgesamt zwei Zwecke zu verfolgen vor: *„zum Schutz vor Fälschungen“* und *„erheblich zum Schutz vor einer betrügerischen Verwendung von Pässen oder Reisedokumenten bei[zu]tragen“*. Letzterem Zweck zugeschrieben steht im Erwägungsgrund (3) die bloße Eigenart des Mittels der Aufnahme biometrischer Identifikatoren in Pässe und Reisedokumente – nämlich: *„eine verlässlichere Verbindung zwischen dem Inhaber und dem Pass oder dem Reisedokument her[zu]stellen“*. Genannten „Zwecken“ als „Mittel“ sollen dienen: *„auch Fingerabdrücke“* – wobei dieser „Identifikator“ allenfalls heimlich „erwogen“ worden ist (vgl. Erwägungsgründe zur Verordnung (EG) Nr. 2252/2004, in: ABl.EU Nr. L 385 v. 29.12.2004, S. 1 f.).

*„Zum Schutz vor Fälschungen“* ist die obligatorische Erfassung von Fingerabdrücken in Pässen und Reisedokumenten nicht geeignet, da die in den EU-Mitgliedsstaaten ausgestellten Pässe und Reisedokumente bereits weitestgehend „fälschungssicher“ sind. Denn „Fälschungssicherheit“ kann ja nur bedeuten, dass diesbezüglich einschlägige Delikte zahlenmäßig gering „ausfallen“ bzw. bei Kontrollen allemal „auffallen“. Beides liegt offensichtlich vor. Dagegen würden heimliche Verfälschungen von Pässen und Reisedokumenten ermöglicht, wenn deren Inhaber ihre Daten dort wie vorgesehen weder selbst „auslesen“ können, noch in der Lage sind stets zu bemerken, ob ein Lese-/Schreibgerät ihre Daten per Funk ausliest oder verändert.

Die obligatorische Erfassung von Fingerabdrücken ist nicht geeignet „*erheblich zum Schutz vor einer betrügerischen Verwendung von Pässen oder Reisedokumenten beizutragen*“. Zwar würden es im Pass gespeicherte Fingerabdrücke im „Idealfall“ möglich machen festzustellen, ob eine Person, die ihren Pass im Rahmen einer Kontrolle vorlegt, auch der berechnigte Inhaber des PASSES ist. Theoretisch könnte erkannt werden, wenn sich eine Person mit einem fremden Pass einer ähnlich aussehenden Person ausweist. Praktisch würde dies aber vielfach nicht funktionieren. Entsprechend der Rechtsgrundlage der EG-PassVO könnten betrügerische Verwendungen von Pässen oder Reisedokumenten nur festgestellt werden „*bezüglich des Überschreitens der Außengrenzen der Mitgliedstaaten*“, vgl. Art. 62 Nr. 2 EGV. Das würde auch nur gelten „*bei der Durchführung der Personenkontrollen an diesen Grenzen*“, vgl. Art. 62 Nr. 2 a) EGV. Zumal Maßnahmen getroffen werden sollen, „*dass Personen, seien es Bürger der Union oder Staatsangehörige dritter Länder, beim Überschreiten der Binnengrenzen nicht kontrolliert werden*“, vgl. Art. 62 Nr. 1 EGV. Sofern jedoch die biometrisch gestützten Grenzkontrollen an den EU-Außengrenzen auf der Zwei-Finger-Präsentation basieren sollte, würde die Europäische Union quasi zu einer „biometrischen Insel“: Die Prüfung der Bindung von biometrischer Charakteristik zum Pass könnte lediglich für EU-Bürger vorgenommen werden, da Bürger anderer Herkunft keine entsprechenden Referenzen in ihren Pässen vorweisen könnten – „*das ist ein europäischer Alleingang, der hier gewählt wird*“ (vgl. *Peter Schaar*, in: Protokoll Nr. 16/37 zur öffentlichen Anhörung des Innenausschusses des Bundestages am 23. April 2007, S. 63). Und vor (seltener) betrügerischer Verwendung von EU-Reisepässen durch Drittstaatsangehörige würden die Fingerabdruckdaten wahrscheinlich zerstört, ohne das dies „auffallen“ müsste:

„*Wir würden davon ausgehen, dass die Haltbarkeit nicht länger als 4 bis 5 Jahre gegeben ist, aufgrund allein der mechanischen Belastung, wenn man sieht, wie wir teilweise mit unseren Pässen umgehen*“ (vgl. *Lukas Grunwald*, in: Protokoll Nr. 16/37 zur öffentlichen Anhörung des Innenausschusses des Bundestages am 23. April 2007, S. 40). Dazu noch: „*Der Anteil der Bevölkerung, der beispielsweise durch Hautkrankheiten – temporär oder dauerhaft – keine Fingerbilder in ausreichender Qualität liefern kann, wird von Hausärzten auf 3% bis zu 11% geschätzt*“ (vgl. *Christoph Busch*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Passgesetzes und weitere Vorschriften, in: Innenausschuss-Drucks. 16(4)192 A, S. 4).

Die obligatorische Erfassung von Fingerabdrücken ist also „offensichtlich ungeeignet“ zum Schutz vor einer betrügerischen Verwendung von Pässen oder Reisedokumenten beizutragen.

Die obligatorische Erfassung von Fingerabdrücken ist nicht erforderlich, um die gesetzten Ziele zu erreichen. Das Gebot der „Erforderlichkeit“ setzt voraus, dass es kein alternatives Mittel gibt, mit dem das verfolgte Ziel ebenso gut erreicht werden kann und das weniger in das Grundrecht eingreift (vgl. *EuGH*, Rs. 265/87, Slg. 1989, 2237 Rn. 21; Rs. 254/94, Slg. 1996, I-4235 Rn. 55; BVerfGE 53, 135 [145 ff.]; 102, 197 [217 f.]; 103, 1 [17 ff.]).

„Zum Schutz vor Fälschungen“ bedarf es überhaupt keiner „Aufnahme biometrischer Identifikatoren“, und mithin auch nicht der obligatorischen Erfassung von Fingerabdrücken. Das zeigt schon der EG-Reisepass, der in der Bundesrepublik Deutschland am 1. Januar 1988 eingeführt wurde. Damit sind Nachfertigungen (Fälschungen) weitestgehend ausgeschlossen und Nachahmungen sowie Verfälschungen leicht erkennbar geworden:

*„Die seit Einführung des neuen Ausweissystems gemachten Erfahrungen zeigen, dass mit der zentralen Herstellung und dem auf dem Prinzip der Integration der Ausweisdaten basierenden Sicherheitskonzept die Schwachstellen der alten Ausweispapiere beseitigt wurden. Seit 1987 wurden mehr als 90 Millionen neue Personalausweise und EG-Reisepässe produziert. Verfälschungsversuche beschränkten sich auf äußerliches Überkleben einzelner Daten und ähnlich einfache Manipulationen, die fälschliche Ausstellung ist bei den neuen Dokumenten durch das System unterbunden. Lediglich Nachahmungsversuche von Personalausweiskarten durch Einsatz moderner Farbkopiertechniken sind inzwischen in einigen Fällen bekannt geworden. Abgesehen vom Fehlen der nicht kopierbaren Echtheitskriterien sollten derartige Falsifikate bei entsprechender Kontrolle aber nach wie vor an der durch Farbaufbau und Rasterung bedingten Unschärfe und mangelnder Detailauflösung der Reproduktionsergebnisse im Vergleich zum Originalsicherheitsdruckbild erkennbar sein“* (vgl. *Edgar Friedrich*, Sicherungstechnische Anforderungen bei Ausweisdokumenten als Präventionsansatz gegen Identitätsmanipulationen, in: Bundeskriminalamt (Hrsg.), Aktuelle Methoden der Kriminaltechnik und Kriminalistik, Wiesbaden 1995, S. 227 ff. [234 f.]).

„Zum Schutz vor Fälschungen“ empfehlen sich also keine Fingerabdrücke, sondern Echtheitsmerkmale wie mehrstufige Wasserzeichen, lumineszierende Melierfasern, Guillochen- und Mehrfarben-Irisdruck, Kippeffekt- und Mikroschriftelemente, Reliefprägungen, Laminierungen und Hologramme oder Kinegramm-Strukturen sowie materialmäßig und

verfahrenstechnisch immer weiter denkbare Kriterien, die aber das Recht auf informationelle Selbstbestimmung vollkommen unberührt lassen, also jedenfalls auch „mildere“ Mittel sind.

Die obligatorische Erfassung von Fingerabdrücken ist auch nicht erforderlich, um „*erheblich zum Schutz vor einer betrügerischen Verwendung von Pässen oder Reisedokumenten bei- [zu]tragen*“. Denn es gibt ein alternatives Mittel, mit dem das verfolgte Ziel - die maschinelle Identifizierung von Personen zu verbessern und zu verhindern, dass Personen sich mit fremden Papieren ähnlich aussehender Personen ausweisen – besser erreicht werden kann. Dabei handelt es sich um die „Iriserkennung“, ein biometrisches Verfahren, mit dem auch sehr viel weniger in das Grundrecht auf informationelle Selbstbestimmung eingegriffen wird.

Als Iris oder Regenbogenhaut wird der farbige Ring um die Pupille bezeichnet. Sie ist ein frontal gestelltes Segel zwischen vorderer und hinterer Augenkammer und damit ein Teil der mittleren Augenhaut. Im Zentrum der Iris befindet sich eine zentrale kreisrunde Öffnung – das Sehloch (Pupille). Die Iris jedes Menschen zeichnet sich durch ein einzigartiges Muster aus. Dieses Muster wird durch ein komplexes Gewebegeflecht geformt. Es bildet sich vorgeburtlich aus und bleibt konstant über die gesamte Lebenszeit (vgl. *Marco Breitenstein*, in: *Veronika Nolde/ Lothar Leger* (Hrsg.), *Biometrische Verfahren*, Köln 2002, S. 50).

Die Iris verfügt über den großen Vorteil, dass sie ein durch die Cornea geschütztes inneres Organ des Auges ist. Dadurch ist sie weitgehend immun gegenüber Umwelteinflüssen (vgl. *Marco Breitenstein*, in: *Veronika Nolde/ Lothar Leger* (Hrsg.), *Biometrische Verfahren*, Köln 2002, S. 50). Dagegen wird die Fingerbildererkennung durch Umweltbedingungen oder handwerkliche Tätigkeit erheblich beeinträchtigt. So können 3% bis zu 11% der Menschen dauerhaft oder temporär keine Fingerbilder in ausreichender Qualität abgeben (vgl. *Christoph Busch*, Stellungnahme zum Entwurf eines Gesetzes zur Änderung des Passgesetzes und weitere Vorschriften, in: *Innenausschuss-Drucks. 16(4)192 A*, S. 4), während bei nur 0,000018% der Menschen überhaupt keine Iris vorhanden ist (vgl. *Thomas Bengs/ Waldemar Grudzien*, *Biometrie in der Kreditwirtschaft*, in: *DuD 31* (2007), S. 157 ff. [158]).

Das zeigt sich auch in der Leistungsfähigkeit biometrischer Systeme, die bestimmt wird durch die Falschrückweisungsrate berechtigter Personen (FRR) und die Falschakzeptanzrate unberechtigter Personen (FAR). Entscheidend sowohl für das Sicherheitsniveau als auch die Akzeptabilität des Systems ist das Verhältnis der FAR zur FRR: „*Im Ergebnis sind schon für*

die Eignung automatischer Kontrollen Fehlerraten (FAR und FRR) von unter 1% zu fordern. Diese Anforderung dürfte derzeit nur die Iriserkennung erfüllen“ (vgl. Alexander Rosßnagel/ Gerrit Hornung, Biometrische Daten in Ausweisen, in: DuD 29 (2005), S. 69 ff. [70]).

Bei Tests von Fingerabdrucklesern erreichte kein System eine FRR unter 5%. Ein Hamburger Kernkraftwerk verwendet seit fast zehn Jahren Fingerabdruckleser zur Zutrittskontrolle. Dort hat sich die FRR um die 8,5% eingependelt (vgl. Marco Breitenstein, in: Veronika Nolde/ Lothar Leger (Hrsg.), Biometrische Verfahren, Köln 2002, S. 39). Andernorts ließe sich mit der Identifikation von zwei Fingern oder mit dem zweimaligen Auflegen desselben Fingers möglicherweise eine Verifikations-FAR von  $10^{-8}$  bei einer FRR von 10% erreichen! Wegen möglicher Korrelationen beim zweimaligen Auflegen desselben Fingers kann die FRR im theoretischen Worst-Case aber auch ca. 30% betragen! (vgl. Manfred Bromba, Ein biometrisches Bezahlssystem für Kaufhäuser, in: DuD 31 (2007), S. 194 ff. [197]).

Die Iris ist das einzige innere Organ des Körpers, dass von außen gesehen werden kann. Das Risiko einer Verfälschung ist dadurch verringert, dass jede versuchte Manipulation die Gefahr der Erblindung birgt (vgl. Marco Breitenstein, in: Veronika Nolde/ Lothar Leger (Hrsg.), Biometrische Verfahren, Köln 2002, S. 50), während es in Skandinavien bereits im ersten Jahr nach der Einführung von Fingerabdrücken im Asylverfahren über 100 Selbstverstümmelungen der Finger gegeben haben soll (vgl. Silke Stokar von Neuforn, in: Protokoll Nr. 16/37 zur öffentlichen Anhörung des Innenausschusses zum Passgesetz am 23. April 2007, S. 61).

Fingerabdrücke sind sogenannte „flüchtige biometrische Daten“. Hinterlassen biometrische Merkmale aber vielerorts häufig und dauerhaft Spuren, so besteht ein erheblich größeres Risiko, dass diese Spuren erhoben und die so gewonnenen Daten mit den für den Pass erhobenen Daten verglichen werden. So besteht beim Fingerabdruck das Risiko einer Datenerhebung von Alltagsgegenständen, während die Iris als „nicht-flüchtiges“ biometrisches Merkmal nirgendwo Spuren hinterlässt (vgl. Alexander Rosßnagel/ Gerrit Hornung, Biometrische Daten in Ausweisen, in: DuD 29 (2005), S. 69 ff. [70] m. w. N.). So wollen Kriminologen keine Iris erfassen, sondern Fingerabdrücke, auch: „genetisch“ (vgl. Christean Wagner, Effektive Strafverfolgung durch DNA-Kartei für alle Straftaten, in: ZRP 2004, S. 14 ff.).

Während also Fingerabdrücke vielerorts häufig ohne Mitwirkung und Wissen der betroffenen Personen erfasst werden, ist die Iriserkennung durch ihre strenge Mitwirkungsgebundenheit

ausgezeichnet, was auch dem datenschutzrechtlichen Transparenzgebot entspricht. Denn eine unbemerkte Datenerhebung scheidet nahezu aus, auch wenn es Verfahren gibt, die eine Merkmalerhebung aus einem Meter Entfernung zulassen (vgl. *Alexander Rossnagel/ Gerrit Hornung*, Biometrische Daten in Ausweisen, in: DuD 29 (2005), S. 69 ff. [70] m. w. N.).

Während sich die Iriserkennung durch hohe Fälschungssicherheit bei Einsatz einer geeigneten Lebenderkennung auszeichnet (vgl. *Marco Breitenstein*, in: *Veronika Nolde/ Lothar Leger* (Hrsg.), Biometrische Verfahren, Köln 2002, S. 50), bergen Fingerabdrücke nach ihrer Art, vielerorts häufig dauerhaft Spuren zu hinterlassen, Fälschungsrisiken, die über jede Lebenderkennung erhaben sind - und das birgt für jeden Merkmalsträger ein unkalkulierbares Risiko:

*„In Marseille wurde ein Engländer monatelang wegen Mordes in Haft gehalten, weil auf der in einem Taxi gefundenen Mordwaffe ein scharfer Fingerabdruck von ihm gesichert worden war. Diesen hatte sich der Täter dadurch verschafft, dass er mit dem Engländer Karten gespielt hatte. Einen dabei von dem Ahnungslosen hinterlassenen Abdruck hatte er fotografiert, um sodann mit Hilfe des Metallabzugs einen Kautschukstempel herzustellen; der so auf seinen Handschuh praktizierte Abdruck des Engländers war seitenrichtig“* (vgl. *Friedrich Geerds*, in: *Hans Groß/ Friedrich Geerds*, Handbuch der Kriminalistik, 10. Aufl., Berlin 1977, Band I, S. 570).

Während die Iriserfassung keinen Ansatzpunkt für eine kriminalistische Strafverfolgung und keinen Ansatzpunkt für eine kriminelle Falschverdächtigung bietet, ist im Falle der obligatorischen Erfassung von Fingerabdrücken mit derart krimineller Energie und daraus resultierendem Strafverfolgungsrisiko zu rechnen - mindestens in proportionaler Abhängigkeit des Umstandes, ob und inwieweit die Strafverfolgungsbehörden in der Lage sind, Tatortfingerspuren bestimmten Personen zuzuordnen. Zur Zeit sind fast drei Millionen Personen im Automatisierten-Fingerabdruck-Identifikations-System AFIS beim BKA registriert (vgl. *Frank Künzer*, in: *Veronika Nolde/ Lothar Leger*, Biometrische Verfahren, Köln 2002, S. 284). Mit der Erfassung der Fingerabdrücke von 88 Millionen Deutschen ist zu befürchten, dass es nicht nur potentiell Dreißigfach mehr Fälle geben wird, in denen eine Strafverfolgung bezüglich gefälschter Fingerabdrücke erfolgt. Die Brisanz steht im Zusammenhang wie folgt:

*„Fingerabdrücke auf dem Ausweis sind sicherheitstechnisch eine Katastrophe... Die Ausweise per Funk auslesbar zu machen, schafft zusätzliche Risiken... Fingerabdrücke in*

*Pässe helfen Kriminellen und nicht nur Strafverfolgern... Ich halte die Sache für dermaßen kritisch... bis dahin, dass ich dem einzelnen Bürger eine Art Notwehrrecht zugestehen würde, sich dieser Sache zu verweigern... Die Aufnahme des biometrischen Merkmals „Fingerabdruck“ in Pässe und insbesondere seine Prüfung werden Menschen daran gewöhnen, ihre Fingerabdrücke an von ihnen nicht kontrollierbaren Geräten in hoher Qualität abzugeben. Es geht mir jetzt nicht darum, dass die Pässe unsicher sind, sondern die Menschen werden ihren Fingerabdruck bei vielerlei Gelegenheit abgeben. Damit werden Fingerabdrücke vielen Akteuren zugänglich... All diese werden sich dieser Technik anschließen... Sie werden dort ein Gerät hinstellen und die Fingerabdrücke abnehmen und die Bundesbürger werden ihre Fingerabdrücke dort abgeben, denn sie sind entsprechend konditioniert. Damit haben fremde Geheimdienste und auch Kriminelle nach kurzer Zeit eine große Sammlung von deutschen Fingerabdrücken, und sie werden natürlich von diesen Mitteln in ihrem Sinne Gebrauch machen... Sie können mit Fingerabdrücken, mit Bildern von Fingerabdrücken so gute Fingerreplikate herstellen, dass gängige Fingerabdrucksensoren problemlos zu überlisten sind. Schlimmer noch ist, wenn sie noch ein bisschen Biologie und Chemie kennen, und das ganze mit ein paar Aminosäuren anreichern, dann werden Sie auch damit am Tatort Fingerabdrücke hinterlassen können, die zumindest für die Forensik eine große Herausforderung darstellen, ob sie die von natürlichen Fingerabdrücken unterscheiden können. Damit wird es Kriminellen wie auch fremden Geheimdiensten gelingen, falsche Spuren am Tatort zu hinterlassen. Sei es, um die Polizei in die Irre zu schicken... oder aber... Personen in eine Notlage zu bringen, dass sie sich recht-fertigen müssen, dass sie mit diesem Verbrechen nichts zu tun haben. Und der vernehmende fremde Geheimdienst wird sagen: „Wissen Sie, wenn Sie mit uns zusammenarbeiten, sind Sie alle diese Probleme los.“ Das ist aus meiner Sicht der kritischste Punkt, den ich Sie bitte, nicht passieren zu lassen. Die Auswirkungen, wenn Sie es passieren lassen, wären katastrophal“ (vgl. Andreas Pfitzmann, in: Protokoll Nr. 16/37 der öffentlichen Anhörung des Innenausschusses des Bundestages zum Passgesetz am 23. April 2007, S. 13 ff.).*

Diese Falschverdächtigungs- und Erpressungsrisiken, die auch für freiheitlich demokratische Rechtsstaaten selbst fundamental bedrohlich sind, sie lassen sich nicht einfach negieren, wenn auch der Bundesinnenminister *Wolfgang Schäuble* und andere erklären mögen, dass selbst ihre Fingerabdrücke ja schließlich schon lange abgenommen werden könnten, beispielsweise von Gläsern, die natürlich tagtäglich vielerorts nicht sogleich persönlich abgewaschen werden. Dabei wird gleichwohl verkannt, dass sich Falschverdächtigungen und Erpressungen

mit abgenommenen und gefälschten Fingerabdrücken beim Hinterlassen an Tatorten von Tätern glaubhaft nur darstellen lassen, wenn damit ein „Strafverfolgungsrisiko“ begründet werden kann. Es setzt voraus, dass die Kriminalisten ein älteres Register, eine Sammlung, eine Datenbank mit Fingerabdrücken haben. Vergleichung ist der methodische Kern der Daktyloskopie. Identifikation ist nur als Wiedererkennung möglich. Nur wessen Fingerabdrücke nicht registriert sind, der kann damit auch nicht verdächtigt oder erpresst werden.

Die obligatorische Erfassung von Fingerabdrücken ist schließlich auch „unangemessen“, weil die verursachten Nachteile in keinem angemessenen Verhältnis zu dem angestrebten Ziel stehen und die Maßnahme im Hinblick auf den verfolgten Zweck einen unverhältnismäßigen, nicht tragbaren Eingriff darstellt. Dafür sprechen schließlich sowohl die Belange des Allgemeinwohls als auch die Erfordernisse des Schutzes der Grundrechte des Einzelnen.

Hier ist davon auszugehen, dass „*die in den Mitgliedsstaaten der Europäischen Union ausgestellten Pässe und Reisedokumente*“ im Rahmen der gewählten Rechtsgrundlage – mithin: „*bezüglich des Überschreitens der Außengrenzen der Mitgliedstaaten*“ und „*bei der Durchführung der Personenkontrollen an diesen Grenzen*“, vgl. Art. 62 Nr. 2 a) EGV – kaum eine betrügerische Verwendung durch Unionsbürger finden können. Denn dafür müssten nach dem Schutzzweck der Norm schon Ein- oder Ausreisebeschränkungen bestehen, die aber jedenfalls zu vernachlässigen sind im freiheitlichen Kontext, dem sich die Europäische Union insgesamt verschrieben hat. So kann denn nur der Schutz vor (seltener) betrügerischer Verwendung der in den Mitgliedsstaaten der Europäischen Union ausgestellten Pässe oder Reisedokumente durch Drittstaatsangehörige im angeblichen Regelungszusammenhang bestehen bleiben. Dabei wird offensichtlich das allgemeine Problem der „Migration“ mit einer „Kriminalisierung“ kurzgeschlossen, und die obligatorische Erfassung der Fingerabdrücke von 490 Millionen Unionsbürgern soll „*erheblich beitragen*“, diese zu bekämpfen - zuoberst: „*ein gleichgültiges und zynisches Informationsregime, das kein Interesse hat an den Personendaten all jener Personen, die es für unerwünscht erklärt*“ (vgl. Valentin Groebner, *Der Schein der Person – Steckbrief, Ausweis und Kontrolle im Mittelalter*, München 2004, S. 176). Das ist vollkommen abwegig – „*unangemessen*“ und „*untragbar*“.

Weiter ist davon auszugehen, dass mit der obligatorischen Erfassung der Fingerabdrücke aller Unionsbürger ein supranationales Passregister entsteht (vgl. *Kommission der EG*, in: KOM(2004) 116, S. 7). Es entstehen auch nationale Passregister (vgl. *Gerrit Hornung*,

„Digitale“ Ausweise im Ausland, in: DuD 29 (2005), S. 62 ff. [65]). Dafür ist in jedem Falle, also sozusagen auch für den „Notfall“ vorgegeben, dass der Pass 10 Jahre gültig ist, während die Fingerabdruckdaten dort durchschnittlich nur 4-5 Jahre „haltbar“ sind!? – Schließlich entstehen auch private Fingerabdruckdatenbanken (vgl. *Manfred Bromba*, Ein biometrisches Bezahlungssystem für Kaufhäuser, DuD 31 (2007), 194 ff.). Mit der obligatorischen Erfassung von Fingerabdrücken in Pässen und Reisedokumenten wird letztlich allenthalben der Zwang zur Gewohnheit und so zu einem Geschäft zu Lasten Dritter, sogenannter: „freier Bürger“.

Denn gewöhnlich wie geschäftlich werden biometrische Daten in Datenbanken so verwaltet, dass sie als „Zugriffsschlüssel“ für die verschiedensten Datensätze einer Person verwendet werden sowie dazu, verschiedenste Daten zu einem Profil einer Person zusammenzuführen. Das ist die Funktion eines „Personenkennzeichens“. Die derzeitige Praxis, Kombinationen aus personenbezogenen Daten, beispielsweise Name *und* Adresse *und* Geburtstag zu verwenden, ermöglicht es auch heutzutage, Informationen aus verschiedensten Datenbeständen zusammenzuführen. Es ist aber immerhin noch möglich, eine solche Informationskette willentlich zu unterbrechen, etwa durch Namenswechsel, Umzug und Sperrung der Adressweitergabe. Damit kann Dritten der Zugriffsschlüssel auf ihre x-beliebigen Datensammlungen quasi auch wieder entzogen werden. Genau diese Möglichkeit würde entfallen, wenn biometrische Merkmale, die sich gerade durch ihre „Personengebundenheit“ auszeichnen, als Schlüssel für Datenbankzugriffe verwendet würden: „*Die Gefahr, dass der Inhaber irgendwann die alleinige Kontrolle über die Verknüpfung seiner Person mit seinen biometrischen Daten verliert, kann nicht vernachlässigt werden*“ (vgl. *Peter Biltzinger*, Biometrie und Datenschutz, in: DuD 29 (2005), S. 726 ff. [729]). Dem Gemeinwohl in freiheitlich demokratischen Rechtsstaaten kann es zudem nur abträglich sein, wenn alle Bürger erkennungsdienstlich behandelt und so „diszipliniert“ werden, die „Schlüsselgewalt“ ihrer „Personenkennzeichen“ auf unbeschränkbare Zeit und unabsehbare Folgen „abzugeben“. Das ist ebenfalls vollkommen „unangemessen“ und „untragbar“.

Schließlich ist davon auszugehen, dass mit obligatorischer Erfassung von Fingerabdrücken, diese auch mit Tatortspuren abgeglichen werden. Schon jetzt gelingen der Spurensicherung in Deutschland jährlich rund 13.000 Treffer, also Identifizierungen von Personen oder latenten Tatortspuren durch den Abgleich mit den laufenden Beständen (vgl. *Katharina Teutsch*, in: FAZ vom 1. November 2007, S. 33). So ist zu ermessen, dass und wie weit die obligatorische Erfassung von Fingerabdrücken einem Zwang zur Selbstbeichtigung nahe kommt – und:

*„demselben Prinzip zufolge [ist] der perfekte Ausweis derjenige, der ein Fehlverhalten seines Besitzers oder seiner Besitzerin dokumentiert... Identifikation als Kontrolle heißt, den Kontrollierten in einen Zustand zu bringen, in dem er bereits einen Fehler gemacht hat, den er daraufhin dauernd verdecken, verbergen oder wiedergutmachen muss. Das ist das Verfahren, dass die politische Praxis des Identifizierens bestimmt“* (vgl. Valentin Groebner, *Der Schein der Person – Steckbrief, Ausweis und Kontrolle im Europa des Mittelalter*, München 2004, S. 179). Zuletzt die Antastung der Menschenwürde macht bereits die obligatorische Erfassung von Fingerabdrücken *„unangemessen“* und *„untragbar“*.

### 3 Perspektiven

*„Mit ubiquitous computing, allgegenwärtigem Rechnen, gelangt die Datenverarbeitung in die Alltagsgegenstände der körperlichen Welt – und damit auf eine neue, dritte Stufe. Sie erfasst potenziell alle Lebensbereiche und diese potenziell vollständig. In dieser Welt wachsen Körperlichkeit und Virtualität zusammen. Informationen aus der virtuellen Welt werden in der körperlichen verfügbar, Informationen aus der realen Welt in die virtuelle integriert. Aus dieser Welt und der in ihr stattfindenden Datenverarbeitung gibt es keinen Ausweg. Insofern verschärft sich das Problem des Datenschutzes radikal, und seine Lösung wird existenziell... Zusammenfassend ist festzustellen: Alle Bestandteile des überkommenen Schutzprogramms werden durch allgegenwärtige Datenverarbeitung ausgehöhlt oder überspielt. Daher ist die Frage ganz grundsätzlich zu stellen, ob unter diesen Verhältnissen informationelle Selbstbestimmung überhaupt noch möglich ist“ (vgl. Alexander Rossnagel, Datenschutz im 21. Jahrhundert, in: APuZ 5-6/2006, S. 9 ff. [10, 13]. Das muss allerdings so sein.*

Im Falle der obligatorischen Erfassung von Fingerabdrücken in Pässen und Reisedokumenten wird das informationelle Selbstbestimmungsrecht dagegen geradezu negiert oder vernichtet. Die Maßnahme exemplifiziert, dass die Aufhebung von Grundrechten in rechtlich geordneter, d.h. legaler Weise, zu gesetzlichem Unrecht führt. Das Konzept der obligatorischen Erfassung von Fingerabdrücken will dieses Unrecht legalisieren und geht damit hinter den Stand der Rechtstheorie und Praxis der informationellen Selbstbestimmung zurück, der nach dem Fall pervertierter Rechtssysteme der Neuzeit erreicht worden ist - beispielweise nach der NS-Zeit.

*„So stieß etwa – in einer erfreulich sauberen Wertreaktion – die Beibehaltung der Fingerabdrücke auf Personalausweisen auf einhellige Ablehnung, obwohl sie (für die Polizei) durchaus „zweckmäßig“ gewesen wäre“ (vgl. Günter Dürig, in: Theodor Maunz/ Günter Dürig/ Roman Herzog/ Rupert Scholz/ u.a., Grundgesetz, Kommentar, Band I, München 1989, Art. 1 Abs. 1, Rdnr. 37).*

*„Aber an einem Beispiel der primitivsten, die Menschen unterscheidenden biologischen Originalität mag verdeutlicht werden, dass es auch für den modernen Staat letzte Sperren vor der verwaltungstechnischen – im übrigen durchaus gutgemeinten und keineswegs diskriminierend gedachten - „Ent-persönlichung“ gibt“ (vgl. Günter Dürig, in: Theodor Maunz/ Günter Dürig/ Roman Herzog/ Rupert Scholz/ u.a., Grundgesetz, Kommentar, a. a. O.).*

*„Die jüngeren Diskussionen über den internationalen Terrorismus haben die Perspektive einseitig auf die Risiken der Freiheit gelenkt. Dahinter tritt die andere Blickrichtung, nämlich auf die Chancen einer Politik zur Herstellung von Freiheit, völlig zurück. Es geht darum, der Sicherheitspolitik eine Freiheitspolitik zur Seite zu stellen. Sie muss mehr zu bieten haben als Überwachungsmaßnahmen und Grundrechtseingriffe. Eine notwendig mittel- bis langfristige Freiheitspolitik muss bei den Ursachen ansetzen, welche Risiken wie etwa den Terrorismus hervorbringen. Diese Ursachen sind umrisshaft bekannt. Dazu zählen krasse und offensichtliche soziale Gegensätze zwischen Arm und Reich auf engstem Raum; ein hohes Maß an sozialer Unsicherheit der Menschen in den Wechselfällen des Lebens; das Bewusstsein ethnischer, kultureller oder religiöser Benachteiligung bei offenkundiger Bevorzugung anderer Gruppen und die politische, ökonomische und soziale Aussichtslosigkeit, diesen Verhältnissen individuell oder kollektiv zu entrinnen“ (vgl. Christoph Gusy, Geheimdienstliche Aufklärung und Grundrechtsschutz, in: APuZ B 44/2004, S. 14 ff. [20]). Zur Zeit aber weisen „Globalisierung“, „Terror“ und „Krieg“ noch in eine andere Richtung:*

*„Wir sind auf dem Weg zu einer globalen Sicherung von Herrschaftsansprüchen ohne Recht“ (vgl. Peter-Alexis Albrecht, Abschied vom Recht, in: vorgänge Heft 2/2007, S. 27 ff. [28]).*

*„Grüße! – aus dem Zeitalter der Uniformität... aus dem Zeitalter des Doppeldenk – Grüße!“  
(vgl. George Orwell, 1984, 30. Aufl., Berlin 2007, S. 37)*