„Internationaler Datenschutz und Rechtsschutz beim Austausch biometrischer Daten – eine Würdigung des ePasses und des Prümer Ratsbeschlusses“

Dissertation

zur Erlangung des Doktorgrades

der Fakultät für Rechtswissenschaft

der Universität Regensburg

Vorgelegt von

Carmen Fritz, geb. Hangl

Erstberichterstatter: Prof. Dr. Uerpmann-Wittzack

Zweitberichterstatter: Prof. Dr. Kühling

Tag der mündlichen Prüfung: 03.07.2012

Vorwort

Während des Studiums hatte ich immer den Wunsch zu promovieren, um bei der Abschlussfeier einen dieser anglo-amerikanischen Doktorhüte tragen zu können. Leider ist dies in Deutschland mittlerweile unüblich geworden, weshalb dieser Grund leider ein Wunschtraum blieb. Grund für meine Promotion war daher, dass ich im Laufe meines Studiums beim Schreiben meiner Seminararbeiten einen gewissen Anreiz daran gefunden hatte, ein Thema aufzubereiten. Während der Arbeit an meiner Dissertation stellte sich jedoch heraus, dass die Länge der Arbeit wohl den Reiz mit beeinflusste, denn die Dissertation ist nun mal keine Seminararbeit von zwanzig Seiten Länge. Ausschlaggebend war letztendlich daher mein bis dato gefundenes Thema, nämlich „biometrische Daten“ und „Datenschutz“, was mich ungemein interessierte.

Während der dreijährigen Anfertigung meiner Dissertation durchlief ich verschiedene Phasen des „Sinns und Unsinns“ meiner Arbeit. Ich kürzte mehrmals das Thema und verlor mehrfach den Faden aufgrund der Fülle an Literatur und Ideen. Meine beiden ersten Einführungskapitel dauerten bereits eineinhalb Jahre. Das Hauptkapitel fing ich erst während des Referendariats an.

Ziel meiner Arbeit war eigentlich, die Biometrie und deren Gefahren für den Persönlichkeitsschutz des Bürgers darzustellen und hierfür Lösungen zur Verbesserung des Problems zu entwickeln. Während meiner Arbeit habe ich jedoch - und hierfür danke ich dem Landeskriminalamt Bayern besonders – auch die positiven Seiten des Einsatzes von Biometrie erkennen müssen. Letztendlich versuchte ich einen Ausgleich zwischen Datenschutz und der Arbeit der Ermittlungsbehörden zu finden.

Ich möchte mich daher gerade bei meinem Doktorvater Prof. Dr. Uerpmann-Wittzack bedanken, welcher meine Arbeit trotz meiner Zwiespältigkeit förderte und mich erfolgreich durch das Promotionsverfahren leitete. Ebenso danke ich Prof. Dr. Kühling für sein Zweitgutachten.

Diese Abhandlung wurde im Frühjahr 2012 von der Universität Regensburg als Dissertation angenommen.

Dank gebührt auch meinen Eltern für ihre Unterstützung.

Mein größter Dank gilt aber meinem Mann, Dominik Fritz, welcher mich durch alle Phasen meiner Promotion begleitete und mich nicht nur finanziell unterstützte, sondern auch aus so manchen Tiefen herausholte und mir half, durchzuhalten. Ich danke dir dafür.

12. November 2012 Carmen Fritz

INHALTSVERZEICHNIS

TEIL A Einführung

Die Biometrie wird seit Jahrhunderten angewandt. Bereits Frühe archäologische Funde weisen darauf hin, dass Fingerabdrücke bereits in der Zeit vor Christus als Identifikationsmerkmal genutzt wurden.[1] So dienten sie schon bei den Babyloniern (ca. 1500 v. Chr.) als Signatur auf Urkunden. In China wurden die Fingerabdrücke zwischen 600 und 900 n. Chr. auf Tonsiegeln oder in Strafverfahren verwendet.[2] Doch in neuerer Zeit wird die Biometrie überwiegend zu Überwachungszwecken eingesetzt. So wurden bei einem Football-Spiel in Tampa am 01.02.2001 zwanzig Kameras installiert. Ein Computer verglich mittels einer neuen Software bis zu 128 verschiedene Gesichtsmerkmale eines jeden Stadionbesuchers und konnte diese letztlich 19 Personen zuordnen, welche bereits straffällig und damit in einer Verbrecherkartei vermerkt waren.[3] Für die olympischen Spiele 2004 in Athen wurde ein Budget für Sicherheitsmaßnahmen in Höhe von einer Milliarde Euro eingeplant, welche in rund 2000 Überwachungskameras sowie in eine Software investiert werden sollten, das potentielle Attentäter durch die Gangart und Handbewegungen entlarven sollte.[4] Man erkennt bereits an diesen Beispielen das Potential der biometrischen Überwachung.

Die biometrische Verfahrensweise dient auch gerade dem Interesse der grenzüberschreitenden Ermittlungen, da diesem ein System zugrundeliegt, welches von jedem Staat angewendet werden kann,

---

[1] Hamann, S. 5.
[2] BSI, Grundsätzliche Funktionsweise biometrischer Verfahren, s. unter https://www.bsi.bund.de/ContentBSI/Themen/Biometrie/AllgemeineEinfuehrung/einfuehrung.html.
[3] Heise-online vom 01.02.2001, „Neue Videoüberwachung beim Super Bowl getestet".
[4] Schulzki-Haddouti, S. 31.

sofern entsprechende Kriterien zum Gebrauch geregelt werden. Gerade angesichts der fortschreitenden Entwicklung im Bereich der grenzüberschreitenden Kriminalität sowie der immer neuen technischen Ausstattungen der Straftäter müssen polizeiliche Ermittlungs- sowie die Präventionsmaßnahmen dem Laufe der Zeit angepasst werden. Auch muss immer schnellere Aufklärungsarbeit geleistet werden, um Tätern keine Chance zu lassen, gerade frei gewordene Nischen wieder zu besetzen. Grenzüberschreitende Ermittlungen sind daher enorm wichtig. Hierzu leisten entsprechende Informationssysteme, evtl. unter Anwendung der Biometrie, einen wertvollen Beitrag. Letztere müssen nicht unbedingt zentral vernetzt werden, wie bspw. das Schengener Informationssystem, um ein schnelle Ermittlungserfolge vorweisen zu können. Es reicht durchaus die dezentrale Vernetzung (wie bspw. beim ePass), um Daten miteinander abgleichen zu können.

Hauptthema dieser Arbeit ist der internationale Datenschutz und dessen Beachtung im Rahmen der Einführung des ePasses und „Beschlusses 2008/615/JI des Rates vom 23.06.08 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität“, wobei letzterer Ratsbeschluss Teile des Prümer Vertrages enthält, deshalb im Weiteren auch „Prümer Ratsbeschluss“ genannt.

Basierend auf den vorgenannten Hauptthemen beschäftigt sich diese Arbeit mit dem Austausch von biometrischen Daten nach dem Prümer Ratsbeschluss sowie den ePass-Regelungen, wobei nicht nur der Austausch betrachtet wird, sondern sämtliche Regelungen, die diese Vorschriften mit sich bringen. Dabei liegt das Augenmerk auf den internationalen Vorgaben der Europäischen Menschenrechtskonvention, dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ sowie dessen Zusatzprotokoll und den

hierfür entsprechenden Empfehlungen des Ministerkomitees Nr. R (87) 15 zur Nutzung von personenbezogenen Daten im Polizeibereich und Nr. 1181 (1992) über die Anwendung der DNA-Analyse im Rahmen der Strafrechtspflege.

In Teil B. werden zunächst die in dieser Arbeit wesentlichen biometrischen Merkmale vorgestellt, bevor in Teil C. auf den ePass, die polizeilichen Datenbanken und die europarechtlichen Regelungen zum Austausch von Daten eingegangen wird.

Im Hauptteil D. werden zunächst die internationalen Vorgaben kurz vorgestellt, um dann die materiell-rechtlichen Vorgaben zum Datenschutz, sei es durch Art. 8 EMRK bzw. durch die Datenschutzkonvention und die Empfehlungen, auszuwerten und anhand dieser Vorgaben sowohl den ePass als auch den Prümer Ratsbeschluss einer Prüfung hinsichtlich der Vereinbarkeit mit diesen Vorschriften zu unterziehen. Ebenso wird mit den verfahrensrechtlichen Vorgaben des Datenschutzes verfahren.

Teil E. wirft einen Blick auf die Zukunft der Biometrie, auf das bereits geschlossene bilaterale Abkommen Deutschlands mit den USA, auf weitere Änderungen auch beim Personalausweis und beim Führerschein sowie auf die zukünftigen Änderungen datenschutzrechtlicher Regelungen.

TEIL B Biometrische Daten

Der Begriff „Biometrie“ setzt sich zusammen aus den Wörtern „bios“ (gr.: „Leben“) und „metron“ (gr.: „Maße“) und bezeichnet die Vermessung von Lebewesen.[5] Die Biometrie ist aber nicht zu verwechseln mit der Biometrik, welche versucht, durch Untersuchungen des Menschen biologische, medizinische, ökologische und psychologische Zusammenhänge zu erkennen.[6]

Im Jahr 1890 hat der Anthropologe Alphonse Bertillon die Polizei auf die Einzigartigkeit bestimmter Körperteile hingewiesen, insbesondere hat er schon damals die Einzigartigkeit der Ohrmuschel erkannt. Bertillon entwickelte daraus eine kriminalistische Vorgehensweise – die Bertillonage. Von nun an wurden Täter fotografiert, in Größe, Länge und Gewicht vermessen und die besonderen Kennzeichen auf Karteikarten festgehalten. Der Erfolg der Biometrie bedeutete jedoch den Niedergang der Bertillonage, insbesondere als Bertillon selbst die Fingerabdruckerkennung zur Aufklärung eines Mordes einsetzte.[7] Bereits damals wurden entsprechend den Vorgaben Bertillons die Fotografien en face und en profil gefertigt – dies wurde bis heute beibehalten.[8] Da die Bertillonage sich weiterentwickelte und versuchte aus den körperlichen Messungen Veranlagungen zu

[5] Vgl. Schaar, Das Ende der Privatsphäre, S. 76.
[6] Europäisches Forum und Portal für Biometrie, siehe unter www.biometrie.eu/definition.
[7] Hamann, S. 22.
[8] Hamann, S. 16.

Verbrechen und Krankheiten abzuleiten (ähnlich der Biometrik), nahm man Abstand davon.[9]

A. ALLGEMEINES

Es gibt verschiedene Arten von biometrischen Daten. Diese werden aufgeteilt in verhaltensbasierte (dynamische) und physiologische bzw. biologische (statische) Merkmale. Zu der ersten Gruppe gehören die Handschrift, die Stimme/Sprechverhalten, das Tippverhalten und die Art und Weise des Ganges. Die Vorteile der verhaltensbasierten Merkmale liegen in der – wenn auch nur begrenzten – Änderbarkeit und damit in der Kontrolle durch den Nutzer. Zu den biologischen Charakteristika zählen dagegen bspw. die Gesichtsgeometrie, der Fingerabdruck und die DNA. Oftmals greifen die verhaltensbasierten und die biologischen Charakteristika ineinander wie bspw. bei der Stimme. Diese ist meist auch physiologisch bedingt. Eine genaue Trennung dieser beiden Arten ist daher oft nicht möglich sowie mitunter unnötig und soll daher nur eine grobe Gruppierung wiedergeben.

Biometrische Verfahren werden mittlerweile nicht mehr nur bei Ermittlungsbehörden oder im Ausweis eingesetzt, sondern auch in physischen Zugangskontrollen (z.B. ins Gebäude) oder logischen Zugangssystemen (z.B. Zugriffe auf einen PC). Die Biometrie dient heute sowohl der Legitimation (bspw. mithilfe von Ausweisen) als auch der Überwachung und Kontrolle (bspw. an öffentlichen Plätzen) als auch der Forensik.

[9] Heilmann, in: KrimJ 1/1994, 36 ff.; Meuth, S. 33.

I. PROBLEMFELDER DER BIOMETRIE

Mit der Biometrie sind auch vielfache Problemfelder verbunden. Zum einen besteht die Gefahr der Überwachung oder der Profilbildung durch Verkettung mehrerer Informationen, sei es durch mehrere biometrische Merkmale oder weitere personenbezogene Informationen. Zum anderen könnten die in den Merkmalen enthaltenen überschüssigen Informationen ausgewertet werden; näheres hierzu bei der Betrachtung der einzelnen Merkmale.

Ein Identitätsdiebstahl ist ebenfalls nicht auszuschließen, sofern und soweit hierfür kein technischer Schutz vorgesehen ist bzw. dieser dem technischen Fortschritt nicht angepasst wird. Durch folgendes Beispiel wird dies verdeutlicht: Bei der Gesichtserkennung könnte bspw. ein Angreifer ein Foto vor die Kamera zu halten. Eine solche Systemmanipulation könnte dadurch behoben werden, dass die Kamera das Bild „auf Bewegungen" überprüft (Zucken, Zwinkern, etc.). Nun könnte der Angreifer sich überlegen, eine Videoaufnahme vor die Kamera zu halten. Dem kann man allerdings mithilfe von thermischen Systemen abhelfen, d.h. das System prüft, ob der Gesichtshintergrund durchblutet wird. Jetzt könnte man noch auf die Idee kommen, eine Person gewaltsam vor die Kamera zu drängen.[10] Man sieht bereits an diesem Beispiel: Je ausgefeilter die Technologie des Täters ist, desto fortschrittlicher muss die Wissenschaft sein. Die gleiche Problematik findet sich auch bei den anderen biometrischen Merkmalen.

Diese Probleme sind jedoch nicht die einzigen, die auftreten können; vielmehr gibt es noch zahlreiche weitere Angriffsmöglichkeiten. Zum einen besteht die Möglichkeit, dem System eine große Anzahl unterschiedlicher Merkmale anzubieten,

[10] Vgl. zu diesem Beispiel Münch, S. 298 f.

d.h. dass bspw. statt einem Finger zehn Finger angeboten werden (sog. Brute-Force-Attacken). Dadurch erhöht sich die Wahrscheinlichkeit, dass der Finger erkannt wird, was gerade beim ePass relevant werden könnte. Zum anderen könnte das Sensorsignal eines Berechtigten (d.h. bspw. der Fingerabdruck) abgegriffen und gespeichert werden, damit er bei Bedarf wieder in das System eingespielt werden kann (sog. Replay-Attacken). Doch dieses Problem ist lösbar, indem man bspw. eine Software verwendet, welche prüft, ob sich das eingespielte Merkmal von dem gleichen zuletzt erkannten Merkmal unterscheidet. Dies ist auch durchführbar, da bspw. die Fingerkuppe jedes Mal in unterschiedlicher Weise auf den Sensor gedrückt wird. Ferner sollte noch die Latenzfingerabdruck-Reaktivierung erwähnt werden. Dies sind Fingerabdrücke oder zumindest brauchbare Reste, welche nach der Berührung des Sensors auf diesem als Fett- oder Hornhautrückstände verbleiben. Gerade hier kann der Einzelne selbst einem Missbrauch vorbeugen, indem er nach jedem Gebrauch den Sensor reinigt.[11]

Die Verwendung biometrischer Daten kann auch zu weitergehenden kriminellen Handlungen Dritter und anschließendem Datenmissbrauch führen. Schwerkriminelle werden vor Körperverletzungen oder gar Verstümmelungen nicht zurückschrecken. Um eine solche Vorgehensweise zu unterbinden, sollte man die Lebenderkennung bei jedem biometrischen Verfahren einsetzen. Bei Fingerabdrücken kann dies bspw. durch die Pulserkennung oder Temperaturmessung geschehen, während man beim Gesicht die Bewegung der Augen oder des Gesichtes in den Vergleichsvorgang mit einbeziehen könnte. Weitere Vorkehrungen kann man durch Kontrolle der Eingabe oder durch Zugriffsbeschränkungen treffen. Ferner ist es denkbar, dass der Nutzer zur Verwendung seines Merkmals gezwungen wird (vgl.

[11] Vgl. zu diesem Absatz Adlbrecht, Auf die Finger geschaut, S. 15 ff.

obiges Beispiel). Diesem könnte man mithilfe eines „stillen Alarms“ entgehen, bspw. indem man beim Fingerabdruck einen anderen Finger als üblich verwendet.[12]

Außerdem neigen Menschen zu ständigen äußerlichen Veränderungen. Die derzeitigen Systeme können aber selbst durch geringfügige Änderungen der biometrischen Merkmale noch verwirrt werden, wie bspw. durch das Tragen einer Brille. Auch die Mimik, selbst ein neutraler Gesichtsausdruck, kann aufgrund der Vielzahl von Gesichtsmuskeln derart stark variieren, dass die Person nicht erkannt wird. Altert ein Mensch, sinkt das Weichgewebe, was ebenfalls zu einer Nichterkennung führen kann. Weitere Fehler treten durch fehlerhafte Handhabung der Geräte, falsche Erfassung der Daten oder beim Vergleich auf. Ferner ist zu beachten, dass ein Mensch eben nur über zehn Finger, ein Gesicht etc. verfügt. Werden die Daten missbraucht, kann man diese nicht einfach auswechseln, wie dies bspw. mit einem Passwort möglich ist. Dies sind nur die allgemeinen Risiken; auf die besonderen Risiken der einzelnen Merkmale wird bei der Behandlung der jeweiligen Merkmale eingegangen.

Weitere Bedenken ergeben sich im Hinblick auf die Angst der Betroffenen vor der Einsetzung ihrer Daten bei der Strafverfolgung, welche nicht unbegründet ist. Der Straftatenkatalog für die DNA-Erfassung wird immer länger; so wurde bspw. 2005 in den deutschen § 81g StPO aufgenommen, dass allein die wiederholte Begehung von Straftaten zur DNA-Identitätsfeststellung berechtigt (vgl. dazu Pkt. IV.1.a). Mittlerweile wird die Gesichtserkennung immer mehr auf öffentliche Plätze ausgeweitet. So wurden bspw. in einem Einkaufszentrum im Londoner Stadtteil Newham mehr als 100 Kameras angebracht, deren Bilder mit den polizeilichen Datenbanken fortwährend

[12] TeleTrust, Kriterienkatalog, S. 52.

abgeglichen werden.[13] Die Akzeptanz der Bürger ist jedoch ein wichtiges Kriterium für den Einsatz von biometriebasierten Systemen.

Nachfolgend werden die wichtigsten Arten von biometrischen Daten (Gesichtsgeometrie, Fingerprint, DNA) genauer dargestellt, da auf diesen im weiteren Verlauf dieser Arbeit der Hauptaugenmerk liegt.

Die anderen biometrischen Daten, d.h. Iriserkennung, Sprecherkennung, Handschrif-tenerkennung sowie weitere biometrische Merkmale sind noch im Ausbau bzw. spielen eher eine nebensächliche Rolle, so dass diese erst in Teil E. dieser Arbeit beschrieben werden.

II. DAS BIOMETRISCHE VERFAHREN IM ALLGEMEINEN

Es gibt zwei verschiedene Arten der biometrischen Erkennung: die Verifikation, d.h. es erfolgt ein 1:1 - Abgleich (Bestätigung der Identität), und die Identifikation, also die Feststellung der Identität durch einen 1:n-Abgleich.

Im Groben erfolgt jedes biometrische Verfahren gleich. Zunächst wird das Merkmal erfasst (Enrolement) und, sofern es im Offline-Verfahren bspw. auf Papier aufge-nommen wurde, digitalisiert. Die Erfassung kann passiv (bspw. durch Vorbeigehen) oder aktiv (durch Mitwirkung des Betroffenen) geschehen.[14] Am besten wäre es, wenn die Erfassung von geschultem Personal durchgeführt wird, welches die Quali-tät beurteilen kann und anschließend gleich einen Probedurchlauf startet.[15] Aus den Rohdaten werden dann die markanten Merkmale extrahiert und als Template, als

[13] Petermann/Sauter, TAB Nr. 76, S. 63.
[14] BSI, BioFinger, S. 6.
[15] TeleTrust, Kriterienkatalog, S. 29.

Bilddatei oder als ein durch Umwandlung mittels eines kryptographischen Schlüssels erzeugter Datensatz (anonyme Biometrie) gespeichert.[16]

Zur Begriffserklärung:

- Rohdaten sind die unmittelbar aufgenommene Daten.
- Bilddaten sind behandelte Datensätze (zur Verbesserung des Bildes etc.) des vollständigen Abbilds des aufgenommenen Merkmals.
- Templates sind die aus einem Datensatz mittels eines Algorithmus hergestellten Daten.[17]

Die Speicherung erfolgt entweder zentral in einer Datenbank oder dezentral wie bspw. in einem Chip. Beim Vergleich oder der Identifikation wird das Merkmal des Betroffenen erneut aufgenommen und mit dem bereits gespeicherten Merkmal verglichen (Matching).

Bei der Verwendung biometrischer Daten sollten theoretisch diejenigen Merkmale und Systeme ausgewählt werden, welche für die jeweilige Situation am besten geeignet sind. Dabei wären v.a. folgende Kriterien nach Jain et al.[18] zu berücksichtigen:

- Universalität, d.h. das Merkmal muss bei jeder Person vorhanden sein,
- Einmaligkeit, d.h. es darf nicht mehr als eine Person mit diesem Merkmal existieren,
- Erfassbarkeit, d.h. das Merkmal ist biometrisch erfassbar,
- Beständigkeit, d.h. keine zeitliche Veränderung.[19]

---

[16] Münch, S. 295.
[17] S. auch Hornung, S. 78 f.
[18] Jain et al., in: IEEE Transactions on circuits and systems for video technology, 01/2004, S. 4.
[19] BSI, BioFinger, S. 8.

Im Laufe der Zeit haben sich weitere Kriterien ausgeformt, welche ebenfalls zur besseren Verwendung biometrischer Daten beitragen:

- Datenschutzfreundlichkeit;[20]
- Leistungsfähigkeit des System, d.h. das System muss entsprechend schnell und genau sein und eine gewisse Robustheit besitzen;
- Akzeptanz des Systems, d.h. das System muss allgemein akzeptiert und angewendet werden, ansonsten dann fallen die Fehlerraten oft höher aus. Die Akzeptanz kann durch transparente und einfache Verfahren erreicht werden, welche auch das Hygienebedürfnis des Menschen berücksichtigen;
- Überwindungssicherheit des Systems;
- Ökonomische Machbarkeit, d.h. die Kosten müssen verhältnismäßig sein;
- Benutzbarkeit, Verwendbarkeit, Zuverlässigkeit und Zweckmäßigkeit aus technischer und organisatorischer Sicht.[21]

Oftmals werden biometrische Merkmale miteinander kombiniert oder in Verbindung mit einem Ausweis oder Passwort verwendet.

Grundsätzlich ist ein biometrisches Merkmal einzigartig und kann einem bestimmten Menschen zugeordnet werden. Allerdings besteht natürlich durch das Aufnahmeverfahren bzw. durch die zeitlichen Abstände die Gefahr von geringfügigen Veränderungen der biometrischen Merkmale. Ein System kann daher niemals so konfiguriert werden, dass eine hundertprozentige Übereinstimmung begründet wird. Aus diesem Grund wird nur auf

[20] Münch, S. 300.
[21] BSI, BioFinger, S. 8.

„hinreichende Ähnlichkeit“, aber niemals auf Gleichheit getestet.[22] Das System ermittelt beim Vergleich einen sog. Matching-Score, welcher das Maß der Übereinstimmung ausdrückt. Bei jedem biometrischen System wird ein Toleranzbereich eingebaut, in dessen Bereich der Matching-Score liegen muss. In diesem Fall meldet das System dann eine Übereinstimmung, also ein „Match“ (engl. „gleich, übereinstimmen“). Liegt der Matching-Score dagegen nicht in diesem Toleranzbereich, liegt ein „Non-Match“ vor. Der Toleranzbereich wird bei jedem System voreingestellt. Wird der Toleranzbereich zu eng gehalten, ergibt dies eine hohe Falschzurückweisungsrate (false rejection rate = FRR); ist er zu weit, ist die Falschakzeptanzrate (false acceptance rate = FAR) zu hoch. Wenn die Falschakzeptanzrate gleich der Falschzurückweisungsrate ist, bezeichnet man dies als Gleichfehlerrate (equal error rate = EER). Das System ist qualitativ gut, wenn die EER niedrig gehalten ist.[23] Allerdings muss man bei der Einstellung des Toleranzbereiches beachten, wofür das biometrische Verfahren genutzt wird. Dient dieses der Zugangsbegrenzung im Sicherheitsbereich, ist es sinnvoll, die FAR zu minimieren. Dient das biometrische System dagegen nur als Passwortersatz für den Privatanwender, bspw. am PC, wäre es sicherlich zweckmäßiger, die FRR zu minimieren und damit die Zugangsvoraussetzung etwas zu erleichtern. Das System gilt überdies als sicher, wenn in den Augen eines potentiellen Angreifers der Aufwand den möglichen Ertrag übersteigen würde.[24]

Des Weiteren gibt es natürlich noch Personen, deren biometrische Daten aufgrund Nicht-Vorhandensein bzw. Abschwächung nicht

[22] Vgl. BSI, Grundsätzliche Funktionsweise biometrischer Verfahren, s. unter https://www.bsi.bund.de/ContentBSI/Themen/Biometrie/AllgemeineEinfuehrung/einfuehrung.html.
[23] Münch, S. 296 f.
[24] Meuth, S. 30.

erfasst werden können. Dies wird in einer False Enrolement Rate (FER) angezeigt, d.h. dem Anteil der Bevölkerung, der nicht erfasst werden kann. Nach Einschätzung von Experten liegt dieser Anteil bei ca. 2-5 % der Bevölkerung.[25]

B. GESICHTSGEOMETRIE

Trotz der Tatsache, dass die Gesichtserkennung nicht so alt ist wie die Daktyloskopie, wird diese derzeit häufiger eingesetzt als andere Verfahren. Dies liegt nicht nur an der einfachen Merkmalserfassung, sondern auch daran, dass die Akzeptanz der Bevölkerung höher ist, da bei der Gesichtserkennung nicht viel mehr Merkmale bekanntgegeben werden, als es der Mensch durch seinen Aufenthalt in der Öffentlichkeit ohnehin schon macht.

I. VERFAHREN

Die Stabilität der Gesichtserkennung wird ab einem Alter von 12-14 Jahren voraus-gesetzt, d.h. ab diesem Zeitpunkt verändert sich das Gesicht nur noch geringfügig.[26]

Die Gesichtsgeometrie wird mittlerweile in zwei Dimensionen angewandt, zum einen in der 2D- und zum anderen in der 3D-Version. In Ausweisen wird derzeit die 2D-Erkennung angewandt.

[25] Meuth, S. 29.
[26] Petermann/Scherz/Sauter, TAB Nr. 93, S. 65.

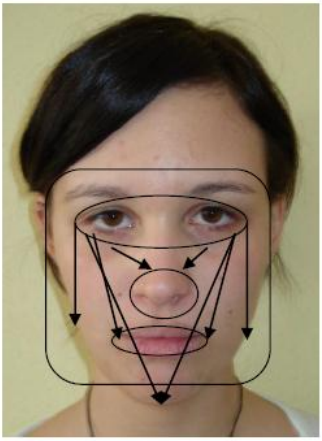


Abb. 1: 2D-Gesichtserkennung

Für die 2D-Gesichtserkennung erfasst eine Kamera zweidimensionale Bilder des Gesichts. Von den Augen ausgehend werden alle weiteren besonderen Merkmale wie Nase, Seitenpartien des Mundes und Knochengerüst geometrisch vermessen und ggf. in Bezug zueinander gesetzt. Diese Merkmale lassen sich nicht oder nur sehr geringfügig durch Mimik verändern, so dass insbesondere ihre Stellung zueinander sehr aussagekräftig ist.[27]

Die Messdaten können dann mittels eines Algorithmus in ein Template umgewandelt werden, was allerdings derzeit noch nicht häufig angewandt wird.

Bei der Gesichtserkennung sind einige Kriterien zu berücksichtigen: ausreichende Ausfüllung des Gesichtes (70%),

[27] BSI, Gesichtserkennung, s. unter https://www.bsi.bund.de/DE/Themen/Biometrie/BiometrischeVerfahren/Gesichtserkennung/gesichtserkennung_node.html.

Bildschärfe, Kontrastverhältnis, neutrale Mimik, Ausleuchtung, keine Verdeckung des Gesichts. Die Kriterien sind jedoch nur schwer einzuhalten, insbesondere beim Matching.[28]

Die 3D-Gesichtserkennung ist hingegen noch in der Entwicklungsphase.[29] Es gibt Bestrebungen zur Verwendung von Tiefenbildern, d.h. jeder Punkt repräsentiert einen bestimmten Wert, welcher den Abstand zwischen Punkt und Bildebene beschreibt. Dazu sind jedoch eine Rundum-Ansicht und damit auch mehrere Bild-Aufnahmen erforderlich.[30] Nachdem alle Aufnahmen zusammengebracht wurden, muss das Bild in eine bestimmte Position gebracht werden. Ausgangspunkt ist hierfür überwiegend die Nasenspitze, da diese meist auf der Symmetrieachse des Gesichts liegt. Erst dann kann ein Merkmalsvergleich erfolgen.[31]

II. ÜBERSCHÜSSIGE INFORMATIONEN UND PROBLEMFELDER

Da das Gesicht meist als Rohdatum verarbeitet wird, d.h. das Datum wird nicht durch einen Algorithmus in einen Datensatz umgewandelt, sind daraus viele Informationen ablesbar. Am Gesicht kann man erkennen, ob eine Person am Down-Syndrom, auch Trisomie 21, (Merkmale: kleiner Kopf, kleiner Augenabstand, kurzes Nasenbein) oder einer Gesichtslähmung leidet. Des Weiteren können aufgrund der Verwendung von Rohdaten Lebererkrankungen (Merkmal: gelbe Haut), die ethnische

[28] Schaar, Biometrie und Datenschutz, S. 40.
[29] Schaar, Biometrie und Datenschutz, S. 44.
[30] Otten, S. 26.
[31] Otten, S. 29 f.

Herkunft (Hautfarbe) oder gar die Religionszugehörigkeit (Kopftuch) erkannt werden.[32]

Überdies ist unklar, ob das derzeitige Gesichtserkennungsverfahren überhaupt ausreicht. Gerade im Zeitalter der Schönheitschirurgie kann es sein, dass Gesichter oftmals sehr stark verändert werden können. Eine komplette Gesichtstransplantation wurde bereits erfolgreich im Herbst 2005 in Frankreich durchgeführt.[33] Einer Falscherkennung könnte man hier durch die Verwendung eines 3D-Verfahrens entgegenwirken, da dabei deutlich mehr Daten erfasst werden. Hierzu gehört bspw. der Knochenbau, insbesondere die Krümmung der Stirn, welche sich auch im Alter kaum verändert.

Da die Systeme derzeit noch nicht ausgereift sind, reicht es für die Verwirrung des Systems bisweilen schon, wenn eine Person eine Brille oder einen Hut trägt oder die Beleuchtung falsch eingerichtet ist. Gerade Letzeres kann die Gesichtserkennung stark beeinflussen. Demnach fällt die Erkennungsleistung rapide, sofern das Licht von der Seite kommt, während Licht aus dem Hintergrund die Erkennungsleistung nur geringfügig abfallen lässt.[34] Aus diesem Grund sollten stabile Lichtverhältnisse bei der Aufnahme geschaffen werden.[35] Auch ein Lächeln oder ein Bart kann das System bereits zu einer Ablehnung der Person veranlassen.

C. FINGERABDRUCK

Das Verfahren zur Erkennung von Fingerabdrücken (Daktyloskopie, griech. „Fingerschau“) wurde bereits 1877 von

[32] Meints, Folien 26 ff.
[33] Schaar, Biometrie und Datenschutz, S. 45.
[34] Siehe BSI, BioP I, S. 10.
[35] So das Ergebnis von BSI, BioP I, S. 91.

William Herschel bei der Gehaltsauszahlung eingesetzt. Kurze Zeit später versuchte Sir Henry Faulds, die Daktyloskopie im Rahmen der Strafverfolgung zum Einsatz zu bringen. Doch erst Fancis Galton hat Ende des 19. Jahrhunderters die wissenschaftliche Begründung dafür geliefert, indem er auf die Unveränderlichkeit und Einzigartigkeit hinwies.[36] Der europäische Polizeikongress beschloss schließlich im Jahr 1914 die europaweite Verwendung der Daktyloskopie.[37] Im Jahr 1952 hat der Bundesgerichtshof den Beweiswert der Daktyloskopie anerkannt.[38]

I. VERFAHREN

Das Fingerabdruckverfahren ist hinsichtlich der Erkennungsleistung sehr stabil, da die Papillarlinien bereits im dritten Schwangerschaftsmonat ausgereift sind.[39] Änderungen können somit nur durch Verletzungen etc. (vgl. Pkt. II.) auftreten.

Entscheidend für die Erkennung des Fingerabdrucks sind der Verlauf der Papillarlinien sowie einzelne kleine Merkmale (Minutien), wie bspw. Gabelungen oder Kreuzungen.

Beim Fingerabdruck wird zunächst entweder durch ein Offline-Verfahren (z.B. auf Papier) oder per Online-Verfahren (z.B. durch einen Sensor) ein Bild des Fingerabdrucks erzeugt. Dabei entsteht ein Bild in verschiedenen Graustufen, welches die Papillarlinien zeigt. Verwendet man das Offline-Verfahren, muss der Fingerabdruck vor der weiteren Bearbeitung erst noch per Kamera oder Scanner digitalisiert werden. Dadurch ist ein Verlust von Daten bzgl. der Tiefe der Papillarlinien und Temperatur möglich. Ein weiterer Nachteil des Offline-Verfahrens liegt darin, dass durch

[36] Siehe Meuth, S. 33.
[37] Siehe Hamann, S. 24.
[38] BGH-Urteil vom 11.06.1952, 3 StR 229/52.
[39] Siehe Schubert, „Verräterische Rillen“, in: tagesspiegel.de, Bericht vom 08.05.2007.

das Abrollen eine Verzerrung möglich ist. Allerdings ermöglicht dies wiederum eine größere Oberfläche.[40] Beim Online-Verfahren (Live-Scan) gibt es mittlerweile mehrere Methoden, u.a. optische, thermische, Infrarot-, Ultraschall- oder Druck-Verfahren.

Bei dem Bild handelt es sich zunächst noch um ein Rohdatum. In einem Bildbearbeitungsprogramm wird der Finger so verändert, dass die Papillarlinien deutlicher hervortreten.

Danach wird der Finger klassifiziert, d.h. grob in eine der drei Hauptfingerklassen eingeordnet. Die Grundlagen der Klassifizierung wurden von dem englischen Anthropologen Sir Francis Galton geschaffen. Später hat der englische Scotland Yard-Präsident Edward Henry diese Methode weiterentwickelt; die heutige Klassifizierung beruht auf seinen Erkenntnissen.[41] Eine solche Klassifizierung erfolgt aufgrund der Vielzahl der Vergleichsdaten jedoch nur in den Informationssystemen, nicht aber in Zutrittssystemen, d.h. im Ausweis ist eine Klassifizierung nicht erforderlich.

Für die Klassifizierung wird allein der innere Bereich des Abdrucks benötigt, welcher durch Linien (sog. type lines) begrenzt wird.

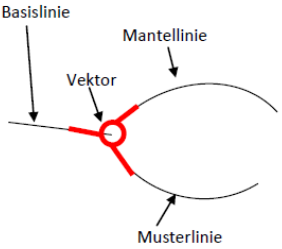


Abb. 2a: Umgrenzung des Deltas

[40] Siehe BSI, BioFinger, S. 11.
[41] Siehe Adlbrecht, S. 5.

Der innere Bereich wird v.a. durch seinen Kern (Delta) bestimmt. Nach dem Klassifizierungssystem von Henry gibt es demnach folgende drei Kategorien:

- Schleife (engl. Loop) -> ein Delta
- Wirbel (engl. Whorl) -> zwei oder mehr Deltas
- Bogen (engl. Arch) -> kein Delta[42]

Abb. 3a: Klassifizierung des Fingerabdrucks (Quelle: LKA Bayern)

1892 wurde anhand dieser Klassifizierung erstmals ein Mord aufgeklärt.[43]

In der Daktyloskopie gibt es zwei verschiedene Verfahren: das mikroskopische Verfahren, d.h. die Analyse der Minutien (lat. „Kleinigkeiten"), sowie das makroskopische Verfahren (pattern matching), d.h. zum Vergleich wird der komplette Fingerabdruck samt der eingezeichneten Minutien als Vergleichsdatum herangezogen. Letzteres erhöht aufgrund dem Mehr an Informationen die Erkennungsleistung, dauert in der Anwendung jedoch länger.[44]

[42] Siehe BSI, BioFinger, S. 13 ff.
[43] Mehr dazu in Hamann, S. 19.
[44] Siehe auch Petermann/Scherz/Sauter, TAB Nr. 93, S. 57.

Bei der Minutienanalyse werden nach der Klassifizierung die einzelnen Minutien nach Art, Lage und Richtung erfasst. Ein Vektor kennzeichnet dabei die Richtung, während ein Kreis das Muster festsetzt. Durch die Verwendung eines Algorithmus werden die Kennzeichnungen in einen Datensatz übersetzt, sog. Template.[45]

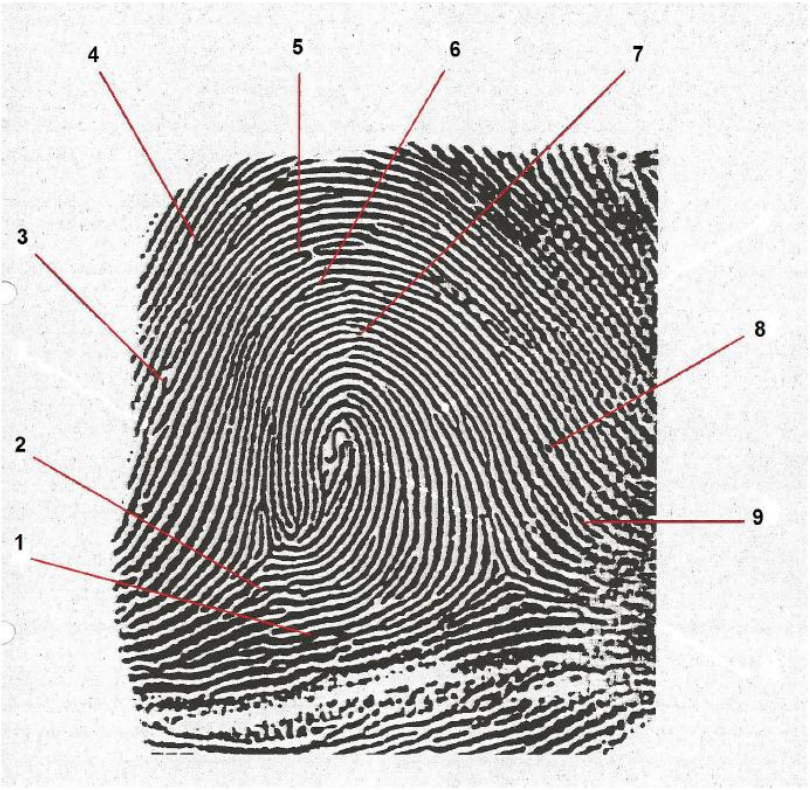
Abb. 3b: Analyse des Fingerabdrucks anhand des AFIS (Quelle: LKA Bayern)

Dieser Datensatz wird dann in dem Medium bzw. im System gespeichert und kann zum Abgleich herangezogen werden. Für den Abgleich sind aber nicht nur die Minutien von Bedeutung, sondern auch deren Art. Dabei gibt es unterschiedliche Arten:

- Papillarlinienende

[45] Mündliche Auskunft LKA Bayern vom 02.03.2009.

- Gabelung
- Berührungen von Linien
- Haken
- Punkt
- X-Linie
- Brücken, etc.



1 = Linienverästelung	4 = Gabelung	7 = Linienende
2 = Auge	5 = eingelagerte Schleife	8 = Punkt
3 = Haken	6 = Insel	9 = eingelagerte Linie

Abb. 4: Anatomische Merkmale (Minutien) des Fingers (Quelle: LKA Bayern)

Anhand dieser Auflistung erkennt man, wie vielseitig der Fingerabdruck ist. Nicht jedes der Merkmale kommt bei jedem Menschen vor. Dadurch wird eine enorme Vielfalt gewährleistet.

Die Identität zweier Fingerabdrücke ist sichergestellt, wenn zwei Fingerabdrücke zur gleichen Kategorie gehören, die Minutien nach ihrer Art übereinstimmen (qualitativer Faktor) und sich eine bestimmte Anzahl von Punkten überschneiden (quantitativer Faktor). [46] In Deutschland gilt der numerische Standard, d.h. es müssen derzeit acht Merkmale sowie das Grundmuster übereinstimmen. Stimmt das Grundmuster nicht, so müssen zwölf Merkmale einander entsprechen.[47]

Im Bereich der Forensik erfolgt dann noch eine Berechtigungsabfrage, d.h. alle diejenigen Personen, welche rechtmäßig am Tatort sein dürfen (Mieter, etc.), müssen ihre Fingerabdrücke abgeben, um die aufgefundenen Abdrücke zu sondieren. Die Überprüfung geschieht mittels eines Direktvergleichs unter der Lupe und nicht im System.[48]

II. ÜBERSCHÜSSIGE INFORMATIONEN UND PROBLEMFELDER

Beim Fingerabdruck können in den Rohdaten viele überschüssige Informationen über den Gesundheitszustand enthalten sein. U.a. kann man Hauterkrankungen wie bspw. Ekzeme erkennen. Nach einer US-Studie ist am Fingerabdruck des Kindes auch der Ernährungszustand der Mutter in den ersten drei Schwangerschaftsmonaten erkennbar. Eine schlechte Ernährung wirkt sich auf die Wahrscheinlichkeit aus, an Diabetes zu erkranken. Eine solche Wahrscheinlichkeit ist durch den

[46] Siehe BSI, BioFinger, S. 16 f.
[47] Mündliche Auskunft LKA Bayern vom 02.03.2009.
[48] Mündliche Auskunft LKA Bayern vom 02.03.2009.

Fingerabdruck erkennbar.[49] Außerdem ist in bestimmten Fällen die geographische Herkunft zu ermitteln; dies ist bspw. bei Personen asiatischer Herkunft der Fall.

Durch Schweiß, Veränderungen der Position oder Hautveränderungen können vielfach Messfehler auftreten. Gerade Hautveränderungen werden des Öfteren bei Senioren sowie Personen, welche viel körperliche Arbeit leisten, der Fall sein, da hier oft Schwielen oder Abnutzungen an den Fingern auftreten. Auch bei Verbrennungen oder Vernarbungen, bspw. durch die Arbeit mit toxischen Mitteln, fällt die Erkennungsleistung merklich ab[50], insbesondere wenn die untere Hautschicht betroffen ist.

Kleine Frauen asiatischer Herkunft bergen ebenfalls die Gefahr hoher Fehlerraten, da bei diesen die Minutien nicht in der Weise ausgeprägt sind, wie dies bspw. bei Europäern der Fall ist.[51]

Zudem wurde bereits vom Chaos Computer Club unter Beweis gestellt, wie einfach ein Fingerabdruck zu kopieren ist. Die Gruppe hat einen Fingerabdruck allein durch Zuhilfenahme von Sekundenkleber, einem Flaschenverschluss, einer Digitalkamera, einem Drucker und Holzleim hergestellt, diesen auf einen anderen Finger aufgesetzt und bei einem der Lesegeräte eingesetzt. Ein herkömmlicher Fingerabdruck-Scanner konnte damit überlistet werden.[52] Das Gleiche hat bereits ein japanischer Mathematiker mithilfe von Gummibärchenfingern geschafft.[53] Vorteil des

[49] Siehe Focus-Bericht vom 05.12.05, „Diabetes Typ 1 – Fingerabdruck zeigt Zuckerrisiko".
[50] Siehe Petermann/Scherz/Sauter, TAB Nr. 93, S. 62.
[51] Siehe Spiegel-Online vom 28.02.04, „Biometrie-Pannen. Die Probleme kleiner asiatischer Frauen".
[52] Siehe CCC vom 09.10.2004, „Wie können Fingerabdrücke nachgebildet werden?".
[53] Siehe dazu Winkels, Vortrag v. Oktober 2004; Der Mathematiker Tsutomu Matsumoto presste seinen Finger in einem Silikonball, den er aus aufgewärmten Silikonkügelchen hergestellt hatte. In die abgekühlte Form goss er dann Gummibärchen-Gelatine. Nach kurzer Kühlung konnte er den Abdruck herauslösen.

Gummibärchenfingers war nicht nur, dass man den durchsichtigen Abdruck auf dem Finger nicht erkennen kann, sondern auch, dass sämtliche Beweismittel sofort vernichtbar sind. Ein weiterer Angriffspunkt sind die Rückstände eines Abdrucks auf dem Sensor, wobei der Abdruck durch einfaches Anhauchen reaktiviert werden konnte. Die damaligen Redakteure der Computerzeitschrift c't testeten weitere Techniken und fanden heraus, dass man den Sensor nur mit Graphitpuder bestäuben, eine Klebefolie darüber legen und leichten Druck auf den Sensor ausüben musste (Latenzfingerabdruck, s. Pkt. A. I.). Der Sensor reagierte – und ließ sich täuschen.[54]

Dennoch schneidet der Fingerabdruck als biometrisches Merkmal aufgrund seiner einfachen Erfassbarkeit und relativen Sicherheit am besten ab. Die Sicherheit könnte man noch erhöhen, indem man – insbesondere bei Ausweisen – den Daumenabdruck als Erkennungsmerkmal nutzt, da bei diesem eine größere Anzahl an auswertbaren Merkmalen vorhanden ist.[55]

Durch eine Lebenderkennung kann zudem vermieden werden, dass ein toter Finger oder Fingeraufsätze verwendet werden. Für diese Form der Erkennung dienen bspw. Schweißdetektoren, Pulsmessgeräte, Wärmefühler oder künstliche Nasen.

Durch die hohe Feuchtigkeit der Gelatine überlistete der Gummifinger auch solche Systeme, die ein Silikonfinger nicht schaffte.

[54] Siehe Thalheim/Krissler/Ziegler, in: c't 11/2002, S. 114 ff.

[55] Siehe BSI, BioP II, S. 16 f.

D. DNA

Die DNA-Analyse wurde im Jahre 1984 von Alec Jeffreys, Professor der Universität von Leicester in Großbritannien, entwickelt. Schon ein Jahr nach der Entdeckung konnte damit ein Mörder gefasst werden. Dennoch entschied der Bundesgerichtshof Anfang der 90er Jahre noch, dass die DNA-Methode keineswegs unumstritten und als alleiniger Beweis nicht ausreichend für eine Verurteilung sei.[56] Dass die Methode auch in den USA keineswegs unstreitig war, konnte man anhand des Falles O. J. Simpson erkennen. Die Verteidiger plädierten darauf, dass die Indizien bedeutungslos und Ergebnis eines Komplotts seien. Tatsächlich hatte es des Öfteren Sachverständige gegeben, welche die DNA-Analysen manipuliert hatten, u.a. auch der Chefserologe des Kriminallabors der West Virginia State Police.[57]

Nicht nur die Gesetze zur DNA-Analyse gaben Anlass zu Diskussionen; auch so manche Zukunftsvisionen lösten heftige Debatten aus. So forderte bspw. der Londoner Polizeichef Peter Imbert 1992 die Einführung einer landesweiten DNA-Erhebung aller männlichen Personen zur schnelleren Aufklärung von Sexualverbrechen.[58] Der ehemalige hessische Innenminister Volker Bouffier (CDU) forderte, die DNA bereits bei der Geburt zu erheben und den Code bei den Ermittlungsbehörden zu speichern, um organisierte Laden- und Handtaschendiebstählen durch Kinderbanden einfacher aufzuklären zu können.[59]

---

[56] BGH, Urteil vom 12.08.1992, 5 StR 239/92, in: BGHSt 38, 320; siehe auch Herb, S. 3.
[57] Siehe Nogala, in: CILIP 61.
[58] Siehe Nogala, in: CILIP 61.
[59] Lorscheid, „Kinder-DNA-Datei für «Klau-Kids»“, Bericht bei telepolis vom 09.01.2004.

I. GESETZLICHE REGELUNGEN ZUR DURCHFÜHRUNG DER DNA-ANALYSE IN DER BUNDESREPUBLIK DEUTSCHLAND

1. GESETZLICHE ENTWICKLUNGEN IN BEZUG AUF DIE DNA-ANALYSE

Seit dem Jahr 1990 werden bei den Polizeibehörden DNA-Spuren verwertet. Da es zur Erhebung und Verarbeitung solcher Daten bisher noch keine gesetzliche Grundlage gab, wurde mit dem *Strafverfahrensänderungsgesetz – DNA-Analyse (StVÄG) vom 17.03.1997*[60] in den heutigen §§ 81a III, 81c V S. 2, 81e und 81f StPO eine Rechtsgrundlage geschaffen, worin die Durchführung der DNA-Analyse geregelt wurde.

Aufgrund zahlreicher Fälle mit Sexualbezug im Jahre 1998 wurde zusätzlich das DNA-Identitätsfeststellungsgesetz (DNA-IFG) vom 07.09.1998[61] geschaffen, um DNA sowohl für Altfälle (Retrograd-Erfassung) als auch für künftige Verfahren (Vorwärts-Erfassung) zu speichern. Dies beinhaltete die Einführung des § 81g StPO. Die Einführung dieser Gesetze verursachte jedoch zahlreiche Probleme, da § 81g StPO bzw. § 2 DNA-IFG zu ungenau gefasst wurden.[62]

Daraufhin wurde das *Gesetz zur Änderung des DNA-Identitätsfeststellungsgesetz* vom 02.06.1999[63] erlassen. Jedoch erst Art. 10 des *Gesetzes zur Änderung und Ergänzung des*

[60] BGBl. I 1997, Nr. 18, S. 534 f.
[61] *„Gesetz zur Änderung der Strafprozessordnung (DNA-Identitätsfeststellungsgesetz)"*, BGBl. I 1998, Nr. 61, S. 2646 f.
[62] Siehe Graalmann-Scheerer, „Entwicklung und Tendenzen der molekulargenetischen Untersuchung im Strafverfahren", in: Sokol, Der gläserne Mensch, S. 39 [40 f.] mwN.
[63] BGBl. I 1999, Nr. 29, S. 1242 f.

Strafverfahrensrechts 1999 (StVÄG 1999) vom 02.08.2000[64] hat die vorhandenen Probleme hinreichend beseitigt.[65]

Weitere Änderungen ergaben sich mit dem *Gesetz zur Änderung der Strafprozessordnung* vom 06.08.2002[66] sowie mit dem *Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften* vom 27.03.2003[67].

Mit Einführung des *Gesetzes zur Novellierung der DNA-Analyse (DNA-Gesetz)* vom 12.08.2005[68] sind sowohl das DNA-IFG als auch sämtliche vorherigen Änderungen hinfällig geworden, vgl. Art. 4 DNA-Gesetz. Einzig die Änderungen des StVÄG 1997 –mit Ausnahme des § 81f StPO – sowie die Änderung des § 81e I S. 1, 2. HS durch das letzte Änderungsgesetz vom 27.03.2003 genossen noch Geltung, da diese durch das DNA-Gesetz nicht berührt wurden. Mit der Einführung des DNA-Gesetzes wurden zahlreiche Änderungen vorgenommen. Zum einen wurde der Richtervorbehalt für Spurenmaterial gestrichen und zum anderen wurde ein Einwilligungsvorbehalt für den Betroffenen in Bezug auf Personendaten eingeführt. Bei den Anlasstaten zur Speicherung der Daten in der DNA-Datei wurden die Anforderungen herabgesetzt, d.h. zur Speicherung reicht bereits die wiederholte Begehung irgendeiner Straftat aus. Das letztgenannte Kriterium reicht auch für die Negativprognose, d.h. für die Speicherung ist es zukünftig hinreichend, wenn prognostiziert werden kann, dass der Betroffene irgendwann wieder eine Straftat begeht. So reicht es schon aus, wenn eine Person bereits wegen Ladendiebstahls

---

64 BGBl. I 2000, Nr. 38, S. 1253 ff.
65 Siehe Graalmann-Scheerer, „Entwicklung und Tendenzen der molekulargenetischen Untersuchung im Strafverfahren", in: Sokol, Der gläserne Mensch, S. 39 [41].
66 BGBl. I 2002, Nr. 56, S. 3018 f.
67 BGBl. I 2003, Nr. 67, S. 3007 ff.
68 BGBl. I 2005, Nr. 49, S. 2360 ff.

bekannt ist und nun nochmals ein Vergehen begeht, indem sie bspw. eine Zahnbürste für zwei Euro stiehlt. Allein diesbezüglich erscheint die Verhältnismäßigkeit sehr fraglich. Eine diesbezügliche Prüfung bleibt jedoch anderen Arbeiten vorbehalten.

Im Übrigen wurde nun auch der Reihengentest gesetzlich festgeschrieben.

Heute dürfte die Diskussion um die Entnahme von DNA-Zellen ihre Schärfe verloren haben. Die Gesetze sind nun wesentlich präziser gefasst und letztlich führt eine DNA-Untersuchung nicht nur zur Überführung des Täters, sondern dient in vielen Fällen auch zum Beweis der Unschuld. So wurde im Rahmen einer Studie des amerikanischen Justizministeriums festgestellt, dass in 28 dokumentierten Fällen die Unschuld jener Täter, welche bereits zu Tode bzw. zu lebenslanger Haft verurteilt waren, durch nachträgliche DNA-Tests bewiesen werden konnte.[69]

2. ÜBERBLICK ÜBER DIE AKTUELLE GESETZESLAGE

Die molekulargenetische Untersuchung ist heute in den §§ 81e ff. StPO geregelt.

§ 81e StPO regelt die molekulargenetische Untersuchung in anhängigen Verfahren. Für die Gewinnung der DNA sind allerdings § 81a und 81c StPO heranzuziehen, da in § 81e StPO nur die DNA-Analyse selbst geregelt ist. Somit ist nicht nur für die Gewinnung des Probenmaterials ein Richtervorbehalt vorgeschrieben, sondern auch für die Untersuchung des Materials (vgl. § 81f StPO). Zeitweise wurde die Streichung des Richtervorbehalts diskutiert, was jedoch wieder verworfen wurde. Eine DNA-Analyse kann nicht mit einem herkömmlichen

[69] Siehe Connors, E. et al.: Convicted by Juries, Exonerated by Science: Case Studies in the Use on DNA Evidence to Establish Innocence after Trial; Nogala, in: CILIP 61.

Fingerabdruck verglichen werden. Nicht ohne Grund hat das Bundesverfassungsgericht in mehreren Entscheidungen[70] festgehalten, dass die DNA-Analyse nur mit Blick auf die derzeitigen Voraussetzungen verfassungsmäßig ist, d.h. es muss eine Tat von erheblicher Bedeutung vorliegen, welche eine negative Prognose zulässt. An eine DNA-Analyse ohne richterliche Anordnung ist also nicht zu denken.[71]

§ 81e StPO teilt sich wiederum auf in die Analyse von Personen-DNA (Abs. 1) und in die von Spurenmaterial (Abs. 2).

§ 81g StPO regelt die DNA-Untersuchung zur Feststellung der Identität in künftigen Strafverfahren. In dieser Vorschrift ist nicht nur die genetische Untersuchung geregelt, sondern auch die Erhebung, also die Entnahme von Körperzellen. Da dieser Eingriff schwer wiegt, sind die Voraussetzungen auch strenger geregelt. Es bedarf einer Straftat von erheblicher Bedeutung bzw. der wiederholten Begehung und einer Negativprognose. Des Weiteren muss die Entnahme erforderlich und verhältnismäßig sein. Die Körperzellen sind nach § 81g II S.1 StPO sofort zu vernichten, wenn die Analyse abgeschlossen ist. Das aus den Zellen gewonnene Identifizierungsmuster wird gemäß den Bestimmungen des Bundeskriminalamtgesetzes (BKAG) in einer Datei gespeichert.

Zu beachten ist, dass auch die durch die nach § 81e StPO durchgeführte Untersuchung gewonnenen Identifizierungsmuster in der DNA-Datei gespeichert werden können, vgl. § 81g V StPO. Hierzu ist allerdings im Unterschied zu § 81g StPO die Benachrichtigung des Beschuldigten erforderlich. Des Weiteren steht dem Beschuldigten dann das Recht der richterlichen Überprüfung zu.

---

[70] Siehe u.a. BVerfG, Urteil vom 15.03.2001, 2 BvR 1841/00, in: NJW 2001, S. 2320 ff.; BVerfG, Urteil vom 12.03.2003, 1 BvR 330/96, in: NJW 2003, S. 1787 ff.

[71] Siehe Pressemitteilung (5/05) des Bundesbeauftragten für den Datenschutz, in: RDV 2/2005, S. 89.

II. DIE STRUKTUR DER DNA

Die DNA eines Menschen ist einzigartig und somit in der Erkennung präziser als die anderen biometrischen Merkmale. Aus diesem Grund liegt die Falscherkennungsrate annähernd bei Null.

Um die Bedeutung der DNA-Analyse erkennen zu können, muss man zunächst die Struktur der DNA verstehen:

Die menschliche Zelle besteht aus 23 Chromosomenpaaren. Paar Nr. 23 charakterisiert das Geschlecht. Jedes Chromosom enthält einen DNA-Doppelstrang. Dieser ist aufgereiht und verschlungen, so dass eine kompakte Hülle – das Chromosom – entsteht.

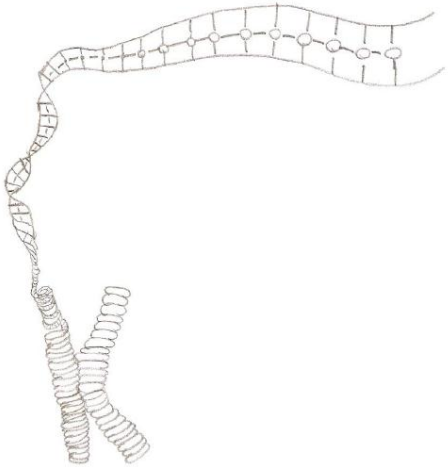


Abb. 5: Chromosom mit DNA-Doppelhelix
(in freier Bearbeitung nach Brodersen/Anslinger/Rolf, S. 94)

Die gegenüberliegenden Stränge der Doppelhelix sind komplementär zueinander und ergänzen sich jeweils. Ein solcher Strang besteht aus vielen Einzelteilen, den Nukleotiden. Diese setzen sich zusammen aus Phosphor und Desoxyribose (Zucker), welche den mittleren Teil der Doppelhelix bilden, sowie aus einer

der vier Basen Adenin, Guanin, Thymin und Cytosin. Da die Phosphor- und Zucker-Einheiten immer gleich sind, werden die Abkürzungen der Basen A, G, T und C auch als Bezeichnung für die Nukleotide verwendet, da diese letztlich für die Verschiedenartigkeit der Nukleotiden verantwortlich sind. In der Doppelhelix stehen sich immer zwei Basen gegenüber: Adenin und Thymin sowie Guanin und Cytosin.

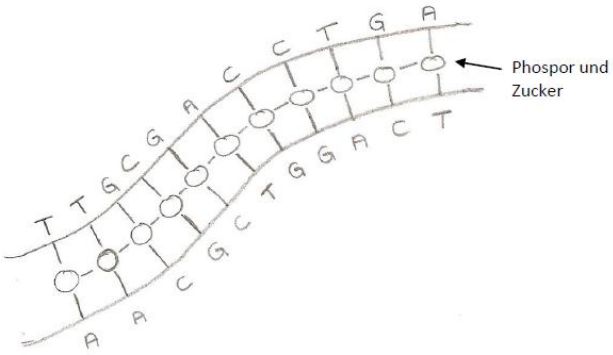


Abb. 6: Nukleotide

Die komplette Kern-DNA besteht aus ca. 3 Milliarden dieser Basenpaare. Nach heutiger Schätzung sind darin ca. 30.000 bis 50.000 Gene enthalten. Diese Gene liegen in codierten, informationstragenden DNA-Sequenzen, welche unsere Eigenschaften und unser Aussehen wiedergeben. Dieser Teil macht etwa 2-3 % der Gesamt-DNA aus.

Die Genabschnitte werden getrennt durch den nicht-codierten Teil, welcher die Basis für den biometrischen Vergleich bildet. Allein dieser Bereich wird in der Kriminaltechnik verwendet. Der nicht-codierte Teil der DNA ist nicht nur eines der zuverlässigsten

biometrischen Merkmale – die Abfolge dieses Teils tritt theoretisch nur ein Mal unter 450 Milliarden Menschen auf –, sondern auch an den meisten Tatorten aufzufinden. Einzig und allein bei eineiigen Zwillingen bzw. Mehrlingen ist die DNA auch im nicht-codierten Teil identisch.

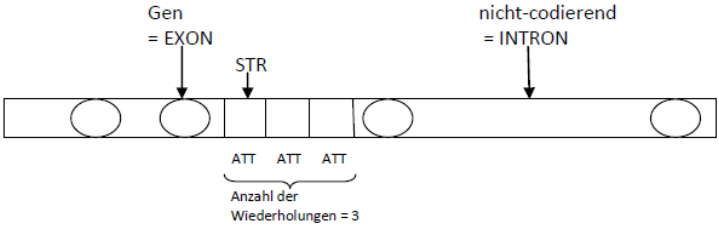


Abb. 7: Exons und Introns sowie die Darstellung der STR

Für die zuverlässige DNA-Ermittlung ist heutzutage nur ein geringer DNA-Bestand erforderlich. Dieser DNA-Bestand kann aus frischen Haarwurzeln, Schweiß, Hautschüppchen, weißen Blutkörperchen, Körpersekreten etc. gewonnen werden. Zum Teil reichen heutzutage sogar Kontaktspuren, also bspw. Spuren an Holzgriffen, aus, sofern ein intensiver Hautkontakt (Abschürfungen, etc.) bestand. Rote Blutkörperchen hingegen enthalten keine DNA und sind damit für die DNA-Analyse ungeeignet.[72]

[72] Committee of Ministers, Explanatory Memorandum zu Rec. (92) 1, Nr. 35.

III. VERMESSUNGSVERFAHREN[73]

Für die forensische Analyse werden jeweils kleine Abschnitte des nicht-codierten Teils untersucht. Seit 1992/93 arbeitet die Kriminaltechnik mit der VNTR (= variable number of tandem repeats)-Typisierung auf Basis der PCR-Methode (= polymerase chain reaction; engl. „biochemische Kettenreaktion"). Diese Methode ist nicht nur sicherer als die alte RFLP-Methode (Restriktionsfragmentlängen-Polymorphismus), sondern auch bei geringsten DNA-Mengen sowie bei sehr alten Spuren anwendbar.

Für die DNA-Analyse muss die DNA zunächst aus den Spuren extrahiert werden. Dies geschieht durch Enzyme und anschließende Zentrifugierung. Die dann vorliegende DNA ist der Ausgangspunkt für die nachfolgende Analyse.

Wie in Abb. 7 gezeigt, liegen zwischen den codierten Sequenzen (den sog. Exons) nicht-codierte Abschnitte (sog. Introns). Die anschließende VNTR-Typisierung basiert auf der Tatsache, dass sich auf der DNA in bestimmten Abschnitten kurze Sequenzen ständig wiederholen. Die Anzahl dieser Wiederholungen unterscheidet sich zwischen den Individuen. Diese Abschnitte sind die VNTRs und lassen sich entsprechend ihrer Länge in Minisatelliten (Länge von 15-50 Basen) und Mikrosatelliten (STRs = short tandem repeats) einteilen. In der Kriminaltechnik werden nur die STRs verwendet, welche aus einer Basenlänge von ca. zwei bis fünf sich wiederholenden Basen besteht. Gemäß der *Entschließung des Rates vom 30.11.09 über den Austausch von DNS-Analyseergebnissen*[74] bilden derzeit zwölf STRs den Europäischen Standardsatz (ESS): D21S11, VWA, D3S1358, D8S1179, D18S51, FGA,

---

[73] Siehe Berg/Tymoczko/Lubert, S. 92 ff., 162, 166 ff., 184 f.; Berufsschulzentrum Miesbach, DNA-Analyse, s. unter http://bsz-mb.berufsschulnetz.de/frauenschulstrasse/berufsoberschule/unterricht/faecher/biologie/genet_finger/dna-analyse.htm; Herb, S. 11 ff.

[74] ABl. C 296 vom 05.12.2009, S. 1 ff.

D1S1656, D2S441, D10S1248, D12S391 und D22S1045. Alle erwähnten STRs liegen auf unterschiedlichen Chromosomen und beschreiben ihre jeweilige Lage. Dementsprechend ergeben sich die Namen aus der Sequenz benachbarter Gene (bspw. VWF = Von-Willebrand-Faktor) bzw. aus genetischen Nomenklaturen (bspw. D18S51 = D18 für Chromosom 18, S51 für die Lage auf dem Chromosom).

Die Untersuchung von weniger als sieben STRs ist nicht ausreichend. So wurde im Jahr 2000 durch die Polizei in Großbritannien festgestellt, dass ein Unschuldiger wegen Raubs verurteilt wurde. Die DNA-Analyse erfolgte damals nur anhand von sechs Abschnitten. Sein handfestes Alibi rettete den Mann; es wurden daraufhin zehn Abschnitte untersucht, was den Mann schließlich entlastete[75].

Unterschiede ergeben sich durch die Anzahl der Wiederholungen der verschiedenen Sequenzen. Liegen bspw. 10 Wiederholungen einer Basenabfolge vor, spricht man vom Typ (auch Allel) 10. Da die gesamte Erbsubstanz zweimal, d.h. ein Chromosomensatz vom Vater und einer von der Mutter, vorhanden ist, liegen zwei Allele pro Person und pro STR vor. Im DNA-Identifizierungsmuster werden daher zwölf STRs mit je zwei Allelen erfasst; Allel 1 ist dabei immer nur das kleinere Allel.

SE 33		**D21S11**		**VWA**		**TH01**		**FIBRA**	
All. 1	All. 2	All. 1	All. 2	All. 1	All. 2	All. 1	All. 2	All. 1	All. 2
				20	12			26,2	20
D3S1358		**D8S1179**		**D18S51**		**Amel**			
All. 1	All. 2	All. 1	All. 2	All. 1	All. 2	All. 1	All. 2		
15	15								

Abb. 8: DNA-Identifizierungsmuster (Leerbogen mit Beispielen) (Quelle: LKA Bayern)

[75] Siehe Howard, in: Scoop, New Zealand News v. 10.02.2000.

Diese Unterschiede basieren im Besonderen auf evolutionsbedingten Mutationen im menschlichen Erbgut. Durch den Selektionsdruck haben sich die Gene im Laufe der Zeit angepasst und sämtliche Mutationen wurden immer wieder durch bessere Mutationen ersetzt. Im Gegensatz zum codierten Bereich bleiben jedoch im nicht-codierten Abschnitt alle Mutationen erhalten, da dieser Bereich nicht das Überleben des Organismus sichern muss. Durch diese Mutationen werden die genetischen Unterschiede deutlich erhöht.[76]

In der forensischen DNA-Analyse wird die PCR-Methode zur Fragmentlängenanalyse eingesetzt.

Ziel der PCR-Methode ist, die STRs künstlich zu vervielfältigen. Die Vervielfältigung erfolgt in drei Schritten: Schmelzen (Melting), Anlagern (Annealing), Verlängerung (Elongation). Zunächst wird die DNA-Doppelhelix mittels hoher Temperatur in zwei Einzelstränge aufgespalten (Melting). Anschließend wird die Temperatur wieder auf 50°C bis 65°C abgekühlt. Die daraufhin zugesetzten Primer (Startermoleküle), welche durch ihre komplementäre Zusammensetzung die Ziel-DNA bestimmen, setzen an den Enden der gewünschten DNA-Fragmente an (Annealing). Bei einer Temperatur von 72 °C wird die Ziel-Sequenz durch das Enzym Polymerase wieder zum Doppelstrang (Elongation).

[76] Siehe Zykla-Menhorn, in: Deutsches Ärzteblatt v. 28.01.2005.

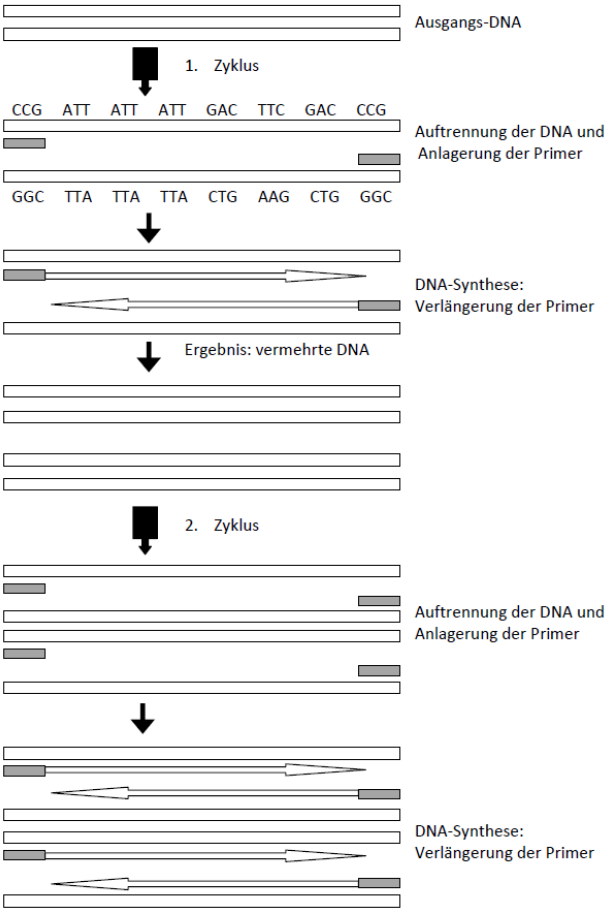


Abb. 9: Vereinfachte PCR-Technik (in freier Bearbeitung nach Berg/Tymoczko/Stryer, S. 167)

Die oben genannten Schritte werden etwa 32 Mal wiederholt, bis ausreichende DNA für eine Analyse vorhanden ist. Da die DNA-Sequenzen exponentiell vermehrt werden, sind nach der Vervielfältigung ca. 2 Milliarden Kopien der DNA-Sequenz vorhanden.

Zur weiteren Analyse bedient man sich der Elektrophorese. Vorher werden die Teilchen radioaktiv markiert. So können sie später in einer Autoradiographie betrachtet werden.

Die Apparatur ist mit einem Gelen gefüllt. In ein Startloch werden die vervielfältigten DNA-Fragmente gegeben. In ein anderes Startloch kommt ebenfalls eine Mischung von DNA-Fragmenten, deren Größe allerdings bekannt ist (Allel-Cocktail). Legt man nun Spannung an, wandern die negativ geladenen Teilchen von der Kathode zur Anode, welche sich am unteren Ende, d.h. am vertikalen Ende der Apparatur, befindet. Das Gelen wirkt dabei wie ein Filter; die kleinen Teilchen bewegen sich rascher durch das Gel, wodurch eine Aufteilung der Teilchen nach ihrer Größe bewirkt wird. Durch das Mitlaufen der bekannten Allele kann man nach Beendigung der Elektrophorese auf die unbekannten DNA-Abschnitte schließen, da gleiche Allele sich in derselben Höhe positionieren.

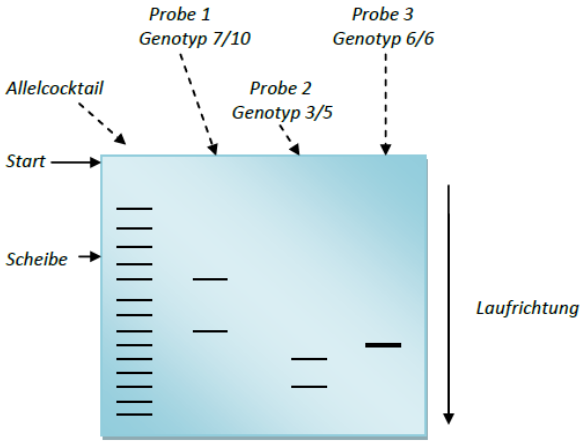


Abb. 10: Gelelektrophorese: Auftrennung der DNA-Fragmente (in freier Bearbeitung nach Brodersen/Anslinger/Rolf, S. 105)

Ist die Elektrophorese beendet, werden die Scheiben der Apparatur vorsichtig voneinander getrennt und das daran haftende Gelen wird mit Essigsäure begossen, um die DNA-Stücke zu fixieren. Anschließend wird auf die Glasplatte ein Filterpapier gelegt, welche das Gelen samt der DNA-Stücke aufnimmt. Nach Trocknung des Filterpapiers können die DNA-Stücke durch Autoradiographie sichtbar gemacht werden. Durch eine Längenmessung der DNA-Teile wird ein Zahlencode gewonnen, welcher das DNA-Identifizierungsmuster darstellt. Beim anschließenden Röntgenbild sind dann genau an den Stellen, an welchem sich die DNA-Stücke hybridisiert haben, radioaktive Färbungen zu erkennen.

Die vorangestellte Methode bildet die Grundlage zum Verständnis der heutigen DNA-Analyse, welche mittels der Kapillar-Elektrophorese durchgeführt wird. Bei dieser wird die DNA in eine Glaskapillare aufgezogen. Die Kapillaren sind ebenfalls mit einer gelartigen Masse gefüllt, durch welche dann die Elektrophorese erfolgt. Im Unterschied zur vorherigen Methode werden die Primer bereits in der PCR-Phase mit Fluoreszenzfarbstoffen (gelb, blau oder grün) markiert. Daneben wird ein mitlaufender Allel-Cocktail rot markiert. Bewegen sich dann die Fragmente zur Anode, wandern sie am Fenster eines Detektors vorbei, welcher die Farbstoffmoleküle durch einen Laserstrahl dazu anregt, zu fluoreszieren. Dadurch kann die Länge der DNA-Fragmente aufgrund der Zeit (oder der Wegstrecke) von dem Laser ermittelt und am Computer ausgewertet werden. Die sich ergebenden Werte werden anschließend mit den bekannten Allelen verglichen und den einzelnen STRs nach Markierung und Länge zugeordnet.

Der Vorteil der Kapillar-Elektrophorese liegt darin, dass bis zu viermal mehr Proben gleichzeitig untersucht werden können.[77]

Die Kosten sind mittlerweile verhältnismäßig gering. Die Analyse kann im Notfall innerhalb von wenigen Stunden durchgeführt werden.[78]

IV. PROBLEMFELDER UND AUSSAGESICHERHEIT DER ANALYSE

Man weiß, dass die DNA durch den codierten Teil Aufschluss über sensible Daten gibt. Der codierte Teil verrät nicht nur Einiges über unser Aussehen, sondern auch über unsere Gesundheit. Durch die DNA lassen sich auch Rückschlüsse auf familiäre Beziehungen erkennen, wodurch der Kreis des „Betroffenen" ausgedehnt wird. Des Weiteren ähnelt sich die DNA umso mehr, je näher Personen miteinander verwandt sind, so dass ggf. auch die Verwandtschaftsverhältnisse festgestellt werden können. Dies hätte Auswirkungen auf das Erfordernis des Einverständnisses, insbesondere bei der Einwilligung.

Allerdings ist die DNA-Analyse derzeit nur auf die Erkennung von Personen beschränkt. Durch § 81e I StPO wird eine Entschlüsselung von Genen per DNA-Analyse ausgeschlossen. Das einzige personenbezogene Merkmal, welches bei der DNA-Analyse zusätzlich untersucht wird, betrifft das Geschlecht. Hierzu wird nur Chromosom Nr. 23 untersucht. Allerdings treten bei Männern hier vermehrt Krankheiten, wie bspw. die Bluterkrankheit, die Rot-

[77] Vgl. zu diesem Absatz: Berufsschulzentrum Miesbach, DNA-Analyse, s. unter http://bsz-mb.berufsschulnetz.de/frauenschulstrasse/berufsoberschule/unterricht/faecher/biologie/genet_finger/dna-analyse.htm.

[78] Siehe Berns, S. 37; Mündliche Auskunft LKA Bayern vom 02.03.2009.

Grün-Blindheit und die Duchenne'sche Muskeldystrophie[79] sowie das Klinefelter Syndrom auf[80], welche durch die DNA-Analyse erkannt werden können.

Zur Bestimmung des Geschlechts wird ein Zahnschmelz-Protein herangezogen. Dieses ist sowohl auf dem X- als auch auf dem Y-Chromosom vorhanden und unterscheidet sich lediglich in der Basenlänge.[81]

Die Erkennung von Krankheiten wird durch die Gesetzesbegrenzung allerdings nicht eingeschränkt. In wenigen, aber doch denkbaren Fällen deutet ein bestimmtes Allel auf die Möglichkeit einer Erkrankung hin, insbesondere wenn das Allel neben dem die Krankheit ausweisenden Gen liegt.

Des Weiteren treten oft auch Fehler durch menschliches Versagen (Unkonzentriertheit, falsche Proben-Bezeichnung, Irreführende DNA-Muster) auf, d.h. es sind vom Ermittlungsbeamten über die Spurensicherung bis hin zum Labor Sicherheitsvorkehrungen erforderlich, um eine Kontamination der DNA zu vermeiden. Dementsprechend sind Handschuhe, Schutzanzüge sowie gereinigtes Labormaterial zu verwenden.[82] Aus diesem Grund wird zur Überführung eines Täters eine zweite Vergleichsprobe gefordert.

Oftmals kann es sein, dass in bestimmten DNA-Regionen des Körpers mehrere DNA-Stränge vorhanden sind, so z.B. im Knochenmark nach einer Spende[83], oder in der Mundschleimhaut

---

[79] Entwicklungsstörung der Muskeln, welche mit Muskelschwund einhergeht (Lexikon).
[80] Vgl. Wikipedia, „Chromosom", s. unter http://de.wikipedia.org/wiki/Chromosom#Geschlechtsbestimmung_durch_Chromosomen_und_ihre_Folgen.
[81] Siehe Brodersen/Anslinger/Rolf, Rn. 253 f.
[82] Siehe Brodersen/Anslinger/Rolf, Rn. 241 f.
[83] Siehe Focus-Online vom 19.10.2008, „Leiche mit männlicher und weiblicher DNA entdeckt".

nach Kontakt mit anderen Personen; dadurch entstehen Mischproben. Dabei kann bspw. folgendes Allel herauskommen: 15/16/21. Als Spurenverursacher kommen daher Personen mit dem Genotyp 15/16 oder 16/21 oder 15/21 oder auch 15/15 etc. in Betracht. Dementsprechend müssen Hypothesen über die Spurenverursacher angestellt werden. Die Sachverständigen fertigen anhand dieser Hypothesen ein Gutachten an, dessen Ergebnis bspw. lauten könnte: Hypothese B ist zehnmal wahrscheinlicher als Hypothese A.[84] Heutzutage können Mischproben von bis zu zwei Personen ausgewertet werden. Besonderheiten ergeben sich bei Sexualdelikten: Aufgrund der besonderen Eigenschaften der Spermien und Eizellen ist es möglich, die Misch-DNA zu entmischen und dann zu analysieren.[85]

Im Gegensatz zur alten RFLP-Methode ist die PCR-Methode aufgrund der Vervielfältigungen der DNA-Fragmente jedoch hoch empfindlich. Die Wahrscheinlichkeit, dass bei zwei Menschen die Anzahl der Wiederholungen an einem STR identisch ist, ist sehr niedrig. Diese Wahrscheinlichkeit verringert sich, je mehr dieser STR-Loci untersucht werden. Damit lässt sich statistisch errechnen, wie viele Personen untersucht werden müssen, damit das gleiche Identifizierungsmuster zweimal in der Bevölkerung auftritt. [86] Bei Untersuchung der acht vorgenannten STR-Loci ergibt sich eine Häufigkeit der Merkmalskombination von eins zu 3.000 Milliarden.[87] Diese Berechnung betrifft aber nur die Häufigkeit in der entsprechenden, ethnisch gleichen Bevölkerung, hier besonders in Deutschland und Europa.

---

[84] Siehe Brodersen/Anslinger/Rolf, Rn. 249 f.
[85] Siehe Brodersen/Anslinger/Rolf, Rn. 251.
[86] Vgl. Wikipedia, „Genetischer Fingerabdruck“, s. unter http://de.wikipedia.org/wiki/Genetischer_Fingerabdruck.
[87] Siehe Hohoff/Brinkmann, „Beweisstück Mensch – Molekulargenetische Möglichkeiten und Eingriffsbefugnisse“, in: Sokol, S. 29 (35).

Trotz des heutzutage häufig erfolgenden Einsatzes der DNA ist diese keinesfalls mit dem Fingerabdruck gleichzusetzen, insbesondere nicht in Bezug auf die rechtlichen Voraussetzungen. Dies ergibt sich v.a. daraus, dass der Mensch permanent Spuren hinterlässt wie Haare oder Hautschuppen, worauf er keinen Einfluss hat. Dadurch erhöht sich die Gefahr, dass Unbeteiligte aufgrund ihrer zufällig hinterlassenen Spuren zum Verdächtigen werden.

V. EXKURS: DNA-REIHENUNTERSUCHUNG

Auch wenn die DNA-Reihenuntersuchung nicht Bestandteil dieser Arbeit ist, so ist sie doch aufgrund ihrer datenschutzrechtlich bedenklichen Aspekte wichtig und sollte daher kurze Erwähnung finden.

Massengentests wurden bereits vor In-Kraft-Treten der gesetzlichen Grundlage am 01.11.2005 durchgeführt. Die heutige rechtliche Grundlage für die DNA-Reihenuntersuchung ist § 81h StPO.

Als großes Problem wird die Freiwilligkeit der Teilnahme an einer solchen Untersuchung angesehen. Zwar darf nach der gesetzlichen Vorschrift eine Verweigerung theoretisch nicht negativ gewertet werden, da dies gegen die Unschuldsvermutung und damit gegen das Rechtsstaatsprinzip verstoßen würde. In der Realität könnte eine Verweigerung in den Köpfen der Exekutive jedoch anders bewertet werden. Tatsächlich löst eine Verweigerung an der Untersuchung eine Überprüfung des Alibis aus. Sollte letzteres sich als nicht haltbar erweisen bzw. gar keines vorhanden sein, wird mit der Begründung, es sei dadurch ein Anfangsverdacht entstanden, ein richterlicher Beschluss für eine Untersuchung

bewirkt. Eine „echte“ Freiwilligkeit kann damit angezweifelt werden.

Des Weiteren wäre gerade aufgrund des enormen Eingriffs ein Richtervorbehalt erforderlich. Aus diesem Grund wurde mit dem Gesetz zur Novellierung der forensischen DNA-Analyse vom 12.08.2005 ein gesetzlicher Richtervorbehalt eingefügt, welcher das Problem der Freiwilligkeit jedoch kaum beheben wird.

Zu kritisieren ist außerdem, dass Personen an einer Untersuchung teilnehmen „müssen“, obwohl gegen diese gar kein Anfangsverdacht besteht. Beispielsweise werden Personen oftmals allein aufgrund ihres Wohnortes ausgewählt. Ein Betroffener muss aktive Mithilfe leisten, um seine Unschuld zu beweisen. Zudem verursacht ein solcher Massengentest hohe Kosten, ohne dass ein Erfolg sichergestellt ist. Wie bereits bei anderen Datenerhebungen besteht zudem auch hier die Gefahr, dass die Daten aufgrund ihres enormen Werts missbraucht werden und entgegen der gesetzlichen Vorgabe gespeichert werden. Dies ist keineswegs absurd.

Die hier erwähnte Problematik wird insbesondere vom Mordfall Wudy im Herbst 2002 getragen: Aufgrund der Ermordung der 38-jährigen Gudrun Wudy wurden im Dorf Poing lebenden Männer (1.500) zur „freiwilligen“ Speichelprobe aufgefordert. Trotz der „Freiwilligkeit“ wurden 14 nicht teilnehmende Männer per Gerichtsbeschluss zur Abgabe ihrer DNA gezwungen, da aufgrund der Nichtteilnahme ein Anfangsverdacht unterstellt wurde. Nachdem dieser erste Test nicht erfolgreich war, wurde der Test zunächst auf 2300 Personen und später auf einen Umkreis von fünf Kilometern, d.h. 10.000 Tests, ausgeweitet. Die Polizei war der Ansicht, dass der Täter über sehr gute Ortskenntnisse verfügen musste und aus dem Bekanntenkreis der Toten käme. Beide Tests verliefen negativ. Der Täter wurde letztlich gefasst, weil seine

Freundin das vom Täter selbst aufgenommene Tatvideo sah und ihn der Polizei meldete. Tatsächlich stammte der Täter aus München und kannte das Opfer nicht.[88]

Im Übrigen ist es eine Frage der Verhältnismäßigkeit, ob der Test bereits in einem frühen Stadium oder erst nach der erfolglosen Ausschöpfung aller Ermittlungsmöglichkeiten angewendet wird. Auch stellt sich die Frage nach einer vorherigen sorgfältigen Einschränkung des möglichen Täterkreises, was nicht nur im Interesse der Betroffenenrechte liegt, sondern auch die Kosten des Verfahrens geringer hält.

[88] Merkur-Online vom 13.09.2002, Mordfall Wudy: 1500 Männer zum Speicheltest; Merkur-Online vom 29.01.2003, „Speicheltest: Ein Mann fehlt"; Merkur-Online vom 18.03.2003, „Zweiter Speicheltest im Fall Wudy"; Merkur-Online vom 28.10.2004, „Nur Gewalt und Porno im Kopf".

TEIL C Datenquellen und deren Rechtsgrundlagen

Seit 2005 werden biometrische Daten im Reisepass gespeichert und sollen nun auch in Personalausweisen zur Geltung kommen. Eine Verwendung biometrischer Daten ist aber nicht neu. Vielmehr werden diese seit Jahren in Informationssystemen von Ländern oder europäischen und internationalen Organisationen sowie Behörden gespeichert.

Das nachfolgende Kapitel soll die konkrete Verarbeitung der Daten in Ausweisen sowie eine ausgewählte Auflistung der Informationssysteme aufzeigen, in welchen biometrische Daten verarbeitet werden. Dabei werden die Informationssysteme allein auf solche der Ermittlungsbehörden und auch hier nur auf solche Systeme beschränkt, welche nach dem Prümer Ratsbeschluss zum Austausch von Fingerabdruck-, DNA- und Kfz-Daten hervorzuheben sind. Auch der Austausch mit EU-Staaten beschränkt sich auf den Austausch zwischen den Ermittlungsbehörden bzw. Sicherheitsbehörden. Somit bleiben bspw. das EURODAC-System als spezielles Informationssystem für Ausländer sowie andere Informationssysteme der Ermittlungsbehörden (ZEVIS etc.) unberücksichtigt.

Ferner soll dieses Kapitel auf die entsprechenden Rechtsgrundlagen hinweisen. Diese werden für den Datenschutz und den Rechtsschutz unerlässlich sein.

A. DER EPASS

Bereits vor mehr als 20 Jahren wollte man als Reaktion auf den Terrorismus der RAF einen maschinenlesbaren Personalausweis mit Fingerabdrücken einführen. Das Volkszählungsurteil des Bundesverfassungsgerichts vom 15.12.1983[89] führte jedoch dazu, dass die Verwendung von Fingerabdrücken im Personalausweis nach § 1 Abs. 2 S. 2 PersAuswG a.F. ausdrücklich verboten wurde.[90] Doch nun stellt sich die Frage, ob dieses Verbot tatsächlich überholt ist.

I. ENTWICKLUNG

1993 brachte die Internationale Zivilluftfahrtorganisation (ICAO), eine Sonderorganisation der Vereinten Nationen, eine Empfehlung namens „Blueprint" (engl. „Blaupause") heraus. Darin hielt die ICAO die UN-Mitgliedstaaten an, Reisepässe mit biometrischen Merkmalen auszustatten. Nach den Ereignissen vom 11. September 2001 übten auch die USA Druck aus und fordern in ihrem „Enhanced Border Security and Visa Entry Reform Act" die Länder auf, bis zum 26.10.2006 biometrische Pässe einzuführen.[91] Zu diesem Zweck sollte die ICAO technische Richtlinien entwickeln. Die Richtlinien der ICAO gelten in den Mitgliedstaaten jedoch nicht unmittelbar, weshalb diese in nationales Recht umgesetzt werden müssen. Letztlich besteht jedoch keine Verpflichtung zur Umsetzung, sondern lediglich eine Vereinbarung dahingehend, zur Einheitlichkeit beizutragen (Art. 37 Chicago Convention).

[89] BVerfG, Urteil vom 15.12.1983, 1 BvR 209, 83, in: BVerfG 65, 1.
[90] Siehe Schaar, Das Ende der Privatsphäre, S. 138 f.
[91] S. „Vorschlag für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger", Dok. 2004/0039 (CNS) der Europäischen Kommission vom 18.02.2004, S. 3.

In Folge dessen beschloss der Rat der Europäischen Union durch die Verordnung 2252/2004/EG vom 13.12.2004[92], Reisepässe entsprechend der Empfehlung der ICAO[93] mit zwei biometrischen Merkmalen auszustatten. Der ursprüngliche – dem Europäischen Parlament vorgelegte – Entwurf sah nur die Pflicht zur Aufnahme eines Merkmals vor. Dementsprechend befasste sich das Europäische Parlament gem. Art. 67 EGV auch nur mit der Verwendung von Gesichtsdaten. Da Art. 67 I EGV dem Europäischen Parlament jedoch keine weiteren Befugnisse verleiht, war der Rat an dessen Stellungnahme letztlich nicht gebunden.[94] Der letzten Endes gefasste Beschluss ist wohl auf den deutschen Innenminister Wolfgang Schäuble zu zurückzuführen, welcher statt des geforderten einen Merkmals versuchte, ein zweites Merkmal durchzusetzen.[95] Die Verordnung zum ePass wurde daher mit zwei biometrischen Merkmalen verabschiedet.

In der Folgezeit erließ die Europäische Kommission – ebenfalls den Empfehlungen der ICAO folgend – mehrere Entscheidungen über „technische Spezifikationen zu Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“[96], welche verbindliche Vorgaben zu den technischen Anforderungen und zur Sicherheit der Daten enthalten. Des Weiteren wurden von der International Organization of Standardization (ISO) Standards zu den Bilddaten

---

[92] *„Verordnung (EG) Nr. 2252/2004 des Rates vom 13.12.2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten2*, ABl. L 385 v. 29.12.2004, S. 1 ff.

[93] ICAO 9303, später ISO/IEC 7501: diese beschäftigen sich mit „Machine Readable Travel Documents“ (MRTD, dt. „maschinenlesbare Reisedokumente“), Dokumente kostenpflichtig einsehbar unter www.iso.org/iso/iso_catalogue.htm.

[94] Siehe Hornung, S. 96.

[95] So Frau Piltz, Frau Pau, Frau Stokar von Neuforn, in: Schaar, Biometrie und Datenschutz, Podiumsdiskussion (S. 77 ff.), S. 79 f.

[96] Kommissionsentscheidungen C (2006) 2909 endg. vom 28.06.2006 und C (2005) 409 vom 28.02.2005.

der einzelnen biometrischen Merkmale sowie Standards zu den Lesegeräten festgelegt.[97]

Aufgrund der unmittelbaren Geltung der EU-Passverordnung werden bspw. in Deutschland seit November 2005 die neuen – mit RFID-Chip und biometrischem Gesichtsbild ausgestatteten – Pässe ausgeliefert. Seit November 2008 werden zusätzlich zwei Fingerabdrücke gespeichert. Dies war früher nicht möglich. § 16 I 1 PassG a.F. verbot die Speicherung von Fingerabdrücken im Reisepass.

Durch Art. 7 Terrorismusbekämpfungsgesetz[98] wurde das Verbot gestrichen[99] und mit § 4 III PassG eine Regelung zur Verwendung biometrischer Merkmale aufgenommen. Zweckmäßigerweise soll der ePass zur Bekämpfung von terroristischen Gefahren sowie zur Feststellung der Fälschungssicherheit dienen.

Die EG-Verordnung 2252/2004 wurde durch die *Verordnung (EG) Nr. 444/2009 des Europäischen Parlaments und des Rates vom 28.05.2009 zur Änderung der Verordnung (EG) Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen*[100] geringfügig geändert. Entsprechend der Stellungnahme des Europäischen Datenschutzbeauftragten vom 26.03.2008 zur Verordnung 2252/2004[101] wurden Befreiungen von der Pflicht zur Abgabe der Fingerabdrücke für Kinder unter zwölf Jahren und für Personen vorgesehen, bei denen eine Abnahme von Fingerabdrücken physisch unmöglich ist. Bei vorübergehender

---

[97] Gesichtserkennung: ISO/IEC 19794-5; Fingerabdrücke: ISO/IEC 19794-4; Iriserkennung: ISO/IEC 19794-6; Chipkarten: ISO 14443; Dokumente kostenpflichtig einsehbar unter www.iso.org/iso/iso_catalogue.htm.

[98] *"Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) vom 09.01.2002"*, BGBl. I 2002 Nr. 3, S. 361 ff.

[99] S. Meuth, S. 49 f.

[100] ABl. L 142 vom 06.06.2009, S. 1 ff.

[101] ABl. C 200 vom 06.08.2008, S. 1 ff.

Unmöglichkeit soll ferner ein anderer Finger verwendet werden; sollte auch dies nicht möglich sein, so ist ein provisorischer Pass auszustellen. Ebenso hat der Europäische Datenschutzbeauftragte das Konzept „1 Person-1 Pass“ bekräftigt. Ebenso wurde Art. 4 III Unterabsatz 2 eingefügt, wonach die Überprüfung zusätzlicher Sicherheitsmerkmale nach Art. 7 II Schengener Grenzkodex möglich ist.

II. TECHNISCHE AUSGESTALTUNG

Der ePass setzt sich zusammen aus einem optisch maschinenlesbaren Bereich und einem kontaktlosen Chip, dem RFID-Chip. Im optisch maschinenlesbaren Bereich befinden sich die personenbezogenen Daten sowie das biometriefähige Foto, vgl. Art. 1 II EG-VO. Im Chip werden neben dem Foto zusätzlich die beiden Fingerabdrücke gespeichert, vgl. Anhang zur Kommissionsentscheidung vom 28.06.2006, Pkt. 3.3.

Eine zentrale Speicherung der Passdaten ist – zumindest in Deutschland – derzeit nicht vorgesehen[102], was aber nicht heißt, dass das in Zukunft nicht möglich wäre. Des Weiteren dürfen die biometrischen Daten nur zur Verifikation, d.h. zum Abgleich des Passinhabers mit den Daten im Pass (1:1-Vergleich), und nicht zur Identifikation Einzelner unter Vielen (1:n-Vergleich) benutzt werden, vgl. Art. 4 III lit. b) EG-VO.

1. RFID-TECHNOLOGIE

RFID („Radio Frequency Identification“) ist ein automatisches Identifikations- und Datenerfassungssystem, durch welches Daten kontaktlos ausgelesen werden können. Vereinfacht betrachtet besteht das RFID-System aus einem Lesegerät und einem

[102] § 4 III 3 PassG; siehe ferner „Antwort der Bundesregierung auf eine Anfrage zu «Biometrischen Daten in Ausweispapieren»“, BT-Drs. 15/4616 v. 04.01.2005, S. 3.

Datenträger. Bei den biometrischen Pässen können Daten nur ausgelesen werden, d.h. es handelt sich um einen Read-Only-Tag. Im Gegensatz dazu gibt es auch Read-Write-Tags, welche sowohl ausgelesen als auch vom Erfassungsgerät beschrieben werden können. Letztere spielen allerdings für den ePass keine Rolle. Tags haben den Vorteil, dass sie extrem klein sind, sichtkontaktlos ausgelesen und an fast jedem Objekt angebracht werden können.[103]

Die Tags enthalten einen Transponder, in welchem die Daten gespeichert sind. Der Transponder besteht aus einer Antenne, welche Funkwellen empfangen und senden kann, und einem Mikrochip. Alle Tags befinden sich in einem Ruhezustand, bis sie in Reichweite eines Lesegerätes kommen und dieses ein Aktivierungssignal aussendet.[104] Über magnetische oder elektromagnetische Felder können die Daten dann ausgelesen werden.

Im Chip sind neben den biometrischen Daten auch die maschinenlesbaren Informationen gespeichert, wie bspw. der Name oder die Anschrift des Passinhabers.

Derzeitige RFID-Chips bereiten jedoch noch einige technische Probleme: So können Störsender bspw. die Kommunikation zwischen Pass und Lesegerät behindern; der Chip kann durch Abknicken zerstört werden. Allerdings ist der Pass auch dann gültig, wenn der Chip kaputt sein sollte. Hier ist jedoch mit Einzelkontrollen zu rechnen.

2. SPEICHERUNG BIOMETRISCHER DATEN

Die Speicherung weiterer biometrischer Merkmale ist durch die Verordnung nicht ausgeschlossen. Dennoch wählte man entsprechend den Empfehlungen der ICAO aufgrund der

[103] Siehe Schmitz/Eckhardt, in: CR 3/2007, S. 171 (172).
[104] Siehe Schmitz/Eckhardt, in: CR 3/2007, S. 171 (ebd.).

Praxistauglichkeit die Verwendung des Gesichts und der Fingerabdrücke.[105] Neben der Speicherung von Bilddaten werden auch weitere Informationen, d.h. bspw. die Augenfarbe, Größe etc. gespeichert.

Die biometrischen Merkmale werden als Bilddatei gespeichert, um die internationale Interoperabilität zu gewährleisten. Zwar ist die Erkennungsleistung hier noch nicht zufriedenstellend, aber es besteht Verbesserungspotential. Templates werden derzeit nicht verwendet, da diese in Europa nicht einheitlich festgelegt sind.[106] Die Bilddatei muss ferner eine bestimmte Qualität aufweisen, d.h. sie muss zwar komprimiert werden, um einen schnellen Abgleich zu ermöglichen. Gleichzeitig darf die Komprimierung aber nicht zu stark sein, da damit ein deutlicher Abfall der Erkennungsleistung einhergeht. Bei geringer Kompression dagegen ist die Erkennungsleistung nur schwach gemindert.[107]

Hinsichtlich der Gesichtsmerkmale ist ein Foto mit Frontalaufnahme erforderlich. Die Qualität der Bilder muss die Anforderungen der ICAO erfüllen. Eine korrekte Erfassung der Bilddaten reicht jedoch nicht aus. Beim Vergleich müssen zusätzlich zu der Erfassung entsprechende Umweltbedingungen wie Licht und Erfassungsgeräte gegeben sein.

Indes bestehen noch Bedenken bzgl. der mehrjährigen Verwendungszeit der Daten. Während beim Gesicht die Matching-Scores mit jedem Jahr, aber dennoch in unbedenklichem Maße sinken[108], hat man herausgefunden, dass die FRR bei Fingern nach zehn Jahren doppelt so hoch ist wie zur Zeit der Erfassung.[109]

---

[105] Siehe „Antwort der Bundesregierung auf eine Anfrage zu «Biometrische Daten in Ausweispapieren»“, BT-Drs. 15/4616 v. 04.01.2005, S.3.
[106] Siehe BSI, BioP I, S. 90.
[107] Siehe BSI, BioP I, S. 91.
[108] Siehe BSI, BioP I, S. 70; BSI, BioFace, S. 7.
[109] Siehe BSI, BioFinger, S. 3.

Trotz oder gerade aufgrund des Einsatzes der Technik ist zu bedenken, dass diese den Beamten nur unterstützen, aber nicht ersetzen soll.[110]

III. SICHERHEIT IM EPASS

In diesem Abschnitt wird die technische Ausgestaltung des Passes angesprochen. Ob diese letztlich den datenschutzrechtlichen Anforderungen genügt, wird in Teil D. zu erörtern sein.

Bei der Verifikation sind die Sicherheit der Chips und der Daten sowie der sichere Umgang mit den Daten während des Verifikationsvorgangs zu gewährleisten. Durch die von der ICAO vorgegebenen Verfahren wird sichergestellt, dass die Daten auch authentisch sind.[111]

Das Ausspähen der Daten („Skimming“) wird durch den Basic Access Control (BAC) verhindert. Der Datenverarbeiter muss hierzu einen Schlüssel, bestehend aus Geburtsdatum, Passnummer und Ablaufdatum, eingeben, ohne den ein Auslesen nicht möglich sein soll. Damit soll sichergestellt werden, dass der Pass bewusst zur Verfügung gestellt wurde.[112]

Dennoch ist es dem britischen Sicherheitsexperten Adam Laurie Anfang 2007 gelungen, die auf dem Pass vorhandenen Daten mithilfe einer selbstentwickelten Software auszulesen.[113] Der Ausweisinhaber wird dies i.d.R. nicht bemerken. Der Schlüssel kann von jedem ausgelesen werden, der im Besitz des Ausweises ist, da die erforderlichen Daten in der MRZ (engl. machine readable zone = maschinenlesbare Zone) stehen. Derzeit wird das Auslesen des Chips aber dadurch behindert, dass über Stunden ein

110 Siehe auch TeleTrust, Kriterienkatalog, S. 62.
111 Siehe TeleTrust, Kriterienkatalog, S. 63.
112 Siehe TeleTrust, Kriterienkatalog, S. 63 f.
113 Bericht der Nachrichtenagentur GmbH v. 08.03.2007, „Britischer Experte knackt elektronischen Reisepass“.

unmittelbarer Kontakt zum Chip bestehen muss. Der Chip konnte jedoch bereits aus einer Entfernung von 50 cm ausgelesen werden.

Hinsichtlich der Fingerabdrücke wird dem Schutz mehr Bedeutung beigemessen, indem zum Auslesen mathematische Verfahren angewandt werden, die nur den Staaten bekannt sind, welche die Befugnis zum Auslesen haben (Extended Access Control = EAC), vgl. Kommissionsentscheidung vom 28.06.2006, Pkt. 5.2. Dadurch haben nur berechtigte Lesegeräte die Möglichkeit, auf die Fingerabdrücke zuzugreifen.

Ferner soll eine Veränderung der Daten bzw. der Software durch Unbefugte beim ePass nicht möglich sein, da die Daten durch eine elektronische Signatur (Passive Authentification = PA) vor Verfälschung geschützt werden. Da die Zugangscodes nicht öffentlich bekannt sind, können die Daten auch nicht weitergegeben werden. Allerdings hat man mittlerweile den Chip erfolgreich kopieren können[114], so dass berechtigte Bedenken in Bezug auf die Zugangssicherheit bestehen.

Des Weiteren besteht die fakultative Möglichkeit, eine digitale Signatur als Active Authentification (AA) einzusetzen, wodurch bewiesen werden könnte, dass es sich bei dem Chip nicht um eine Kopie, sondern um das Original handelt. Im Gegensatz zur PA, welche nur Modifikationen erkennt, ist jeder Chip-Austausch erkennbar. Fälle, in denen sich jemand über die PA hinwegsetzt, sind dann durch die AA erkennbar, was eine doppelte Sicherung bedeuten würde. Durch die Kommissionsentscheidung C (2006) 2909 wurde die Chip-Authentifizierung eingeführt, welche ebenfalls beweisen soll, dass der Chip nicht ausgewechselt wurde. Dies gilt zumindest für Fingerabdruck-Daten bzw. generell

[114] Siehe heise-Meldung v. 03.08.2006, „Sicherheitsexperte führt Klonen von RFID-Reisepässen vor".

spätestens 36 Monate nach Annahme der Spezifikationen, d.h. ab dem 28.06.2009.

Die vorgenannten Erläuterungen beziehen sich aber nur auf die Sicherheit der Soft- und Hardware. Natürlich besteht immer noch die Möglichkeit des Missbrauchs der Daten durch die Datenverarbeiter selbst, insbesondere durch die Passbehörden, die Druckereien bzw. die Kontrollstellen an den Grenzen. Diesbezüglich wurden national, in Deutschland z.B. mit den §§ 16 II, III, 16a S.3, 18 IV, 21 IV PassG Löschungsregelungen geschaffen, wodurch die Datenverarbeiter verpflichtet sind, die biometrischen Passdaten unmittelbar nach Herstellung des ePasses zu löschen.

Ein Missbrauch kann dennoch nicht ausgeschlossen werden.

Einer Reporterin des Fernsehsenders BBC ist es gelungen, auf dem Schwarzmarkt Reisepässe aus 14 europäischen Ländern mit ihrem eigenen digitalen Passbild zu erwerben. Offenbar sind diese von den nationalen Passbehörden falsch ausgestellt und dann ausgesondert worden.[115]

Des Weiteren wurde bereits festgestellt, dass die Überwindungssicherheit sehr niedrig ist und die Lesegeräte in Testreihen mit Schwarz/Weiß-Bildern sowie mit Farbfotos mit nur geringem Aufwand getäuscht werden konnten.[116] Gerade aufgrund der Komplikationen sollten dem Inhaber eines ePasses Sicherheitshinweise an die Hand gegeben werden.

[115] Siehe BBC News vom 01.12.2006, "My fake passports and me"; Meints, in: DuD 2007, 189 (192).
[116] Siehe BSI, BioP I, S. 73.

IV. VOR- UND NACHTEILE DES EPASSES

Kritikerwürdig ist die mangelnde Informationstransparenz. Viele Personen sind entweder gar nicht oder nur schlecht darüber aufgeklärt, was mit ihren Daten geschieht, wenn sie in ein anderes Land reisen. Die Daten könnten dort in zentralen Datenbanken gespeichert und für missbräuchliche Zwecke verwendet werden. Zudem wurde in anderen Ländern das Gebot der dezentralen Speicherung – wie es bspw. in Deutschland besteht – nicht durchgesetzt. Hierbei bestehen erhebliche Risiken in Bezug auf eine Profilbildung. Da beim Reisepass aufgrund der internationalen Verwendung nur mit Bilddaten gearbeitet wird, besteht auch die Möglichkeit, Zusatzinformationen zu gewinnen und zu verarbeiten. Im Übrigen galt auch der vorherige deutsche Reisepass als eines der sichersten Dokumente der Welt.[117] Man konnte im Zeitraum zwischen 2001 und 2006 nur sechs Fälschungen und 344 Verfälschungen verzeichnen.[118] Da die Merkmale zusammen mit den personenbezogenen Daten auf einem Chip gespeichert werden, ist zudem eine Verknüpfung der Daten sehr einfach. Des Weiteren steckt die Biometrie, insbesondere die dazugehörigen Lesegeräte, noch in der Entwicklungsphase. Darüber hinaus ist zu kritisieren, dass in den einschlägigen Vorschriften keine Angaben darüber gemacht werden, welche Falschzurückweisungsrate anzuwenden ist, da hiervon abhängt, in welchem Ausmaß Betroffene, die nicht akzeptiert werden, mit einer weiteren Prüfung zu rechnen haben.[119] Diese richtet sich nämlich nach den nationalen Einreisebestimmungen des Ziellandes.

---

[117] „Antwort der Bundesregierung auf eine Anfrage zu «Biometrischen Daten in Ausweispapieren»", BT-Drs. 15/4616 v. 04.01.2005, S. 2.
[118] „Antwort der Bundesregierung auf eine Anfrage zur «Notwendigkeit neuer biometrischer Pässe aus Sicherheitsgründen", BT-Drs. 16/5507 v. 29.05.2007, S.1.
[119] Vgl. Stellungnahme des Europäischen Datenschutzbeauftragten zur Verordnung 2252/2004, Abl. C 200 vom 06.08.2008, S. 1 ff., Nr. 30.

Die Befürworter halten dennoch am Nutzen biometrischer Pässe fest, insbesondere der ehemalige deutsche Innenminister Otto Schily betonte immer wieder deren Vorteile: so sollen die Kontrollen an den Flughäfen durch die neuen Pässe nun schneller und reibungsloser ablaufen; es würde eine noch höhere Sicherheit gewährleistet, was gerade aufgrund des großen Sicherheits-Gefälles innerhalb der EU von großer Bedeutung sei. Zudem können die Daten bei der Fahndung äußerst hilfreich sein. Die Passdaten sollen in diesem Zusammenhang mit einer Negativdatenbank verglichen werden, welche nicht nur Daten zu gesuchten Personen enthält, sondern auch Seriennummern gestohlener Pässe.[120]

B. DATENSYSTEME BEI NATIONALEN UND INTERNATIONALEN ERMITTLUNGSBEHÖRDEN

Biometrische Daten werden mittlerweile vielfach in Informationssystemen von nationalen und internationalen Behörden gespeichert. Hierzu werden immer mehr Abkommen und Verträge geschlossen, welche nicht nur die jeweiligen nationalen Systeme miteinander vernetzen sollen, sondern auch die nationalen Systeme mit den internationalen und europäischen Informationssystemen. Nachfolgend wird eine Auswahl nationaler und internationaler Informationssysteme sowie Abkommen dargestellt, wobei allerdings nur das INPOL-System und der Austausch nach dem ehemaligen Vertrag von Prüm in dieser Arbeit weitere Beachtung finden.

[120] Siehe TeleTrust, Kriterienkatalog, S. 62.

I. POLIZEILICHES INFORMATIONSSYSTEM IN DEUTSCHLAND – INPOL

Allein in Deutschland existiert eine Vielzahl von Informationssystemen, welche mit biometrischen Daten arbeiten. Um diese Arbeit überschaubar zu halten, wird allerdings nur auf die polizeilichen Informationssysteme Bezug genommen. Damit werden Register über Asylbewerber und Ausländer (EURODAC), etc. ausgenommen. Des Weiteren wird die folgende Darstellung auf Systeme beschränkt, welche mit biometrischen Daten arbeiten.

Das INPOL-System (auch POLAS) wurde 1972 beim BKA in Betrieb genommen. Die Errichtung beruht auf § 2 III BKAG. Die zentrale Stelle des INPOL-Systems ist das BKA, § 2 II, IV BKAG. Organisatorisch teilt sich das INPOL-System in das beim BKA geführte INPOL-Bund (Zentraldatei) und das bei den jeweiligen Landeskriminalämtern geführte INPOL-Land (Verbunddatei). Im Dezember 2001 ist die EU-Kommission vom Rat der Europäischen Union zur Entwicklung eines SIS II (Näheres Pkt. II.) beauftragt worden. Aufgrund der zahlreichen Erweiterungen des SIS, welches z.T. mit dem INPOL-System gekoppelt wurde, musste man auch einer Umstellung des INPOL-Systems ins Auge sehen. Nach langer Entwicklungsphase und mehreren Tests wurde schließlich im Oktober 2008 das INPOL-System auf das neue INPOL 6.0 (INPOL-neu) umgestellt.[121]

Das INPOL-neu umfasst nicht nur wesentlich mehr Informationen – auch für strategische Auswertungen –, sondern schafft auch Querverweise zwischen den Teilen des Systems. Neben dem BKA haben auch das Zollkriminalamt, die Bundespolizei, vgl. § 11 II BKAG, und das Auswärtige Amt hinsichtlich Fahndungsausschreibungen, vgl. § 11 IV BKAG, Zugriff auf INPOL-Bund. Unter den Voraussetzungen des § 14 BKAG können die

[121] Ausführlicher Huke, in: Bayerns Polizei 1/2009, S. 19 (19 f.).

Daten auch an andere Stellen weitergegeben werden, bspw. Europol oder Interpol. In dieser Arbeit wird nur auf die DNA-Analyse-Datei, das Gesichtserkennungssystem und das Automatische Fingerabdruck-System Bezug genommen.

Ob und welche Daten gespeichert werden dürfen, richtet sich nach den speziellen Gesetzen, also dem Strafverfahrensrecht, den Polizeigesetzen der Länder, den §§ 7-9a, 20, 20b, 20i, 20g, 22 BKAG sowie den Errichtungsanordnungen. Letztere müssen den inhaltlichen Anforderungen des § 34 BKAG genügen.

Problematisch kann eine Speicherung werden, wenn die Errichtungsanordnung zu ungenau oder zu weit gefasst ist.

> *Beispiel: Maximilian W. saß exakt sechs Minuten auf der Straße, um einen NPD-Aufmarsch zu blockieren und verstieß damit gegen das Versammlungsgesetz. Das Verfahren wurde letztlich gegen Zahlung von EUR 300,00 eingestellt. Dennoch wurde er von der Polizei als „linksorientierter politisch motivierter Gewalttäter" in die Gewalttäterdatei im Bereich der „Personenfahndung" aufgenommen. Diesem liegt ein Beschluss der Innenministerkonferenz vom 24.11.2000 (Errichtungsanordnung zur Gewalttäterdatei) zugrunde, wonach man schon dann in diese Datei aufgenommen wird, wenn die „Persönlichkeit" annehmen lässt, dass weitere Strafverfahren gegen diese zu führen sind. Anlass kann dabei ein bloßer Platzverweis sein. Folge dieser Anordnung ist, dass Maximilian W. wegen einer Sitzblockade als Gewalttäter gespeichert ist und ihm daraufhin im Juli*

2001 die Ausreise nach Italien gem. § 7 PassG verweigert wurde.[122]

INPOL-Bund wird als Zentral- und als Verbunddatei (§ 11 BKAG) geführt. Im Rahmen der Verbunddatei werden die Daten direkt von den einzelnen Teilnehmern, also bspw. von den Polizeidienststellen, eingegeben und abgefragt, während die Daten der Zentraldatei an das BKA übermittelt und dort eingegeben werden.[123] Berichtigungen und Löschungen dürfen dabei nur von der eingebenden Stelle vorgenommen, Erweiterungen hingegen von jedem durchgeführt werden.

Zugriffe erfolgen aufgrund eines komplexen Berechtigungssystems, d.h. nicht jeder Polizeibeamte hat Zugriff auf alle Daten, ebenso haben alle Polizeibeamten – dies umfasst auch den Zoll, die Bundespolizei sowie die Kriminalamtsbeamten – unterschiedlich weite Zugriffsberechtigungen. Es handelt sich insgesamt um ein hierarchisches Zugriffssystem. Letztlich gibt es jedoch zu jeder Personalnummer eine bestimmte Berechtigung.[124] Wegen der verschiedenen Berechtigungen wird unterschieden zwischen Zugriff auf Daten sowie auf Funktionen.

Bei der Verwendung von Daten ist grundsätzlich die Erforderlichkeit des zur Aufgabenerfüllung notwendigen Datenumfangs zu beachten. Dies ist bei dem hierarchischen System nur schwer möglich,[125] da das System nicht nach der jeweiligen Aufgabe, sondern nach der jeweiligen Berechtigung des Sachbearbeiters differenziert. Zum Großteil wird dies Hand in Hand gehen, z.T. wird das System jedoch mehr bzw. weniger Informationen anbieten als der Fall erfordert.

---

122 Bittner/Staud, in: Zeit-Online v. 15.02.2009, „Vorsicht, Sammelwut".
123 Siehe Riegel, S. 39.
124 Mündliche Auskunft LKA Bayern vom 02.03.2009.
125 Diese Bedenken sieht auch Wirth, in: CILIP 62 (1/1999).

Im Übrigen existieren keine festen Fristen, nach welchen die Daten gelöscht werden müssen, sondern nur Fristen, nach deren Ablauf jeweils die weitere Erforderlichkeit zu prüfen ist, d.h. die Aufbewahrungszeit der Daten kann je nach Fall immer wieder verlängert werden.

Wie in jedem System sind auch beim INPOL-neu probeweise die Abrufe zu protokollieren, § 11 VI BKAG. Vom BKA wird jeder zehnte Abruf protokolliert; im INPOL-Land wird sogar jeder Abruf protokolliert.[126]

Für die Kontrolle von INPOL sind die Datenschutzbeauftragten des Bundes und der Länder zuständig. Des Weiteren sind in den jeweiligen Landeskriminalämtern auch interne behördliche Datenschutzbeauftragte vorhanden.

1. GESICHTSERKENNUNGSSYSTEM[127]

Mithilfe des Systems wird das Gesicht einer Person verformelt. Erst dann kann ein Abgleich erfolgen, welcher teilweise zahlreiche Ergebnisse anzeigt. Daher hat der Endvergleich auch durch den Menschen, und zwar im Vier-Augen-Prinzip, zu erfolgen. So wird beim BKA mittlerweile eine halbjährige Ausbildung zum Lichtbildspezialisten angeboten. Das System kann nur Ähnlichkeiten berechnen, aber bisher nicht die Arbeit des Menschen ersetzen. Aufgrund der Verformelung kann es zudem passieren, dass sich die gesuchte Person vollkommen von dem Ergebnis unterscheidet. Sucht man bspw. einen 45-jährigen weißen Mann, kann es durchaus passieren, dass als Ergebnis eine 18-jährige schwarze Frau präsentiert wird. Im Übrigen muss das Bild eine bestimmte Auflösung aufweisen, was oft zu einem

[126] Wirth, in: CILIP 62 (1/1999).
[127] Zum gesamten Pkt. 1: Mündliche Auskunft LKA Bayern vom 02.03.2009.

Qualitätsverlust führt, weswegen derzeit Bestrebungen vorhanden sind, sämtliche Bilder nur noch als Digitalfotos in das System einzuspeisen.

Es ist festzuhalten, dass das System nur ein Indiz liefern und damit einen Verdachtsmoment schaffen kann, es dient jedoch niemals als Beweis.

Hauptanwendungsbereich der Gesichtserkennung ist der Vergleich von Personen mit Bildern, welche im Rahmen einer Radarkontrolle gemacht worden sind.

2. DNA-ANALYSE-DATEI (DAD)

Bereits 1996 wurde vom LKA Rheinland-Pfalz die erste deutsche DNA-Datenbank eingerichtet.

Die DNA-Analyse-Datei wurde in Deutschland am 17.04.1998 eingerichtet.[128] Vorbild für die deutsche Datenbank war die DNA-Datenbank (National DNA Database) in Großbritannien, welche bereits 1995 eingerichtet wurde.[129] Die Datenbank ist Teil der Zentraldatei beim BKA. Zugriff haben daher auch nur speziell berechtigte Mitarbeiter des BKA und der Landeskriminalämter.

In dieser Datei werden sowohl Spurendatensätze als auch ermittelte DNA-Datensätze von bekannten Personen (Personendatensätze) gespeichert.

Wird eine Spur gefunden, wird dieses an das Kriminaltechnische Institut, in welchem ausschließlich Naturwissenschaftler arbeiten, weitergeleitet. Diese haben keinen Zugriff auf die polizeilichen Systeme und können daher die zugeordnete Nummer auch nicht

[128] Bundesministerium des Innern, „DNA-Analyse“, s. unter www.bmi.bund.de/SharedDocs/Standardartikel/DE/Themen/Sicherheit/ohneMarginalspalte/DNAAnalyse.html?nn=246816.
[129] Brodersen/Anslinger/Rolf, Rn. 273.

dechiffrieren. Aufgrund der organisatorischen Trennung des LKA von Kriminaltechnischen Institut ist die Anforderung des § 81f II S.1 StPO gewahrt.[130]

Nach Erstellung des Identifizierungsmusters wird die DNA vernichtet und das Muster an das zuständige Dezernat im Landeskriminalamt weitergeleitet. Dieses gibt die Daten in die DNA-Analyse-Datei ein und kann sie mithilfe einer Nummer entanonymisieren.[131]

Die DNA-Analyse-Datei macht eine fallübergreifende Analyse möglich, wodurch die Aufklärung von Serienstraftaten erleichtert wird.[132] Dadurch ist nicht nur eine Zuordnung von Spuren zu Personen möglich, sondern auch von verschiedenen Spuren zueinander.

Nach einer gewissen Zeit erfolgt eine Aussonderungsprüfung, d.h. es wird die weitere Erforderlichkeit der Daten überprüft. Diese Prüfung hat bei Erwachsenen in der Regel nach zehn Jahren, bei Jugendlichen nach fünf Jahren zu erfolgen. Spuren werden für immer gespeichert.[133]

Wird eine Spur untersucht und ergibt sich dadurch ein Treffer, darf maximal ein STR abweichen; in diesem Fall ist dann eine Nachuntersuchung fällig.[134]

Da durch die Beschlüsse zum Austausch von DNA-, Fingerabdruck- und Kfz-Daten (vgl. Pkt. III.) mittlerweile eine Vernetzung der beteiligten mitgliedstaatlichen Datenbanken erfolgt, können auch DNA-Profile aus anderen Ländern in den

---

130 Mündliche Auskunft LKA Bayern vom 02.03.2009.
131 Mündliche Auskunft LKA Bayern vom 02.03.2009.
132 Polizei Rheinland Pfalz, „Der Gentische Fingerabdruck (DNA-Analyse)“, s. unter www.polizei.rlp.de/internet/nav/cfb/broker.jsp?uCon=78034500-1ced-0014-4b94-615af5711f80&uBasVariantCon=22222222-2222-2222-2222-222222222222.
133 Mündliche Auskunft LKA Bayern vom 02.03.2009.
134 Mündliche Auskunft LKA Bayern vom 02.03.2009.

Abgleich einbezogen werden. Es erfolgt hierbei ein automatisierter Austausch der Identifizierungsmuster. Wird ein Treffer angezeigt, kommt es zu einer Nachricht an die eingebende Stelle. Der weitere Datenverkehr erfolgt dann zwischen den Polizeibehörden.[135] Bisher sind nur folgende Länder beteiligt: Spanien, Österreich, Slowenien, Luxemburg und die Niederlande.[136]

3. AUTOMATISCHES FINGERABDRUCK-IDENTIFIZIERUNGS-SYSTEM (AFIS)[137]

Das AFIS wird seit 1992 – zunächst im Asylbereich, ab 1993 auch zur Spurenauswertung – beim BKA betrieben und ermöglicht den Vergleich zweier aktueller Fingerabdrücke (1:1) sowie der Identifizierung einer Person (1:n). Das AFIS stellt eine Verbindung zwischen Spur und Person bzw. zwischen verschiedenen Spuren her. Seit 2002 werden im AFIS auch Handflächen erfasst. Dies ist überaus sinnvoll, wenn der Täter eine Identifizierung des Opfers verhindern will und aus diesem Grund die Fingerabdrücke abtrennt – was durchaus schon vorgekommen ist.[138]

Zum AFIS haben nur bestimmte Personen Zugriff. Auch die Bearbeitung erfolgt nur durch Personen, welche dafür ausgebildet worden sind. Wie bereits beim Gesichtserkennungssystem gilt jedoch auch hier das Vier-Augen-Prinzip.

Die Fingerabdrücke werden derzeit noch offline erfasst und verschlüsselt über eine Polizeileitung oder über Mobilfunk an das BKA versendet. Letzteres geschieht v.a. durch neuartige mobile

---

[135] Mündliche Auskunft LKA Bayern vom 02.03.2009.
[136] Mündliche Auskunft LKA Bayern vom 02.03.2009.; s. auch Antwort der Bundesregierung auf die Kleine Anfrage zu „Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden polizeilichen Zusammenarbeit, BT-Drs. 16/14150 vom 22.10.2009, S. 2.
[137] Hierzu erfolgte eine mündliche Auskunft LKA Bayern vom 02.03.2009.
[138] Mündliche Auskunft LKA Bayern vom 02.03.2009.

Auslesegeräte (sog. FAST-ID, welche nur Minutien zum Abgleich verwenden). Diese speichern die Daten als Template sowie als Rohdatum ein. Mittlerweile werden die Daten digital gespeichert.

Die Klassifizierung wird nunmehr vom System automatisch durchgeführt, bedarf aber der Nachbearbeitung.[139] Die Minutien werden im System zwar automatisch codiert; allerdings ist auch hier eine Nachbearbeitung erforderlich. Die Automatik wirkt daher nur unterstützend. Ein Abgleich erfolgt aufgrund der Kombination aus Rohdatum und Template. Je nach Übereinstimmung wird ein bestimmter Punktewert vergeben. Da die Übereinstimmung je nach Druck und Auflage des Fingers variiert, ist sie eher relativ. Die besten Treffer werden daher noch einem Direktvergleich unter der Lupe unterzogen.

Es muss zweifelsfrei feststehen, dass der Täter der Spurenverursacher ist; ansonsten ist der Abdruck für das Verfahren wertlos.

Die AFIS-Daten sind anonymisiert, d.h. es sind nur eine Nummer sowie einige andere erforderliche Daten angegeben. Die Nummer kann erst mithilfe des INPOL-Systems entanonymisiert werden. Dadurch wird sichergestellt, dass der AFIS-Bearbeiter keine Ahnung von der Identität des Abdruckinhabers bekommt.

Die Daten werden beim BKA 24 Stunden am Tag ausgewertet. Die Fehlerquote liegt bei guter Erfassung der Daten annähernd bei Null. Jede vierte überprüfte Person ist ein Treffer.

Die Speicherfrist richtet sich nach der Art der Straftat: Bei einem Mord wird der Abdruck unbegrenzt gespeichert, bei Verbrechen fünf bis zehn Jahre und bei Vergehen in der Regel ein Jahr.[140]

[139] Mündliche Auskunft LKA Bayern vom 02.03.2009.
[140] Mündliche Auskunft LKA Bayern vom 02.03.2009.

Durch die Beschlüsse zum Austausch von DNA-, Fingerabdruck- und Kfz-Daten (vgl. Pkt. III.) erfolgt nun auch ein Abgleich mit anderen Datenbanken. Derzeit ist nur ein Abgleich mit der österreichischen Datenbank möglich, was sich aber noch ausdehnen wird.[141]

4. ERKENNUNGSDIENST

Auch in der Erkennungsdienstlichen Datei sind biometrische Daten gespeichert. Zu diesen gehören theoretisch auch die Körpergröße, die Schuhgröße etc., welche für diese Arbeit jedoch nicht relevant sind.

II. INFORMATIONSSYSTEME BEI EUROPÄISCHEN UND INTERNATIONALEN ERMITTLUNGSBEHÖRDEN

1. EUROPOL UND DAS TECS

Aufgrund der steigenden terroristischen Bedrohung beschloss der Europäische Rat 1975 in Rom, ein regelmäßig tagendes Gremium der Innen- und Justizminister der damals neun Mitgliedstaaten[142] zur Erörterung der Fragen der inneren Sicherheit und öffentlichen Ordnung einzurichten[143], die TREVI-Kooperation[144]. Auf Basis dieser Einrichtung wurde am 28./29.06.1991 vorgeschlagen, eine

---

[141] Mündliche Auskunft LKA Bayern vom 02.03.2009.; s. auch „Antwort der Bundesregierung auf die Kleine Anfrage BT-Drs. 16/14120 – Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Polizeizusammenarbeit", BT-Drs. 16/14150 vom 22.10.2009, S. 2.

[142] Es handelte sich dabei um die BRD, Dänemark, Frankreich, Irland, Italien, die BENELUX-Staaten und das Vereinigte Königreich.

[143] Milke, S. 23.

[144] Über die Herkunft des Namens besteht bisweilen Uneinigkeit. TREVI komm entweder von der Abkürzung „Terrorisme, Radicalisme, Extremisme, Violence Internationale" (vgl. u.a. Akmann, in: JA 1994, S. 49 (51) oder bezeichnet den Gründungsort der Minister bei der Fontana di Trevi in Rom (Wenzel, in: Milke, S. 23.).

Europäische Kriminalpolizeiliche Zentralstelle („Europol“) einzurichten.[145] Daher wurde im Dezember 1991 die „Europol-Drogeneinheit“ (European Drugs Unit = EDU) als Vorläuferorganisation von Europol mit Sitz in Den Haag institutionalisiert. Am 03.01.1994 nahm die EDU ihre Arbeit auf.[146] Zunächst diente eine Ministervereinbarung vom Juni 1993 als Rechtsgrundlage[147], wurde aber dann durch eine Gemeinsame Maßnahme[148] der Staats- und Regierungschefs im März 1995 ersetzt, wobei beide Rechtsgrundlagen keine echte Ermächtigungsgrundlagen darstellten, da sie für den Datenaustausch auf die jeweiligen nationalen Gesetze verwiesen und auch kein einheitliches Datenschutzrecht vorhanden war.[149]

Gem. Art. K1 Nr. 9 des EU-Vertrags von Maastricht wurde die Errichtung eines Europäischen Polizeiamtes (Europol) vorgeschrieben, wobei die zukünftigen Aufgaben auf den Informationsaustausch, die Terrorismusbekämpfung, die Bekämpfung des illegalen Drogenhandels und sonstige schwerwiegende Formen der internationalen Kriminalität beschränkt wurden. Im Hinblick auf zukünftige Informationssysteme bei Europol waren sich die Mitgliedstaaten einig, dass wegen der damit verbundenen Eingriffe in das Recht auf Privatsphäre ein völkerrechtliches Übereinkommen als rechtliche Basis aufgrund des Vorbehalts des Gesetztes erforderlich ist, wobei sie mit Art. K 3 II lit. c) EUVM die rechtliche Grundlage für ein

145 Milke, S. 28 f.
146 Milke, S. 34 f.
147 Kämper, S. 53; BGBl. II 1995, Nr. 6, S. 154 ff.
148 *„Gemeinsame Maßnahme vom 10.03.1995 bezüglich der Europol-Drogenstelle, vom Rat aufgrund von Artikel K.3 des Vertrags über die Europäische Union beschlossen“,* ABl. L 62 v. 20.03.1995, S. 1 ff.
149 Kämper, S. 53 f.

Übereinkommen geschaffen haben.[150] Im Juli 1995 kamen die Vertreter der Regierungen der Mitgliedstaaten in Brüssel zusammen und unterzeichneten die auf Art. K 3 II lit. c) EUVM gestützte Konvention (Europol-Übereinkommen, auch EÜK)[151], welche am 01.10.1998 in Kraft trat. In Folge dessen wurden mehrere Protokolle und Durchführungsbestimmungen erarbeitet, welche das Übereinkommen ergänzten. Am 01.07.1999 hat Europol schließlich gem. Art. 45 IV EÜK seine Tätigkeit aufgenommen.[152]

Mitte 2007 hat der Rat der Europäischen Union beschlossen, das Übereinkommen durch einen Ratsbeschluss zu ersetzen.[153] Dieser bietet den Vorteil, dass zukünftig keine zeitraubende Ratifikation mehr erfolgen muss und damit eine Umsetzung der Vorschriften innerhalb kürzerer Zeit möglich ist.

Der Beschluss des Rates 2009/371/JI zur Errichtung des Europäischen Polizeiamtes (Europol)[154]sieht u.a. folgende Änderungen vor:

- Europol ist nicht mehr Bestandteil der dritten, sondern wird Teil der ersten Säule;
- im Gegensatz zum bisherigen Aufgabenbereich ist kein Anknüpfungspunkt an die organisierte Kriminalität mehr erforderlich; der Aufgabenbereich erweitert sich damit wesentlich;

---

[150] Milke, S. 34; Der Grundsatz vom Vorbehalt des Gesetzes gilt nicht nur in der BRD, sondern auch in allen anderen Staaten der EU sowie für die EU selbst, vgl. Zuleeg, in: NJW 1994, 545 (547).
[151] ABl. C 316 v. 27.11.1995, S. 2 ff.: „Übereinkommen aufgrund von Artikel 3.K d) des Vertrags über die Europäische Union über die Errichtung eines Europäischen Polizeiamts (Europol-Übereinkommen)".
[152] ABl. C 185 v. 01.07.1999, S. 1.
[153] Homepage der Europäischen Kommission „Europol"; abrufbar unter http://ec.europa.eu/justice_home/fsj/police/europol/fsj_police_europol_de.htm.
[154] ABl. L 121 v. 20.05.2009, S. 37 ff.

- es wird die Möglichkeit eröffnet, neue Datenbanken einzurichten;
- der Austausch personenbezogener Daten mit Drittstellen/-staaten kann zukünftig auch ohne Vorliegen eines entsprechenden Abkommens durchgeführt werden.[155]

Europol hat am 01.01.2010 seine Arbeit auf Basis dieses Ratsbeschlusses aufgenommen, vgl. Art. 64 II Ratsbeschluss.[156]

Der Ratsbeschluss wurde in Deutschland umgesetzt durch das *Gesetz zur Änderung des Europol-Gesetzes, des Europol-Auslegungsprotokollgesetzes und des Gesetzes zu dem Protokoll vom 27.11.2003 zur Änderung des Europol-Übereinkommens und zur Änderung des Europol-Gesetzes*[157].

Hauptaufgabe von Europol ist gem. Art. 5 Ratsbeschluss die Sammlung und Auswertung von Informationen und Erkenntnissen, die Unterstützung von Ermittlungen sowie die Erleichterung des Informationsaustausches zwischen den Mitgliedstaaten. Mit Art. 6 Ratsbeschluss wurde dem Europol-Personal ferner die Teilnahme an gemeinsamen Ermittlungsgruppen eingeräumt. Dies war vorher nicht möglich. Allerdings haben die Europol-Bediensteten gem. Art. 6 I Ratsbeschluss keine Befugnis zur Durchführung von Zwangsmaßnahmen.

Gem. Art. 9 Ratsbeschluss entsendet jeder Mitgliedstaat Verbindungsbeamte (Europol Liaisaon Officer – ELO) zu Europol, welche in Kontakt zur nationalen Stelle – in Deutschland ist das gem. Art. 1 § 1 Europol-Gesetz das BKA – stehen und für den Austausch von Informationen verantwortlich sind.

---

155 MEPA-Buch (Stand: Nov. 2008), Allgemeiner Teil, Teil 1B, S. 13 f.
156 MEPA-Buch (Stand: Nov. 2010), Allgemeiner Teil, Teil 1B, S. 7.
157 BGBl. II 2009 Nr. 50, S. 2504 ff.; In-Kraft-Treten am 01.01.2010, vgl. § 10 Europol-Gesetz i.V.m. Art. 64 II Ratsbeschluss.

In den Art. 10-20 Ratsbeschluss wird das Europol-Computersystem TECS[158] näher beschrieben. Dabei handelt es sich um das Informationssystem, die Arbeitsdateien zu Analysezwecken und die Indexdatei.

Das Informationssystem soll einen raschen Überblick über die zu einer Person gespeicherten Daten vermitteln.[159] Der Dateninhalt ergibt sich aus Art. 12 I bis III Ratsbeschluss. Zugriff darauf haben gem. Art. 13 I Ratsbeschluss die Verbindungsbeamten, die nationale Stelle i.S.d. Art. 8 Ratsbeschluss und Europol selbst. In Deutschland haben auch die Behörden der Bundespolizei, des Zollfahndungsdienstes sowie der Polizeien der Länder auf Grundlage von Art. 13 VI Ratsbeschluss i.V.m. Art. 1 § 3 Abs.1 Europol-Gesetz über das INPOL-System Zugriff auf das Informationssystem. Das BKA ist gem. Art. 11 III Ratsbeschluss nach außen datenschutzrechtlich verantwortlich. Im Informationssystem werden gem. Art. 12 II lit. g) Ratsbeschluss auch biometrische Merkmale, d.h. Fingerabdrücke und DNA-Profile, gespeichert.

Als Arbeitsdatei dient das Analysesystem. Unter „Analyse“ ist gem. der Legaldefinition in Art. 14 II Ratsbeschluss die „Zusammensetzung, Verarbeitung oder Nutzung von Daten zwecks Unterstützung der kriminalpolizeilichen Ermittlungen“ zu verstehen. Die Errichtung der Dateien erfolgt anlassbezogen durch Errichtungsanordnung des Direktors, welcher aus eigner Initiative oder auf Ersuchen eines Mitgliedstaates handelt, wobei die Errichtungsanordnung gem. Art. 16 Ratsbeschluss der vorherigen Zustimmung des Verwaltungsrates und der Gemeinsamen Kontrollinstanz bedarf. Der Inhalt der Analysedateien ist sowohl bzgl. des Personenkreises als auch des Datenumfangs erheblich weiter als der des Informationssystems (vgl. Art. 15 I

[158] Die Abkürzung steht für „The Europol Computer System“.
[159] Milke, S. 74 f.

Ratsbeschluss). Nähere Angaben zum Inhalt der Dateien sind in den aufgrund des Art. 14 Ratsbeschluss beschlossenen Durchführungsbestimmungen enthalten. Zudem besteht gem. Art. 10 Ratsbeschluss auch die Möglichkeit, besonders sensible Daten wie bspw. die rassische oder ethnische Herkunft, Religionszugehörigkeit oder das Sexualleben zu speichern. Dazu muss allerdings die Erforderlichkeit der Errichtungsanordnung begründet werden. Für jedes Projekt wird gem. Art. 14 II Ratsbeschluss eine Analysegruppe gebildet. Die Mitgliedstaaten sind dann gem. Art. 14 III Ratsbeschluss bei einem Ersuchen von Europol verpflichtet, Daten zu liefern, wenn und soweit die Daten für die spezielle Analysedatei erforderlich sind. Ein Zugriff auf das System ist den nationalen Behörden nur durch die Verbindungsbeamten und dann auch nur einem bestimmten Teilnehmerkreis möglich.[160]

Das Indexsystem stellt ein Fundstellenverzeichnis zu den Analysedateien dar, über welches die Verbindungsbeamten bei einer Abfrage erkennen können sollen, ob in einer der Arbeitsdateien Informationen gespeichert sind, die ihren Entsendestaat betreffen. Allerdings soll es nicht möglich sein, über das Indexsystem Rückschlüsse auf den Inhalt der Arbeitsdateien zu ziehen (Art. 15 III Ratsbeschluss). Zugang zum Indexsystem haben gem. Art. 15 II Ratsbeschluss die Direktoren, das Europol-Personal, die Verbindungsbeamten sowie die ordnungsgemäß ernannten Mitglieder der nationalen Stellen.

Europol unterhält durch Kooperationsabkommen Beziehungen zu anderen Staaten und Organisationen, u.a. Eurojust und Interpol, vgl. Art. 22, 23 des Ratsbeschlusses.

In Art. 29 I des Ratsbeschlusses wird die datenschutzrechtliche Verantwortung geregelt. Demnach sind die Mitgliedstaaten

[160] Meuters, S. 198.

hinsichtlich ihrer eingegebenen und übermittelten Daten (lit. a) und Europol im Übrigen (lit. b) für die Einhaltung der Vorschriften verantwortlich. Die mitgliedstaatliche Einhaltung der Vorschriften wird durch die nationalen Kontrollinstanzen sichergestellt (vgl. Art. 33 des Ratsbeschlusses), während die Gemeinsame Kontrollinstanz (GKI) für die Einhaltung des Datenschutzes durch die Europol-Bediensteten zuständig ist (vgl. Art. 34 des Ratsbeschlusses).

Des Weiteren wurde ein unabhängiger Datenschutzbeauftragter eingerichtet, Art. 28 I Ratsbeschluss. Dieser kontrolliert ebenfalls die Einhaltung der Bestimmungen. Sollte er zu der Überzeugung gelangen, dass diese nicht eingehalten werden, unterrichtet er den Direktor, Art. 28 IV Ratsbeschluss. Bleibt dieser untätig, wird die Angelegenheit dem Verwaltungsrat weitergeleitet. Erfüllt auch dieser seine Verpflichtungen nicht, kann sich der Datenschutzbeauftragte an die GKI wenden.

Neben den üblichen Betroffenenrechten (Auskunft, Löschung, Berichtigung) steht dem Betroffenen zusätzlich die Möglichkeit einer Beschwerde bei der GKI offen, Art. 32 Ratsbeschluss.

Da das Schengener Informationssystem (SIS) in der Praxis viel effektiver genutzt wird als die Informationssuche über Europol, wird Europol bei der nachfolgenden Untersuchung außer Acht gelassen. Dennoch sollte die Europäische Polizeibehörde Europol bekannt sein, da die Befugnisse auch hier immer weiter ausgeweitet werden. Das SIS ist v.a. aufgrund der Erweiterung – auch durch die Beschlüsse zum Austausch von DNA-, Fingerabdruck- und Kfz-Daten – das wesentliche europäische Kommunikationssystem.

2. SCHENGEN UND DAS SCHENGENER INFORMATIONSSYSTEM (SIS)

1985 wurde von den Regierungschefs von Deutschland, Frankreich und den Benelux-Staaten ein *Abkommen über den schrittweisen Abbau der Binnengrenzkontrollen* (Schengener Übereinkommen, Schengen I) beschlossen, dessen Ziel es war, „durch den Wegfall der Grenzkontrollen eine schnellere und effektivere Warenbewegung innerhalb ihrer Vertragsstaaten zu ermöglichen“[161]. Jedoch musste man die mit dem Abbau verbundenen Sicherheitsverluste ausgleichen. Daher wurde am 19.06.1990 das Schengener Durchführungsabkommen (SDÜ, Schengen II)[162] beschlossen, welches in der BRD am 01.09.1993 in Kraft trat.[163] Gem. Art. 140 I SDÜ kann jeder Mitgliedstaat der EU dem SDÜ beitreten. Das Ziel von Schengen war die Sicherstellung eines einheitlichen Niveaus der Kontrollen an den Grenzen, die Einrichtung eines Fahndungssystems sowie die Verbesserung der polizeilichen Zusammenarbeit der beteiligten Staaten.[164]

Schließlich wurde durch den Amsterdamer Vertrag von 1997 der Schengen-Besitzstand (d.h. das Schengener Übereinkommen, das Durchführungsübereinkommen sowie die dazugehörigen Beschlüsse) in den Rechtsrahmen der Europäischen Union überführt. Damit übernimmt automatisch jeder neue EU-Mitgliedstaat den Schengen-Besitzstand.

Bei dem Schengener Informationssystem (SIS), welches auf der Grundlage der Art. 92 SDÜ eingerichtet wurde, handelt es sich um ein gemeinsames polizeiliches Fahndungssystem. Dieses enthält

---

161 Milke, S. 124.
162 BGBl. II 1993, Nr. 23, S. 1013 ff.
163 Dies erfolgte in der BRD durch das *„Gesetz zu dem Schengener Übereinkommen vom 19.Juni 1990 betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen“*, BGBl. II 1993, Nr. 23, S. 1010 ff.; Bekanntmachung des Inkrafttretens, BGBl. II 1994, Nr. 21, S. 631 ff.
164 Kämper, S. 63.

Fahndungsersuchen nach Personen und Sachen, sowie Ausschreibungen zur Aufenthaltsermittlung bestimmter Personen und zur Zurückweisung ausländischer Personen. Die dabei erforderlichen Daten werden von den Polizeibehörden der Mitgliedstaaten über eine nationale Zentralstelle – laut dem Ausführungsgesetz zum SDÜ ist dies in Deutschland das BKA – in das SIS eingegeben.[165]

Das SIS hat mittlerweile eine große Bedeutung für die Europäische Union, da innerhalb der Schengen-Staaten eine internationale Fahndung grundsätzlich nicht mehr über Interpol, sondern über das SIS erfolgt.[166]

Der Rat der EU beschloss Ende 2001, dass das SIS gem. Titel IV SDÜ durch SIS II ersetzt werden soll, damit künftig auch „die jüngsten Entwicklungen auf dem Gebiet der Informationstechnik genutzt werden können und das System um neue Leistungsmerkmale ergänzt werden kann".[167] Dementsprechend wurde die Erweiterung des SIS durch einen Ratsbeschluss sowie durch eine Verordnung umgesetzt. Das derzeitige „SIS all 4 you" oder auch „SIS 1+" stellt dabei lediglich eine Übergangslösung dar, bis das SIS II mitsamt seinen Ergänzungsbestimmungen durchführbar ist.

Die *Verordnung (EG) Nr. 1987/2006 des Europäischen Parlaments und des Rates vom 20.12.2006 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)*[168] betrifft die Einreise und Ausreise sowie Ausschreibungen von Drittstaatsangehörigen, mithin also die ehemalige erste Säule der EU (Immigration und Außengrenze). Die VO (EG) Nr. 1987/2006 bildet die Rechtsgrundlage für das SIS der

---

165 Milke, S. 127 f.
166 Wilkesmann, in: NStZ 1999, 68 (69).
167 Vgl. Grund (3) der Verordnung (EG) Nr. 2424/2001.
168 ABl. L 381 v. 28.12.2006, S. 4 ff.

zweiten Generation. Dementsprechend betrifft die Verordnung sämtliche Angelegenheiten, die in den Bereich des ehemaligen EG-Vertrages fallen, vgl. Grund (3) der Verordnung (EG) Nr. 1987/2006. Ergänzt wird die Verordnung (EG) Nr. 1987/2006 durch die *Verordnung (EG) Nr. 2424/2001 des Rates vom 06.12.2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II)*[169]. Die Verordnung ist unmittelbar anwendbar und bedarf keiner nationalen Umsetzung. Letztere trat am 17.01.2007 in Kraft. In Bezug auf die Verordnung finden die Datenschutzrichtlinie der EG Nr. 95/46/EG vom 24.10.1995[170] sowie die Verordnung der EG Nr. 45/2001 vom 18.12.2000[171] Anwendung.

Weitere Rechtsgrundlage des SIS II ist der *Beschluss 2007/533/JI des Rates vom 12.06.2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II)*[172]. Dieser wird ergänzt durch den *Beschluss 2001/886/JI des Rates vom 06.12.2001 über die Entwicklung des Schengener Informationssystems der zweiten Generation (SIS II)*[173]. Die Ratsbeschlüsse regeln sämtliche Angelegenheiten aus dem Bereich der ehemaligen dritten Säule, die in den Bereich des EU-Vertrages fallen, und betreffen die polizeiliche und justizielle Zusammenarbeit.

Auf den Ratsbeschluss 2007/533/JI finden folgende Datenschutzregelungen Anwendung:

---

169 Abl. L 328 v. 13.12.2001, S. 4 ff.; geändert durch die Verordnung (EG) Nr. 1988/2006 des Rates v. 21.12.2006 (ABl. L 411 v. 30.12.2006, S. 1 ff.)
170 ABl. L 281 v. 23.11.1995, S. 31 ff.
171 ABl. L 8 v. 12.01.2001, S. 1 ff.
172 ABl. L 205 v. 07.08.2007, S. 63 ff.
173 ABl. L 328 v. 13.12.2001, S. 1 ff.; geändert durch den Beschluss 2006/1007/JI v. 21.12.2006 (ABl. 411 v. 30.12.2006, S. 78 ff.).

- *Übereinkommen des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28.01.1981*[174],
- Grundsätze der *Empfehlung R (87) 15 des Ministerkomitees des Europarats vom 17.09.1987 über die Nutzung personenbezogener Daten im Polizeibereich*[175],
- *Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18.12.2000*,
- *Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*[176], sowie
- *die Datenschutzbestimmungen des Europol-Übereinkommens vom 26.07.1995*[177] *und des Eurojust-Ratsbeschlusses vom 28.02.2002*[178].

Der Beschluss 2007/533/JI trat am 27.08.2007 in Kraft. Da der Ratsbeschluss in den Mitgliedstaaten nicht unmittelbar anwendbar ist, muss er in nationales Recht umgesetzt werden. In Deutschland geschah dies durch das SIS II-Gesetz[179]. Der Ratsbeschluss 2007/533/JI und damit auch das SIS II-Gesetz sind bislang noch nicht anwendbar, da vor der Umsetzung die Voraussetzungen des Art. 71 III des Ratsbeschlusses erfüllt sein müssen.

---

174 SEV Nr. 108, Text s. unter http://conventions.coe.int/Treaty/GER/Treaties/Html/108.htm.
175 Text s. unter www.coe.int/t/dghl/cooperation/economiccrime/organisedcrime/Rec_1987_15.pdf.
176 ABl. L 350 v. 30.12.2008, S. 60 ff.
177 ABl. C 316 v. 27.11.1995, S. 2 ff.
178 ABl. L 63 v. 06.03.2002, S. 1 ff.
179 *"Gesetz zum Schengener Informationssystem der zweiten Generation (SIS-II-Gesetz) vom 06.06.2009"*, siehe unter BGBl. I 2009, Nr. 30, S. 1226 ff.

Das SIS II wird künftig aus einem zentralen System, welches sich in Straßburg befindet, sowie den nationalen Systemen (N.SIS II) bestehen. Jeder Mitgliedstaat ist für sein nationales System verantwortlich, vgl. Art. 6, 10 Ratsbeschluss und Art. 6, 10 der Verordnung.

Im SIS II werden fortan auch biometrische Daten verwendet, u.a. durch Gebrauch einer biometrischen Suchfunktion. Vorerst kann nur ein One-to-One-Abgleich (ein Abdruck wird mit einem bestimmten Datensatz in der Datei verglichen) erfolgen. Sobald die Technik ausgereift ist, wird auch eine One-to-Many-Suche (1:n) möglich sein. Dieser Vorteil im Bereich der polizeilichen Ermittlungstätigkeit bringt jedoch auch eine weitergehende Überwachung des Bürgers mit sich. Durch die biometrische Vernetzung könnte das SIS II zu einem biometrischen Register aller Einreisenden in die EU werden. Man kann auf jeden Fall sagen, dass das SIS II nun mehr einem Informationssystem als einem Fahndungssystem gleichkommt. Sämtliche gespeicherten Daten können untereinander verlinkt werden, d.h. es kann bspw. eine Verknüpfung zwischen dem Bereich „illegale Immigration" und „Menschenschmuggel" hergestellt werden.

Ferner wurde die Zahl der Zugriffsberechtigten ausgeweitet. Hatten vorher nur die Polizeibehörden, der Zoll und die Bundespolizei Zugriff, so sind jetzt auch Europol (vgl. Art. 41 Ratsbeschluss), Eurojust (vgl. Art. 42 Ratsbeschluss), die Kraftfahrzeugzulassungsstellen, die Justizbehörden der Mitgliedstaaten und in eingeschränktem Maße auch Interpol (vgl. Art. 55 Ratsbeschluss) zugriffsberechtigt.

Außerdem wurde in jedem Vertragsstaat in den Zentralstellen ein nationales SIRENE[180]-Büro eingerichtet, in welchem zusätzliche

[180] Die Abkürzung steht für „Supplementary Information Request at the National Entry" oder „Supplément d'Information Requis a l'Entrée Nationale" (Wilkesmann, in:

ergänzende Daten über die zur Fahndung im SIS II ausgeschriebenen Personen und Sachen abgefragt werden können.

Das SIS II unterliegt vielfältigen Kontrollmöglichkeiten. Das zentrale SIS wird von der Verwaltungsbehörde beaufsichtigt (vgl. Art. 16 Ratsbeschluss, Art. 16 der Verordnung), welche wiederum durch den Europäischen Datenschutzbeauftragten kontrolliert wird (vgl. Art. 61 Ratsbeschluss, Art. 43 der Verordnung). Die nationalen Systeme sollen von einer nationalen Kontrollinstanz überwacht werden (vgl. Art. 60 Ratsbeschluss, Art. 44 der Verordnung). Die nationalen Kontrollinstanzen und der Europäische Datenschutzbeauftragte arbeiten wiederum zusammen (Art. 62 Ratsbeschluss, Art. 46 der Verordnung).

Die Rechtsgrundlagen des SIS II sehen ferner Sanktionen (vgl. Art. 65 Ratsbeschluss, Art. 49 der Verordnung) sowie Haftungsvorschriften (vgl. Art. 64 Ratsbeschluss, Art. 48 der Verordnung) vor.

3. DAS INFORMATIONSSYSTEM BEI INTERPOL

1923 wurde die „Internationale kriminalpolizeiliche Kommission (IKPK)“ in Wien als Vorläufer von Interpol gegründet. Ziel der IKPK war es, „unter Ausschaltung des zeitraubenden diplomatischen Weges den direkten Amtshilfeverkehr zwischen den Kriminalpolizeibehörden zu etablieren und ein internationales Polizeibüro zu schaffen“[181]. 1956 wurde die Organisation in „Internationale Kriminalpolizeiliche Organisation (IKPO, OICP, ICPO)“, auch „Interpol“, umbenannt und erhielt ihr bis heute gültiges *Statut et règlement général de l'OIPC*[182] *(Interpol)*[183]. Der

NStZ 1999, 68 (69)) -> dt. Übersetzung: „Nationale Zentralstelle für den Informationsaustausch im SIS“.

[181] Milke, S. 116.

[182] “Organisation Internationale de la Police Criminelle“.

[183] Kämper, S. 42.

Sitz Interpols ist seit 1989 Lyon. Interpol vereinigt mittlerweile Polizeibehörden aus 188 Ländern[184].

Ziel der IKPO ist u.a. die Sicherstellung und Weiterentwicklung einer umfassenden Unterstützung aller Kriminalpolizeibehörden sowie die Schaffung und der Ausbau von Einrichtungen, die zur Bekämpfung und Verhütung von Straftaten beitragen. Die Besonderheit von Interpol liegt in der Rechtsform als privatrechtlicher Verein. Dementsprechend bilden die Interpol-Statuten die rechtliche Grundlage. Diesen kommt kein innerstaatlicher Gesetzesrang zu, da die Statuten nicht von Regierungsvertretern in Form eines Vertrages mit Ratifizierungsverfahren abgeschlossen wurden, sondern nur durch Vertreter der nationalen Polizeibehörden, so dass auch nur die Polizeibehörden Mitglieder sind und nicht die Staaten. Interpol ist in verschiedenen völkerrechtlichen Abkommen erwähnt und dort als Rechtssubjekt anerkannt.[185]

Zu den wichtigsten Aufgaben von Interpol gehört die internationale Fahndung, wofür mittlerweile ein weltweites Computernetzwerk eingerichtet wurde, auf das die nationalen Zentralstellen – in Deutschland gem. § 3 I BKAG das BKA – sowie z.T. auch lokale Strafverfolgungsbehörden direkten Zugriff haben. Interpol besitzt außerdem eine eigene DNA-Datenbank. Der Austausch von Informationen erfolgt entweder zwischen den Nationalen Büros oder über die Informationszentrale von Interpol, d.h. das Generalsekretariat. Beim Austausch mit den NZB's gelten die innerstaatlichen Regelungen. Aufgrund des regen Datenaustausches gibt es inzwischen auch ein Europäisches Regionalbüro.

---

[184] Stand: September 2011, vgl. Offizielle Website von „Interpol", s. www.interpol.int/.
[185] Mitteleuropäische Polizeiakademie, MEPA-Buch (Stand: November 2008), Allgemeiner Teil, Teil 1B, S. 2.

Der Informationsaustausch zwischen dem BKA und Interpol erfolgt nach nationalen Gesetzes- und Verwaltungsstatuten sowie den Interpol-Statuten.

Seit 1993 werden bei Interpol auch Analysedateien angelegt. Der Vorteil gegenüber Europol besteht darin, dass Interpol nicht nur EU-Staaten als Mitglieder aufweist, sondern weltweit agiert, so dass für die Analyse ein weiteres Spektrum zur Verfügung steht. Jedoch bringt diese weltweite Beteiligung auch Nachteile durch die unterschiedlichen Rechtssysteme mit sich. Es gibt bisher keine völkerrechtliche Verpflichtung zur Anlieferung von Daten, so dass es den Staaten freisteht, welche Daten sie weitergeben. Dadurch sind die Datenbestände lückenhaft und es ist nur eine eingeschränkte Recherche- und Analysetätigkeit möglich.[186] Zudem sind Befugnisse zur Datenverarbeitung in den Statuten nicht festgelegt.

Interpol besitzt eine Internationale Kontrollkommission, welche als internes, aber unabhängiges Organ das Generalsekretariat kontrolliert. Aufgabe des Generalsekretariats ist u.a. die Überprüfung des Datenbestands auf Übereinstimmung mit den Statuten, weshalb es ungehinderten Zugang zu allen Dateien und Unterlagen hat.

Das Interpol-System wird im weiteren Verlauf der Arbeit keine Beachtung finden, da sich das SIS zum führenden Fahndungssystem entwickelt hat, zumindest im Bereich der EU.

Allerdings sei zum gerichtlichen Rechtsschutz soviel gesagt: Der Verwaltungsrechtsweg ist gegen Interpol nicht eröffnet, da keine deutsche Gewalt ausgeübt wird. Es besteht auch keine völkerrechtlich vereinbarte Rechtswegzuweisung. Die Datenschutzregelungen von Interpol sind völkerrechtlich nicht

[186] Milke, S. 122.

bindend und führen daher nur zur Selbstbindung. Letztlich verbleibt nur die nach diesen Regelungen eingerichtete Kontrollkommission. An diese kann sich jedermann wenden und die Rechtmäßigkeit der Datenerhebung und -verarbeitung prüfen lassen.[187]

III. AUSTAUSCH BIOMETRISCHER DATEN AUFGRUND DES BESCHLUSSES ZUR VERTIEFUNG DER GRENZÜBERSCHREITENDEN ZUSAMMENARBEIT

1. ENTSTEHUNG

Am 27.05.2005 wurde in Prüm der *Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreiche Spanien, der französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration*[188], auch *„Vertrag vom Prüm“*, unterzeichnet, welcher dazu gedacht war, die polizeiliche Kooperation zu vertiefen und den Austausch von personenbezogenen Daten, genauer gesagt den Austausch von DNA-Daten, daktyloskopischen Daten und Daten aus Fahrzeugregistern zu fördern. Die entsprechende Durchführungsvereinbarung gem. Art. 44 des Vertrags von Prüm wurde am 05.12.2006 unterzeichnet[189] und Ende Dezember von den Vertragsstaaten angenommen. Der Vertrag von Prüm wurde in der Bundesrepublik Deutschland mit dem *Gesetz zur Umsetzung des*

[187] So Riegel, S. 46 f.
[188] BGBl. II 2006, Nr. 19, S. 628 ff.
[189] Dokument des Rats der Europäischen Union Nr. 5473/07 v. 22.01.2007.

Vertrages vom 27.05.2005 zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreiche Spanien, der französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration vom 10.07.2006[190] und dem (Zustimmungs-) *Gesetz zu dem Vertrag vom 27.05.2005 zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreiche Spanien, der französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration* vom 10.07.2006[191] in das deutsche Recht implementiert.

Bereits in der Präambel des Vertrags von Prüm wurde festgeschrieben, dass der Vertrag in den Rechtsrahmen der EU überführt werden sollte. Da der Vertrag nicht nur die ehemalige dritte, sondern auch die ehemalige erste Säule betrifft, musste eine Aufspaltung des Prümer Vertrages vorgenommen werden. Mit dem Ratsbeschluss[192] wurden 2008 die für die polizeiliche Zusammenarbeit erforderlichen Maßnahmen in den Rechtsrahmen der EU überführt, während für die Bereiche der ehemaligen ersten Säule weiterhin die Bestimmungen des Vertrags von Prüm gelten. Neben dem Ratsbeschluss als Grundlagenbeschluss wurde

[190] BGBl. I 2006 Nr. 32, S. 1458 ff.
[191] BGBl. II 2006 Nr. 19, S. 626 f.
[192] *„Beschluss 2008/615/JI des Rates vom 23. Juni 2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität";* ABl. L 210 v. 06.08.2008, S. 1 ff.

ebenfalls am 23.06.2008 ein Durchführungsbeschluss[193] – ähnlich der Durchführungsvereinbarung vom 05.12.2006 – verabschiedet, welcher die verwaltungsmäßige und technische Umsetzung des Ratsbeschlusses regelt. Einer Umsetzung bedarf der Durchführungsbeschluss nicht. Beide Ratsbeschlüsse sind am 26.08.2008 in Kraft getreten.[194]

Bei dem zunächst geschlossenen Vertrag wurde im Rahmen der Beratungen und beim Zustandekommen des Vertrags kaum ein nationales Parlament[195], geschweige denn das EU-Parlament oder die Kommission, beteiligt. Die Verhandlungen wurden vielmehr lediglich von den Innenministern geführt. Erst im Rahmen der Ratifizierung wurden die nationalen Parlamente eingebunden und hatten dann nur noch die Möglichkeit der Zustimmung oder der Ablehnung des Vertrages. Ebenso wurde das Initiativrecht der Kommission umgangen. Damit wurden aufgrund fast ausschließlich exekutiver Entscheidungen durch die jeweiligen Minister äußerst weitreiche Regelungen zum Austausch personenbezogener Daten getroffen. Aufgrund der Art und Weise des Zustandekommens des Vertrags von Prüm wird dieser auch als „Schengen III" bezeichnet. Schengen II ist ebenfalls unter Umgehung der europäischen Institutionen entstanden. Interessant ist ferner, dass während der Vertragsvorbereitungen zeitgleich am Vorschlag zum Rahmenbeschluss über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit gearbeitet wurde. Anstatt diesen Rahmenbeschluss abzuwarten, welcher im

---

193 *„Beschluss 2008/616/JI des Rates vom 23. Juni 2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität";* ABl. L 210 v. 06.08.2008, S. 12 ff.

194 Mitteleuropäische Polizeiakademie, MEPA-Buch (Stand: November 2010), Allgemeiner Teil, Teil 1B, S. 24.

195 Ausnahmen hierbei waren lediglich Österreich und Finnland, welche über die Verhandlungen umfassend informiert waren, siehe hierzu Kietz / Maurer, Folgen der Prümer Vertragsavantgarde, Diskussionspapier der Forschungsgruppe EU-Integration, S. 9.

Wesentlichen den gleichen gegenständlichen Inhalt hat, wurde der Vertrag von Prüm jedoch im Eiltempo durchgesetzt.[196]

Allerdings stehen dieser kritisch zu betrachtenden Art und Weise des Zustandekommens auch gewisse Vorteile gegenüber. Durch die wenigen Teilnehmerstaaten konnte quasi eine Probesituation geschaffen werden, wodurch auftretende Schwächen und Gefahren des Vertrages noch vor Überführung in den EU-Rahmen untersucht und beseitigt werden können. Weiterer Vorteil des kleinen Teilnehmerkreises war die raschere Bewältigung bestehender Probleme bei der Ausführung des Vertrages.[197]

Im weiteren Verlauf der Arbeit sind die Bestimmungen der ehemaligen ersten Säule nicht weiter relevant, da es ausschließlich um die Verarbeitung biometrischer Daten im Bereich der polizeilichen und justiziellen Zusammenarbeit geht. Es wird daher lediglich auf den Ratsbeschluss 2008/615/JI (nachfolgend nur „Prümer Ratsbeschluss“) sowie 2008/616/JI (nachfolgend nur „Prümer Durchführungsbeschluss“) Bezug genommen, da nur diese im Rahmen der europäischen und internationalen Untersuchung Beachtung finden sollen.

2. REGELUNGEN

Der Vertrag von Prüm und der Prümer Ratsbeschluss bezwecken die Intensivierung und Beschleunigung des Informationsaustausches zwischen den Behörden.[198]

Im Prümer Ratsbeschlusses wird der automatisierte Abruf von biometrischen Daten – DNA-Profile und daktyloskopische Daten (Fingerabdrücke und Handflächen) – sowie der Austausch von Kfz-

[196] Papayannis, in: ZEuS 2/2008, S. 219 (242).
[197] Vgl. hierzu auch Papayannis, in: ZEuS 2/2008, 219 (244).
[198] Arbeitsdok. des Europäischen Parlaments vom 10.04.07, S. 1, einsehbar unter: www.europarl.europa.eu/meetdocs/2004_2009/documents/dt/660/660824/660824de.pdf

Daten ermöglicht, wobei letztere hier ohne Belang sind. Ursprünglich lief der Vorschlag der Kommission sogar auf sechs Daten hinaus.[199]

Die Übermittlung der Informationen erfolgt nach den für den Grundsatz der Verfügbarkeit geltenden Bedingungen. Dies bedeutet, dass ein Strafverfolgungsbeamter, welcher zur Erfüllung seiner Aufgaben Informationen benötigt, diese von anderen Mitgliedstaaten erhalten kann und dass diese Informationen von den anderen Mitgliedstaaten bereitgestellt werden (Weiteres zum Grundsatz der Verfügbarkeit, vgl. unten Pkt.IV. 1.). Des Weiteren ist die Schwedische Initiative (vgl. Pkt. IV. 2.) zu beachten, welche die Regeln festlegt, nach denen ein rascher Austausch von Informationen zu erfolgen hat.[200]

Der Austausch erfolgt durch direkten Zugriff auf die jeweiligen mitgliedstaatlichen Dateien unter Vernetzung der nationalen Datenbanken, d.h. die Vertragsparteien gewährleisten das Vorhandensein eines Fundstellen- oder auch Indexverzeichnisses. Dadurch soll eine erhebliche Beschleunigung im Vergleich zu den bisherigen Verfahren gewährleistet werden.

Der Prümer Ratsbeschluss differenziert hinsichtlich der Voraussetzungen und Verfahren nach der Art der ausgetauschten Daten, d.h. es gibt für DNA, Fingerabdrücke und Fahrzeugdaten jeweils eigene Voraussetzungen.

Die Verzeichnisse enthalten hinsichtlich der DNA nur das aus dem nicht kodierenden DNA-Teil ermittelte Muster sowie die entsprechende Kennung und damit – ebenso wie bei den Fingerabdrücken – keine personalisierten Daten. Ein Abgleich wird mithilfe des bekannten Hit-/No Hit-Verfahrens durchgeführt. Dabei werden ausschließlich anonyme Profile verglichen. Stellt

[199] Böse, S. 49.
[200] vgl. Erwägungsgründe Nr. (4) und (6).

man hierbei einen Treffer fest, können die abfragenden Mitgliedstaaten den Datei führenden Mitgliedstaat mithilfe der Kennung um weitere Informationen bitten. Die Übermittlung und der Empfang erfolgen dann nach innerstaatlichem Recht des ersuchenden Staates, insbesondere nach den Vorschriften über die internationale Rechtshilfe in Strafsachen. Dadurch muss der ersuchende Staat nur seine eigenen nationalen Vorschriften kennen, was den Austausch erheblich vereinfacht, Art. 5 und 10 Prümer Ratsbeschluss. Der Austausch der Informationen erfolgt über die nationale Kontaktstelle.

Art. 7 Prümer Ratsbeschluss eröffnet den Mitgliedstaaten zusätzlich die Möglichkeit, dass der ersuchte Staat um Gewinnung molekulargenetischen Materials und Übermittlung des DNA-Musters gebeten werden kann. Vorausgesetzt wird dabei, dass die Bedingungen für die Gewinnung und Übermittlung nach dem Recht des ersuchenden und des übermittelnden Staates vorliegen, Art. 7 lit. b) und c) Prümer Ratsbeschluss.

Nach Art. 8 Prümer Ratsbeschluss sind Fundstellendatensätze aus dem Bestand der daktyloskopischen Identifizierungssysteme zu errichten, auf welche gem. Art. 9 Prümer Ratsbeschluss Zugriff zu gestatten ist. Auch hier erfolgt ein automatisierter Vergleich, welcher bei einem Treffer jedoch zunächst von dem ersuchenden Staat endgültig zuzuordnen ist, bevor die Übermittlung weiterer personenbezogener Daten stattfindet.

Weiterer Inhalt des Prümer Ratsbeschlusses sind außerdem allgemeine Bestimmungen zum Datenschutz. Demnach gewährleistet jeder Mitgliedstaat ein Mindestniveau auf Basis des Europaratsübereinkommens von 1981 unter Beachtung der Empfehlung des Ministerkomitees des Europarats Nr. R (87) 15 von 1987[201]. Eine Übermittlung darf demnach erst dann erfolgen, wenn

[201] Näheres zum Abkommen und zur Empfehlung, siehe Teil D.

das Vorliegen der Voraussetzungen durch den Rat der Europäischen Union festgestellt worden ist, Art. 25 II Prümer Ratsbeschluss. Die Feststellung wird in Übereinstimmung mit den jeweiligen unabhängigen Kontrollinstanzen getroffen.[202] Für die damals bereits am Vertrag beteiligten Staaten gilt Abs. 2 nicht, d.h. dass der Austausch der Daten mit Umsetzung der Vorschriften möglich ist, vgl. 25 III. Der Prümer Ratsbeschluss stellt außerdem in den Art. 26-31 weitere spezielle datenschutzrechtliche Anforderungen auf, u.a. zur Zweckbindung, Datenqualität und Datensicherheit, welche den Besonderheiten des grenzüberschreitenden Online-Zugriffs Rechnung tragen. Da – bedingt durch den Online-Zugriff – keine vorherige Prüfung möglich ist, wird der Datenschutz im Prümer Ratsbeschluss insbesondere einer nachträglichen Kontrolle (Dokumentation und Protokollierung) unterstellt, vgl. hierzu Art. 30 Prümer Ratsbeschluss. Regelungen zur Datensicherheit sind im Prümer Durchführungsbeschluss zu finden.

Kritikwürdig ist allerdings, dass trotz der umfangreichen Protokollierungsvorschriften des Art. 30 Prümer Ratsbeschluss die Bundesregierung keine statistischen Informationen über die Anzahl der bearbeiteten Anfragen, über die von Deutschland gestellten Ersuchen um Gewinnung und Untersuchung molekulargenetischen Materials im Ausland sowie über die Zahl der Zufallstreffer beim Abgleich der DNA-Datenbanken geben kann.[203]

[202] Schaar, in: DuD 2006, 691 (693) zur alten Fassung des Vertrags von Prüm.
[203] S. „Antwort der Bundesregierung auf die Kleine Anfrage BT-Drs. 16/14120 – Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Polizeizusammenarbeit“, BT-Drs. 16/14150 vom 22.10.2009, S. 3 f.

Dass ein solcher Abgleich jedoch sinnvoll ist, lässt sich anhand der folgenden Bilanz betreffend den Austausch von DNA-Daten mit Österreich im Zeitraum vom 06.12.06 bis 30.09.09 beurteilen[204]:

Spur-Person	1421
Spur-Spur	1295
Person-Spur	419
Gesamt	3135

Im daktyloskopischen Bereich lag die Anzahl der Treffer im Zeitraum vom 01.06.2007 bis 30.09.2009 (Abgleich Österreich und Deutschland) in Österreich bei 2143 Treffern und in Deutschland bei 325 Treffern.[205]

Betrachtet man jedoch die Deliktarten, bei welchen ein Treffer erzielt wurde, wird einem das Ausmaß des Datenaustausches bewusst. Nicht zu beanstanden ist ein Austausch, bei dem es um Hehlerei, Straftaten gegen das Leben, Gefährliche Körperverletzung, Misshandlung Schutzbefohlener etc. geht. Kritik verdient jedoch die Tatsache, dass auch bei banalen Beleidigungen

[204] S. hierzu „Antwort der Bundesregierung auf die Kleine Anfrage BT-Drs. 16/14120 – Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Polizeizusammenarbeit", BT-Drs. 16/14150 vom 22.10.2009, S. 4.

[205] „Antwort der Bundesregierung auf die Kleine Anfrage BT-Drs. 16/14120 – Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Polizeizusammenarbeit", BT-Drs. 16/14150 vom 22.10.2009, S. 4.

sowie bei der Vereitelung von Zwangsvollstreckung Datenabgleiche durchgeführt werden. Auch u. U. geringe Straftatbestände wie Sachbeschädigung sind hiervon erfasst, wobei nicht mitgeteilt wurde, wie hoch der betreffende Schaden war.[206] Ein solches Ausmaß an Datenaustausch kann nur durch die Erfassung von Katalogtaten beschränkt werden (Genaueres, s. Teil D).

IV. WEITERE RECHTSAKTE MIT BEZUG AUF DEN AUSTAUSCH BIOMETRISCHER DATEN

In Bezug auf den Austausch von Daten existieren noch zahlreiche weitere Abkommen, aber auch Vorschläge für einen rascheren Austausch. Auf die Darstellung der bilateralen Verträge im europäischen Bereich wird verzichtet, da der Prümer Ratsbeschluss nun umfassend für alle Mitgliedstaaten Geltung beansprucht.

1. VORSCHLAG FÜR EINEN RAHMENBESCHLUSS DES RATES VOM 12.10.2005 ÜBER DEN AUSTAUSCH VON INFORMATIONEN NACH DEM GRUNDSATZ DER VERFÜGBARKEIT

Zur Umsetzung des *Haager Programms zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union*[207] hat die Kommission gem. Pkt. III.2.1. die Aufgabe, zur Verwirklichung des Verfügungsgrundsatzes beizutragen und einen dementsprechenden Vorschlag auszuarbeiten. Nach dem Haager

[206] Tabelle der Treffer gegliedert nach Delikten, unter „Antwort der Bundesregierung auf die Kleine Anfrage BT-Drs. 16/14120 – Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Polizeizusammenarbeit“, BT-Drs. 16/14150 vom 22.10.2009, S. 5.
[207] ABl. C 53 v. 03.03.2005, S. 1 ff.

Programm soll der Umstand, dass Daten eine Grenze überschreiten, nicht länger von Belang sein.[208] Dementsprechend hat die Kommission am 12.10.2005 einen *Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit*[209] vorgelegt. Dieser ist auch jetzt noch relevant, da die Überlegungen dieses Vorschlages Eingang in den Prümer Ratsbeschluss gefunden haben.

Der Vorschlag enthält Regelungen zur raschen und wirksamen Übermittlung von strafrechtsrelevanten Informationen vor Einleitung einer Strafverfolgungsmaßnahme. Er enthält u.a. Vorschriften zur automatisierten Übermittlung von Informationen, welche gerade aufgrund des unterschiedlichen Datenschutzniveaus in den Mitgliedstaaten zu kritisieren sind. Der Verfügbarkeitsgrundsatz ist vorerst für die Übermittlung von DNA-Mustern, Fingerabdrücken, Verbindungsdaten und Kfz-Halterdaten vorgesehen, da für diese bereits Datenbanken zur Verfügung stehen.[210] Die Verwendung der Daten ist ausschließlich für Ermittlungen vorgesehen. Soll das Ergebnis als Beweis im anschließenden Strafverfahren verwendet werden, bedarf es hierzu einer Einwilligung durch den angerufenen Staat, vgl. Art. 13 II.

Der Verfügbarkeitsgrundsatz verlangt zudem, dass an die zwischenstaatliche Übermittlung keine strengeren Bedingungen als an die innerstaatliche Übermittlung gestellt werden dürfen; dazu gehört auch die Bereitstellung eines möglicherweise vorhandenen Online-Zugangs zu den Informationen. Allerdings kann der ersuchte Staat verbindliche Verwendungsbedingungen stellen, Art. 12 II. Auch besteht gem. Art. 14 I die Möglichkeit, die Bereitstellung der Informationen unter den dort genannten

[208] Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, S. 7; Böse, S. 46.
[209] Kommissionsdokument Nr. 2005/0207 (CNS) = KOM(2005) 490 endg. vom 12.10.2005.
[210] Siehe Böse, in: EuZ 4/2007, S. 62 (ebd.).

Voraussetzungen zu verweigern. Bedeutsam ist hierbei, dass eine Verweigerungsmöglichkeit auch im Hinblick auf den Schutz der Grundrechte und der Grundfreiheiten eines Betroffenen möglich ist, vgl. Art. 14 I lit. d). Diese Einschränkung findet sich weder in der Datenschutzkonvention des Europarats noch in der Datenschutzrichtlinie der EG.

Wenn für die betreffenden Dateien ein Online-Zugang vorhanden ist, wird ein automatisierter Abruf durchgeführt. Sind die Daten dagegen elektronisch noch nicht verfügbar, soll zumindest ein Zugriff auf Indexdateien gewährleistet werden. Sollte der Abgleich erfolgreich sein, soll auf Ersuchen binnen zwölf Stunden eine Antwort erfolgen.

Um das Datenschutzniveau anzugleichen – was für den Austausch auf Basis dieses Rahmenbeschlusses unabdingbar ist –, wurde ein Vorschlag für einen *Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*[211], vorgelegt (vgl. auch Art. 8). Der Europäische Datenschutzbeauftragte hat darauf hingewiesen, dass der Rahmenbeschluss über Austausch von Informationen nach dem Grundsatz der Verfügbarkeit erst nach Erlass des Rahmenbeschluss für den Datenschutz erlassen werden sollte.[212] Unabhängig von einem datenschutzrechtlichen Rahmenbeschluss enthält auch der Vorschlag für den Rahmenbeschluss über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit Vorgaben zur Rückverfolgbarkeit und zur Transparenz des Informationsaustausches sowie einem Auskunftsrecht des Betroffenen, vgl. Art 16.

---

[211] ABl. L 350 v. 30.12.2008, S. 60 ff.
[212] Stellungnahme des Europäischen Datenschutzbeauftragen, s. ABl. C 116 v. 17.05.06, S. 8 Pkt. 14.

Der Vorschlag knüpft an andere Initiativen zur Vereinfachung des Datenaustauschs an, genauer gesagt an den Vertrag von Prüm und an den etwas später erlassenen *Rahmenbeschluss 2006/960/JI des Rates über die Vereinfachung des Informationsaustausch zwischen den Strafverfolgungsbehörden*[213] vom 18.12.2006 (s. Pkt. 2.). Hierbei ist zu beachten, dass die Schwedische Initiative und der Vertrag von Prüm bzw. der jetzige Prümer Ratsbeschluss den Informationsaustausch im Rahmen eines strafrechtlichen Ermittlungsverfahrens regeln, während der Grundsatz der Verfügbarkeit sich auf das Stadium vor der Einleitung einer Strafverfolgungsmaßnahme beschränkt.

Der Vorschlag blieb bislang ohne Erfolg.[214]

2. SCHWEDISCHE INITIATIVE

Am 18.12.2006 wurde der *Rahmenbeschluss 2006/960/JI des Rates über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union*[215] – auch „Schwedische Initiative" - verabschiedet. Der Rahmenbeschluss stellt eine Weiterentwicklung von Art. 39 SDÜ dar und verfolgt den raschen und wirksamen Austausch von Informationen und Kenntnissen, welche für die Durchführung eines Straf- oder Ermittlungsverfahrens erforderlich sind, Art. 1 der Initiative.

Die Schwedische Initiative bildet gewissermaßen einen Grundsatz-Rahmen für alle künftigen Regelungen im Bereich des Informationsaustausches, auch für den Prümer Ratsbeschluss, vgl. Erwägungsgrund (6) des Prümer Ratsbeschlusses.

---

213 ABl. L 386 v. 29.12.2006, S. 89 ff.; vgl. hierzu Pkt. b).
214 Stand: 27.08.2011.
215 ABl. L 386 v. 29.12.2006, S. 89 ff.; In Kraft seit 30.12.2006; Berichtigung, s. ABl. L 75 vom 15.03.2007, S. 26.

Die Initiative folgt ebenso dem in Pkt. 1. genannten Vorschlag vom Prinzip der Verfügbarkeit der Daten und überschneidet sich daher insoweit mit diesem. Während die Schwedische Initiative die Übermittlung nach den bestehenden Vorschriften – allerdings durch zeitliche Grenzen und bestimmte Übermittlungskanäle rascher abgewickelt – vorsieht, geht der Vorschlag zum Rahmenbeschluss über den Grundsatz der Verfügbarkeit weiter und verlangt die Einrichtung eines Online-Zugangs zu bestehenden Daten. Dadurch besteht natürlich die Gefahr der Umgehung der nationalen Übermittlungsvorschriften.

Nach der Schwedischen Initiative erstreckt sich der Austausch auf Informationen aller Art, welche bei den Strafverfolgungsbehörden vorhanden bzw. bei anderen Behörden oder privaten Stellen für die Strafverfolgungsbehörden verfügbar sind (vgl. Art. 1 II 1 i.V.m. S. 2 lit. d). Der Rahmenbeschluss wird vom Grundsatz der Gleichbehandlung getragen, d.h. für die ersuchenden Mitgliedstaaten dürfen keine strengeren Bedingungen für die Zur-Verfügung-Stellung und Anforderung von Informationen gelten als auf nationaler Ebene, vgl. Art. 3 III.

Die Initiative setzt bei der Übermittlung von Daten zeitliche Grenzen. Ist eine elektronische Datenbank vorhanden, muss auf dringende Ersuchen binnen acht Stunden (Art. 4 I), auf nicht dringende Ersuchen binnen einer Woche geantwortet werden, vgl. Art 4 III. Der Begriff der Dringlichkeit wird in der Schwedischen Initiative nicht konkretisiert. Erst die Leitlinien des Rates der Europäischen Union geben hierüber genauere Auskunft. Danach muss „von Fall zu Fall geprüft werden, ob eine Dringlichkeit gegeben ist, damit vermieden wird, dass der Begriff der Dringlichkeit abgewertet wird“[216]. Dringende Fälle sind somit

[216] Rat der Europäischen Union, „Leitlinien für die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates vom 18.Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den

gegeben, wenn die Informationen zur „Abwendung einer Gefährdung des Lebens oder der körperlichen Unversehrtheit von Personen oder der Gefahr einer schweren Sachbeschädigung [oder zur] Herbeiführung oder Beendigung einer Entscheidung über einen Freiheitsentzug (sofern eine solche Entscheidung rasch ergehen muss) [oder zur] Verhinderung des Verlusts von Informationen, die für die weiteren Phasen der Ermittlung wichtig sind", herangezogen werden.[217] Solche Situationen liegen bspw. bei Geiselnahme, schweren Straftaten, Vermissten usw. vor.[218] Ist eine elektronische Datenbank nicht vorhanden, ist zur Beantwortung der Anfrage eine zeitliche Grenze von 14 Tagen gesetzt, vgl. Art. 4 IV .

Die Kommunikation der Informationen erfolgt u.a. über SIRENE, die Verbindungsbeamten von Europol und die Nationalen Zentralbüros von Interpol.[219] Die Zur-Verfügung-Stellung der Informationen darf nach Art. 10 des Rahmenbeschlusses verweigert werden, wenn die Beantwortung für die verfolgten Zwecke irrelevant ist oder in keinem Verhältnis zu diesen steht bzw. wenn

---

Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union" vom 17.12.2010, S. 7.

[217] Rat der Europäischen Union, „Leitlinien für die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates vom 18.Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union" vom 17.12.2010, S. 7.

[218] vgl. beispielhafte Aufzählung, in: Rat der Europäischen Union, „Leitlinien für die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates vom 18.Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union" vom 17.12.2010, S. 7.

[219] Rat der Europäischen Union, „Leitlinien für die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates vom 18.Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union" vom 17.12.2010, S. 5.

die verfolgte Straftat mit einer Freiheitsstrafe von weniger als einem Jahr bedroht ist.[220]

Allerdings wird bei der Schwedischen Initiative für bedenklich gehalten, dass die Daten nicht nur für den Übermittlungszweck, d.h. zum alleinigen Abgleich der Daten, verwendet werden dürfen, sondern darüber hinaus zur Gefahrenabwehr und weiteren Zwecken. Dies wird allerdings dadurch relativiert, dass nach der Schwedischen Initiative die Verwendung der Informationen als Beweismittel von der Zustimmung des übermittelnden Staates abhängt.[221] Des Weiteren kann der ersuchte Staat nach Maßgabe seines innerstaatlichen Rechts Bedingungen an die Verwendung der Informationen knüpfen, vgl. Art. 9 IV 1.

In der Bundesrepublik Deutschland wurde die Schwedische Initiative gesetzlich bislang nicht umgesetzt.[222]

[220] S. auch Rat der Europäischen Union, „Leitlinien für die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates vom 18.Dezember 2006 über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union“ vom 17.12.2010, S. 8.
[221] Böse, S. 50.
[222] Stand: 23.08.2011.

TEIL D Vereinbarkeit des ePasses und der Prüm-Regelungen mit dem Völkerrecht

A. EINFÜHRUNG

I. DIE ENTWICKLUNG DES DATENSCHUTZES IM INTERNATIONALEN BEREICH

In keinem der völkerrechtlichen Menschenrechtskataloge findet sich bislang ein ausdrückliches Recht auf Datenschutz. Anknüpfungspunkt kann daher nur das Recht auf Achtung des Privatlebens sein, welches sich bereits in Art. 12 der Allgemeinen Erklärung der Menschenrechte von 1948 und in Art. 17 des Internationalen Paktes für Bürgerliche und Politische Rechte von 1966 findet. Aufgrund der ausführlicheren Rechtsprechung des EGMR zur EMRK sind diese Menschenrechtskataloge jedoch zu vernachlässigen.

Obwohl Datenschutz erst seit den 70er Jahren problematisiert wird, existieren Formen des Datenschutzes bereits seit vielen Jahrhunderten. So wird bereits um das 4. Jahrhundert v. Chr. im Eid des Hippokrates die Verschwiegenheitspflicht des Arztes über seine Patienten gefordert, was in etwa der heutigen Verpflichtung auf das Datengeheimnis entspricht. Kurioserweise hat das heutige Datenschutzrecht in den USA seinen Ausgang genommen, als die damalige Regierung unter John F. Kennedy eine große EDV-Datenbank zur Verbesserung des staatlichen Informationswesens aufbauen wollte, in der jeder Bürger erfasst werden sollte. Die Bürger sträubten sich gegen diesen Eingriff in ihr „right to be alone“. Der Kongress erkannte daraufhin die Notwendigkeit der Einführung gesetzlicher Grundlagen für die Verarbeitung

personenbezogener Daten und verabschiedete 1974 den „Privacy Act".

Aufgrund der aufkommenden Diskussionen in den 70er Jahren hat am 23.09.1980 die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) eine *Empfehlung des Rates über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten*[223] verabschiedet. Die Leitlinien treffen Regelungen zum Austausch von Daten sowohl im öffentlichen als auch im privaten Sektor und sind – anders als die DSK – nicht auf automatisierte Daten beschränkt. Diese Leitlinien sind nicht verbindlich, sollen jedoch den Datenschutz vereinheitlichen und insbesondere Hemmnisse für den grenzüberschreitenden Datenverkehr abbauen.[224] Der Inhalt der Leitlinien unterscheidet sich nicht wesentlich von dem der DSK, weshalb die Leitlinien in den weiteren Ausführungen keine große Bedeutung einnehmen.

1976 nahm der Generalsekretär der Vereinten Nationen zum Schutz der Rechte des Betroffenen vor den Gefahren der computerisierten Datenverarbeitung Stellung und machte Vorschläge für den Entwurf internationaler Datenschutzstandards.[225] 1985 hat dann die Menschenrechtskommission der Vereinten Nationen einen Richtlinien-Entwurf zum Datenschutz ausgearbeitet. Nach kleineren Änderungen wurden die Richtlinien[226] am 14.12.1990 durch die Generalversammlung der Vereinten Nationen

---

223 Einsehbar unter www.datenschutz-berlin.de/content/veroeffentlichungen/a-z; „Internationaler und Europäischer Datenschutz", S. 15 ff.
224 Genz, S. 13.
225 Unger, S. 71.
226 *„Richtlinien betreffend personenbezogene Daten in automatisierten Dateien"* vom 14.12.1990, einsehbar unter www.datenschutz-berlin.de/content/veroeffentlichungen/a-z „Internationaler und Europäischer Datenschutz", S. 7 ff.;

angenommen.[227] Diese Richtlinien haben jedoch nur Empfehlungscharakter und sollen den Mitgliedstaaten als Modell zu einem einheitlicheren Datenschutz verhelfen.[228] Bemerkenswert ist, dass die Richtlinien als erstes internationales Dokument die Einrichtung von unabhängigen Kontrollinstanzen vorsahen (Art. 8 UNO-RL).[229]

Eine weitere internationale Regelung stellt die Datenschutzkonvention dar, welche im Folgenden näher erläutert wird.

II. DIE RELEVANTEN VÖLKERRECHTLICHEN REGELUNGEN

Bevor mit der Überprüfung der Regelungen begonnen wird, werden zunächst die relevanten völkerrechtlichen Regelungen erörtert.

1. DIE EUROPÄISCHE MENSCHENRECHTSKONVENTION (EMRK)

Die EMRK ist ein völkerrechtlicher Vertrag zwischen den Mitgliedstaaten des Europarates, welcher am 04.11.1950 unterzeichnet wurde und am 03.09.1953 in Kraft trat.[230] Zwischenzeitlich wurde die EMRK durch zahlreiche Zusatzprotokolle ergänzt.[231] In der EMRK ist ein Grundrechtsschutz vorgesehen, welcher als Mindeststandard nicht

[227] Resolution of the General Assembly at its 68th plenary meeting – A/RES/45/95; Orantek, S. 21; Genz S. 12.
[228] S. Genz, S. 12.
[229] Weitere geschichtliche Hintergründe zum internationalen Datenschutz, vgl. Ellger, S. 147 ff., 460 ff.
[230] S. Heselhaus/Nowak, § 1 Rn. 30.
[231] derzeit 14 Zusatzprotokolle (Stand: August 2011).

unterschritten werden darf. Aufgrund der Tatsache, dass die EMRK bereits sehr früh entwickelt worden ist und auch nur Konturen eines Grundrechts vorgibt, sieht sie der EGMR[232] als „living instrument", welches sich an die technischen, sozialen, wirtschaftlichen und politischen Gegebenheiten anpasst.

Bei Verletzungen der Konventionsrechte besteht unter bestimmten Voraussetzungen die Möglichkeit der Überprüfung vor dem Europäischen Gerichtshof für Menschenrechte (EGMR) in Straßburg. Dem Betroffenen steht hierbei gem. Art. 34 EMRK ein Individualbeschwerderecht zum EGMR zu. Wie anhand der Entscheidungen erkennbar sein wird, gab es bis zum 01.11.1998[233] zwei mit der Rechtsprechung betraute Organe: den EGMR und die Europäische Kommission für Menschenrechte (EKMR). Die Kommission war dem EGMR vorgeschaltet und entschied vorab über die Zulässigkeit der Klage zum EGMR. Durch das 11. Zusatzprotokoll wurde die EKMR jedoch abgeschafft, so dass der EGMR nun das einzige Rechtsschutzorgan ist.[234]

2. DIE DATENSCHUTZKONVENTION DES EUROPARATS (DSK)

Die Datenschutzkonvention des Europarates wurde am 28.01.1981 in Straßburg beschlossen und trat nach Ratifikation durch fünf Mitgliedstaaten am 01.10.1985 in Kraft.[235] Nach aktuellem Stand haben 43 Mitgliedsstaaten des Europarats, darunter alle

[232] EGMR, Urteil vom 28.04.1978 – *Tyrer ./. Vereinigtes Königreich*, § 31.
[233] vgl. SEV Nr. 155, „11. Zusatzprotokoll zur Konvention zum Schutze der Menschenrechte und Grundfreiheiten über die Umgestaltung der durch die Konvention eingeführten Kontrollmechanismen vom 11.05.1994"; s. auch BGBl. II 1995 Nr. 22, S. 578 ff.
[234] Herdegen, S. 15.
[235] Bekanntmachung über das Inkrafttreten des Abkommens vom 26.09.85, in: BGBl. 1985 Nr. 34, S. 1134 f.

Mitgliedstaaten der EU, das Übereinkommen ratifiziert.[236] Für den Transfer in Drittstaaten verabschiedete der Europarat am 08.11.2001 das *Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr*[237], welches ebenfalls nach Ratifikation durch fünf Mitgliedstaaten am 01.07.04 in Kraft trat und mittlerweile durch 30 Mitgliedsstaaten des Europarats ratifiziert wurde.[238] Die Datenschutzkonvention geht auf die Empfehlung Nr. 509 des Ministerkomitees von 1968 zurück, welches untersuchte, ob die EMRK angesichts der technischen Entwicklungen den Schutz der Privatsphäre noch gewährleisten kann.[239]

Die Konvention ist ein „non-self-executing treaty", d.h. das Übereinkommen ist für die Beitrittsstaaten verbindlich, wohingegen der Einzelne keine Rechte aus dem Übereinkommen geltend machen kann.[240] Unmittelbare Rechte kann der Einzelne erst aus dem nationalen Recht ableiten, soweit das Übereinkommen umgesetzt wurde. Des Weiteren enthält die DSK nur einen gemeinsamen Mindestgehalt an Datenschutzvorschriften. Um einen weitgehenden Standard im Datenschutz zu sichern, steht der Beitritt auch Nicht-Mitgliedsstaaten des Europarats offen, vgl. Art. 23 DSK, wobei hiervon bislang kein Gebrauch gemacht wurde.

---

[236] Stand: August 2011, vgl. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=10/11/2010&CL=GER.
[237] SEV Nr. 181.
[238] Stand: August 2011, vgl. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=8&DF=10/11/2010&CL=GER.
[239] "*Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"* (nachfolgend nur noch "Explanatory Report ETS No. 108") Nr. 4; detaillierte Darstellung der Entwicklung, s. Ellger, S. 460 ff.
[240] Explanatory Report No. 108, Nr. 38.

Allerdings kann nicht außer Acht gelassen werden, dass die Datenschutzkonvention das erste völkerrechtliche Instrument zur Vereinheitlichung des Datenschutzes darstellt. Auch wenn die DSK nur ein Minimum an Vorschriften darstellt, so zeigt dies doch den Willen, auf den Schutz der Rechte und Grundfreiheiten des Menschen einzugehen (vgl. auch Präambel der DSK). Zu berücksichtigen ist insbesondere, dass der Europarat zum damaligen Zeitpunkt schon aus 21 Staaten bestanden hat, weswegen eine Einigung auf einen gemeinsamen Standard als bemerkenswerte Leistung anzuerkennen ist, insbesondere zu einem Zeitpunkt, an welchem der Datenschutz gerade einmal angefangen hat, Bedeutung zu erlangen.

Aufgrund des gewählten Minimalkonsenses entstanden mitunter leider auch sehr weit bzw. abstrakt gefasste Vorschriften, was insbesondere anhand der unbestimmten Begriffe – wie z.B. „nach Treu und Glauben verarbeitet" oder „wenn nötig" – in Art. 5 DSK deutlich wird.[241] Des Weiteren gibt es zahlreiche Möglichkeiten, Ausnahmen vom Übereinkommen vorzusehen, vgl. Art 3 und Art. 9 DSK.

Aufgrund der speziellen Problematik der Biometrie und der damit verbundenen Eingriffe in das Recht auf Datenschutz hat das T-PD (Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data) im Jahre 2005 einen Sachstandsbericht zur Anwendung der Prinzipien der DSK in Bezug auf die Sammlung und Verarbeitung von biometrischen Daten *(„progress report on the application of the principles of Convention 108 to the collection and processing of*

[241] So auch Kübler, S. 42.

biometric data“)[242] verabschiedet, welcher in Pkt. B. II. und C. II. ebenfalls einbezogen wird.

Zur Konkretisierung der DSK hat das Ministerkomitee zahlreiche Empfehlungen zu speziellen Bereichen erlassen.

3. DIE EMPFEHLUNGEN DES MINISTERKOMITEES

Die Empfehlungen des Ministerkomitees sind nicht verbindlich. Im Gegensatz zur DSK, welche nur allgemeine Regelungen bereitstellt, sollen die Empfehlungen v.a. solche Tätigkeitsbereiche konkretisieren, welche besonders intensive und persönlichkeitsrechtsgefährdende Eingriffe bereithalten, z.B. der Polizeibereich oder der Austausch von DNA-Daten. Aufgrund dieser konkretisierenden Eigenschaft der Empfehlungen werden diese im Zusammenhang mit der DSK in Pkt. C. II. dargestellt.

Am 17.09.1987 wurde vom Ministerkomitee des Europarates die „*Empfehlung Nr. (87) 15 des Ministerkomitees des Europarats an die Mitgliedstaaten über die Nutzung von personenbezogenen Daten im Polizeibereich*“[243] verabschiedet. Zur Bedeutung dieser Empfehlung gab es mehrere Auswertungen[244] durch die „Project Group on Data Protection (CJ-PD)“, zuletzt im Jahr 2002. 1995 gab es zudem

[242] Verabschiedung des Berichts auf dem 924. Treffen des Ministerrates im April 2005, einsehbar unter https://wcd.coe.int/wcd/ViewDoc.jsp?Ref=CM%282005%2943&Language=lanEnglish&Site=COE&BackColorInternet=DBDCF2&BackColorIntranet=FDC864&BackColorLogged=FDC864, Appendix II.

[243] Dokument abrufbar unter https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=276604&SecMode=1&DocId=694350&Usage=2 (englisch).

[244] S. unter www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%20legal%20instruments/11Evaluation%2887%2915_EN.pdf; www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%20legal%20instruments/12Evaluation%2887%2915_EN.pdf und www.coe.int/t/e/legal_affairs/legal_co-operation/data_protection/documents/international%20legal%20instruments/13Evaluation%2887%2915_EN.pdf (englisch).

Bestrebungen, die Rec. R (87) 15 zu einer Konvention auszuarbeiten und die Anwendung der Empfehlung voranzutreiben; dies geschah durch die *„Recommendation 1181 (1992) on police co-operation and protection of personal data in the police sector"*[245]. Die Projektgruppe Datenschutz (CJ-PD) hat jedoch die Parlamentarische Versammlung darüber informiert, dass die Rec. R (87) 15 einen adäquaten Schutz für personenbezogene Daten im Polizeibereich enthalte und dass kein Bedürfnis für eine Korrektur der Rec. R (87) 15 bestehe.[246] Die Empfehlung ist für den Prümer Ratsbeschluss anwendbar. Gegenüber der Empfehlung wurden ferner von einigen Mitgliedstaaten Vorbehalte ausgesprochen. Die Vorbehalte treffen lediglich die Punkte 2.1 bis 2.4 (mit Ausnahme der Schweiz, welche bezüglich der Befolgung der Empfehlung noch keine konkrete Erklärung abgegeben hat), folglich also die Bestimmungen zur Sammlung von Daten.

Von Bedeutung ist zudem die *„Empfehlung Nr. R (92) 1 des Ministerkomitees über die Anwendung der DNA-Analyse im Rahmen der Strafrechtspflege"*[247], welche am 10.02.92 vom Ministerkomitee verabschiedet wurde. Natürlich gilt diese Empfehlung aufgrund ihres speziellen Charakters nur für den Prümer Ratsbeschluss. Nach Empfehlung 7 ist die Sammlung und Anwendung von DNA-Analysen in Einklang mit der DSK und speziell mit der Empfehlung R (87) 15 durchzuführen. Um diesen Einklang

---

[245] s. http://assembly.coe.int/Main.asp?link=/Documents/AdoptedText/ta92/EREC1181.htm.

[246] s. Doc. 7254 vom 15.02.1995 unter http://assembly.coe.int/Mainf.asp?link=/Documents/WorkingDocs/Doc95/EDOC7254.htm.

[247] *"Recommendation No. R (92) 1 of the committee of ministers to member states on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system"*, einsehbar unter: https://wcd.coe.int/wcd/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=1518265&SecMode=1&DocId=601410&Usage=2.

herzustellen, ist es erforderlich, die Bestimmungen der Empfehlung (92) 1 mit der DSK und der Rec. R (87) 15 zu verbinden und daraus die Erfordernisse für den Prümer Ratsbeschluss abzuleiten. Trotz der Unverbindlichkeit der Empfehlung wurden Vorbehalte ausgesprochen, insbesondere hat sich Dänemark die Anwendbarkeit im Gesamten und die Staaten Deutschland, die Niederlande und Norwegen haben sich das Recht vorbehalten, möglicherweise Empfehlung (nachfolgend „Principle“) Nr. 8 nicht anzuwenden.

III. DIE BINDUNG DER E-PASS- UND DER PRÜM-REGELUNGEN AN DIE VÖLKERRECHTLICHEN BESTIMMUNGEN DER EMRK, DER DSK UND DER EMPFEHLUNGEN DES MINISTERKOMITEES

Auch wenn es sich bei den ePass- und den Prüm-Regelungen um solche des europäischen Rechts handelt, sind dennoch auch bestimmte völkerrechtliche Vorschriften zu beachten. Nach der Änderung der Verordnung (EG) Nr. 2252/2004 enthält Art. 1a II der ePass-Verordnung die Vorgabe, dass die biometrischen Identifikatoren „im Einklang mit den in der Konvention des Europarats zum Schutz der Menschenrechte und Grundfreiheiten […] verankerten Garantien“ zu erfassen sind. Sowohl der Erwägungsgrund (19) als auch Art. 25 I Prümer Ratsbeschluss verlangen, dass jeder Mitgliedstaat für die Verarbeitung seiner personenbezogenen Daten das Mindestniveau des *Übereinkommens des Europarats vom 28.01.1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten*[248], des Zusatzprotokolls zum Übereinkommen vom

[248] SEV Nr. 108.

08.11.2001[249] (nachfolgend DSK-ZP) sowie der *Empfehlung R (87) 15 des Ministerkomitees des Europarats an die Mitgliedstaaten über die Nutzung personenbezogener Daten im Polizeibereich*[250] (nachfolgend „Rec. R (87) 15“) gewährleistet. Damit sind die Vertragsparteien nach Art. 26 des Wiener Übereinkommens über das Recht der Verträge (pacta sunt servanda) gebunden. Damit nehmen bereits sowohl die Regelungen zum ePass als auch der Prümer Ratsbeschluss Bezug auf die völkerrechtlichen Vorgaben, weshalb sich die Frage stellt, ob diese Vorgaben auch eingehalten werden.

Eine weitere Bindung ergibt sich aus den vertraglichen Bindungen der Europäischen Union. Der Vertrag von Lissabon, welcher am 01.12.2009 in Kraft trat, sieht in Art. 6 II EU den Beitritt der EU zur Europäischen Menschenrechtskonvention (EMRK) vor, welcher bereits seit Jahrzehnten diskutiert wurde. Erst durch die Verleihung einer eigenen Rechtspersönlichkeit ist die EU nun in der Lage, der EMRK beizutreten. Da die EMRK bislang keinen Beitritt einer Staatengemeinschaft vorsah, mussten erst die Voraussetzungen für den Beitritt geschaffen werden; dies geschah durch das *Protokoll Nr. 14 zur Konvention zum Schutz der Menschenrechte und Grundfreiheiten über die Änderung des Kontrollsystems der Konvention in die EMRK* vom 13.05.2004[251]. Das Protokoll ist nach Zustimmung aller Vertragsparteien der Konvention am 01.06.2010 in Kraft getreten[252]. Voraussetzung für den Beitritt ist jedoch ein Beitrittsabkommen zwischen der EU und

---

[249] SEV Nr. 181 *„Zusatzprotokoll zum Europäischen Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten bezüglich Kontrollstellen und grenzüberschreitendem Datenverkehr“*

[250] sämtliche Texte des Ministerkomitees sind unter www.coe.int/t/cm/adoptedTexts_en.asp#P43_2297 verfügbar; hier: *„Council of Europe: Recommendation No. R (87) 15 of the Committee of ministers to member states regulating of personal data in the police sector“* vom 17.09.1987 (englisch).

[251] SEV Nr. 194, vgl. auch BGBl. II 2006 Nr. 5, S. 139 ff.

[252] s. Pressemitteilung des Europarats 437 (2010) “Reform des Europäischen Gerichtshofs für Menschenrechte – Protokoll Nr. 14 tritt in Kraft“ vom 31.05.2010.

den derzeit 47 Staaten[253] des Europarates. Das Abkommen bedarf hierzu eines einstimmigen Beschlusses durch den Rat der Europäischen Union gem. Art. 218 VIII AEUV unter Mitwirkung des Europäischen Parlaments gem. Art. 218 VI lit. a) Ziff. ii) AEUV. Der Beitritt zur EMRK hätte zur Folge, dass die EU an die EMRK vertraglich gebunden wäre und dass die Rechtsakte der EU, auch die des EuGH (allerdings nur bzgl. Grundrechtsfragen), einer Überprüfungsmöglichkeit durch den EGMR unterliegen würden.[254] Hierarchisch wäre die EMRK als völkerrechtlicher Vertrag zwischen dem sekundären Unionsrecht und dem primären Unionsrecht anzusiedeln.[255]

Auch vor dem Beitritt der EU zur EMRK ist die EU über Art. 6 III EU an die Grundrechte der EMRK als allgemeine Rechtsgrundsätze gebunden. Der EuGH hat erst zögerlich, doch später in mehreren Urteilen die EMRK als Rechtserkenntnisquelle herangezogen. Später verzichtete der EuGH sogar ganz auf den Umweg über die allgemeinen Rechtsgrundsätze und wendete die EMRK direkt[256] an. Des Weiteren sind sämtliche europäischen Mitgliedstaaten auch Mitglieder des Europarats, weshalb bislang zwar nicht die EU, jedoch deren Mitglieder aufgrund ihrer völkerrechtlichen Verantwortlichkeit die EMRK bei ihrer Rechtssetzung beachten müssen. Die Mitgliedstaaten sind mit der Unterzeichnung der EMRK eine völkerrechtliche Verpflichtung eingegangen, welcher sie sich nicht allein dadurch entziehen können, indem sie Hoheitsbefugnisse auf eine Staatengemeinschaft übertragen.[257]

Aufgrund dieser Bindung an die EMRK werden in Pkt. B. I. und C. I. jeweils zunächst die Anforderungen, welche die Rechtsprechung

---

[253] Stand: August 2011.
[254] Lindner, EuR 2007, 160 (172); Rohleder, S. 386.
[255] vgl. hierzu Mögele, in: Streinz, Art. 300 EGV, Rn. 82; Rohleder, S. 410 f.
[256] vgl. Rspr. des EuGH, Urteil vom 29.04.04 – *Orfanopoulos,* Rn. 98; EuGH, Urteil vom 11.07.02 – *Carpenter,* Rn. 41.
[257] EGMR, Urteil vom 30.06.2005 – *Bosphorus*; siehe auch Grabenwarter, § 4 Rn. 6.

auf Basis der EMRK stellt, erfasst und in einem weiteren Schritt die ePass- und Prüm-Regelungen diesen Anforderungen gegenübergestellt und überprüft.

Neben der EMRK stellen – wie oben angesprochen – auch die DSK und die Empfehlung R (87) 15 Mindestvorgaben hinsichtlich des Datenschutzes und der verfahrensrechtlichen Vorgaben auf, welche in Punkt B II 1. sowie in C. II. zusammengetragen und mit den ePass- und Prüm-Regelungen verglichen werden.

Das Datenschutzrecht differenziert nach materiellen Regelungen, wie z.B. bei der Qualität der Daten, und nach verfahrensrechtlichen Regelungen (Auskunfts-, Löschungsrechte etc.). Ebenso wird daher in Teil D entsprechend dieser Aufspaltung vorgegangen. Im Pkt. C. werden neben den Auskunftsrechten zusätzlich noch weitere völkerrechtliche Vorgaben an einen entsprechenden Rechtsschutz, insbesondere im Rahmen der gerichtlichen Kontrolle, aufgestellt. Auch diese müssen zum Schutze des Betroffenen im Rahmen der ePass- und Prüm-Regelungen Berücksichtigung finden.

B. ÜBERPRÜFUNG DES EPASSES UND DER PRÜM-REGELUNGEN IM HINBLICK AUF DEN MATERIELLEN DATENSCHUTZ

Nach eingehender Betrachtung der völkerrechtlichen Rechtsprechung sowie der materiell-rechtlichen Regelungen der DSK und der Empfehlungen des Ministerkomitees werden die europäischen Regelungen zum ePass und zum Prümer Ratsbeschluss sowie dessen Durchführungsbeschluss auf ihre Vereinbarkeit mit der Rechtsprechung zu Art. 8 EMRK sowie den materiellen Datenschutzvorgaben der DSK und den Empfehlungen des Ministerkomitees untersucht.

I. ART. 8 EMRK UND DIE VÖLKERRECHTLICHE RECHTSPRECHUNG

Art. 8 I EMRK schützt neben dem Recht auf Achtung des Privatlebens auch die Familie, die Wohnung und die Korrespondenz. Für den weiteren Verlauf der Arbeit sind nur das Recht auf Achtung des Privatlebens und dessen Ausprägungen von Bedeutung.

Zum Recht auf Achtung des Privatlebens existiert eine breite Rechtsprechung der Organe der EMRK. Im Folgenden wird daher zunächst auf die für diese Arbeit relevante Rechtsprechung zum Recht auf Achtung des Privatlebens eingegangen.

Da sich die Rechtsprechung seit den 80er Jahren, spätestens seit den 90er Jahren immer mehr mit Fragen des Datenschutzes zu befassen hat, ist auch hier eine breite Palette an Anforderungen hinsichtlich der Erfassung, Speicherung, Übermittlung, Aufbewahrung etc. von Daten ergangen, welche im Folgenden ausführlich diskutiert wird.

Abschließend werden die ePass- und die Prüm-Regelungen anhand der zuvor gefundenen Resultate überprüft.

1. EIN RECHT AUF DATENSCHUTZ IN ART. 8 I EMRK?

Als die EMRK im Jahre 1950 verabschiedet wurde, war mangels entsprechender Technologie ein Bedürfnis nach dem Schutz von Daten noch nicht absehbar,[258] weshalb in der EMRK kein solches Recht existiert. Da persönliche Daten einen Bereich des Privatlebens darstellen, wird der Datenschutz als Teilbereich des Rechts auf Achtung des Privatlebens angesehen, weswegen man den Schutzbereich eines solchen Datenschutzrechts nicht weiter fassen können wird als den Schutzbereich des Privatlebens.[259]

Der EGMR und die damalige EKMR haben seit den 70er Jahren eine deutliche Wandlung durchlaufen, wonach das Recht auf den Schutz persönlicher Daten angesichts immer weitläufigerer Bedrohungen im Rahmen des Rechts auf Privatleben stetig ausgedehnt wurde.

In der Entscheidung *X./.Vereinigtes Königreich*[260] ging es um Fotografien, welche gegen den Willen der Beschwerdeführerin nach deren Festnahme auf einer Demonstration gemacht und zusammen mit den Personalien in einer Akte verwahrt wurden. Die Forderung der Beschwerdeführerin, diese Fotos zu vernichten, wurde abgelehnt; ein Rechtsmittel stand nicht zur Verfügung. Die EKMR ging damals noch davon aus, dass kein Eingriff in das Recht auf Achtung der Privatsphäre vorliegt, gerade weil kein Bezug zum Privatleben bestehe. Die Beschwerdeführerin habe sich in die Öffentlichkeit begeben und müsse daher mit den Folgen rechnen.

---

[258] Siemen, S. 51.
[259] Siemen, S. 57.
[260] EKMR, Entscheidung vom 12.10.73 – *X/Vereinigtes Königreich*; so auch Siemen, S. 63 ff.

Anknüpfungspunkt der Kommission waren die Entstehung der Bilder, die abgebildete Situation sowie der Inhalt der Bilder. Nach der Kommission lag damit keine Beeinträchtigung der Beschwerdeführerin vor. Die Kommission hat jedoch übersehen, dass die Wohnung, also der umgrenzte Privatbereich, bereits von Art. 8 I EMRK selbstständig geschützt wird; zudem lässt die Kommission außer Acht, dass die Beschwerdeführerin schon allein durch die Existenz der Bilder, v.a. im Zusammenhang mit den Personalien, bzw. durch die Aufbewahrung der Bilder in ihrem Recht auf Achtung des Privatlebens beeinträchtigt sein könnte.[261] Datenschutzrechtliche Aspekte wurden in dieser Entscheidung von der EKMR noch nicht angesprochen.

In der Sache *Brüggemann und Scheuten./.BRD*[262] rügten die Beschwerdeführer die Verletzung von Art. 8 I EMRK durch die Entscheidung des deutschen Bundesverfassungsgerichts zu § 218 StGB. Die Kommission entschied, dass Art. 8 I EMRK dem Einzelnen eine Sphäre gewähre, in welcher er die Entwicklung seiner Persönlichkeit anstreben könne.[263] Bereits diese Entscheidung drückt das Recht des Einzelnen auf freie Gestaltung der Lebensführung aus.

Der Gerichtshof selbst ging zwar nur zögerlich, aber immerhin stetig zunehmend auf datenschutzrechtliche Aspekte ein.

In der Entscheidung *Klass u.a.*[264] realisierte der Gerichtshof, dass die Aufnahme des Telefonverkehrs spätestens dann datenschutzrechtlich relevant wird, wenn die gewonnenen Daten aufgezeichnet werden. Die Beschwerdeführer (Rechtsanwälte, Staatsanwälte und ein Richter) fühlten sich durch das neue G10-

[261] Siemen, S. 64 f.
[262] EKMR, Bericht vom 12.07.77 – *Brüggemann und Scheuten./.BRD*; Siemen, S. 67 f.
[263] EKMR, Bericht vom 12.07.77 – *Brüggemann und Scheuten./.BRD*, § 55; Siemen, S. 71.
[264] EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, § 28.

Gesetz der BRD beeinträchtigt, welches unter bestimmten Voraussetzungen die Überwachung des Telefonverkehrs gestattete, ohne jedoch die betreffenden Personen nachträglich zu verständigen. Der Gerichtshof bejahte hier einen Eingriff in Art. 8 I EMRK.

In der Sache *McVeigh u.a.*[265] wurden von den Beschwerdeführern, welche bei ihrer Rückkehr aus Irland aufgrund des Verdachts des Terrorismus festgenommen worden waren, Fingerabdrücke und Fotografien angefertigt und zu den Akten genommen. Trotz der sich später herausstellenden Unschuld – die angeblichen „Terroristen" waren nur „Touristen" – wurden die Daten nicht aus den Akten entfernt. Die Kommission hat hier trotz der offenen Datenerhebung eine Verletzung des Rechts auf Achtung des Privatlebens nicht ausgeschlossen. Leider hat die Kommission jedoch sowohl die Begründung des Schutzbereichs als auch des Eingriffs offen gelassen und den Eingriff zumindest als gerechtfertigt zur Bekämpfung des Terrorismus angesehen.[266]

Auch wenn die Kommission in der Sache McVeigh aufgrund der Erhebung der Daten eine Verletzung nicht ausgeschlossen hat, hatte sie bereits sehr früh in der Entscheidung *X./.BRD*[267] von 1962 die Aufbewahrung kriminalpolizeilicher Akten über bereits abgeschlossene Fälle als mit Art. 8 I EMRK vereinbar angesehen. Zwar könnte man dann einen Eingriff annehmen, wenn die Akten sehr lange Zeit aufbewahrt werden. Allerdings sieht die Kommission eine lange Aufbewahrung als gerechtfertigt an, wenn dies der Verhinderung terroristischer Straftaten dient[268], was der Entscheidung in der Sache McVeigh entspricht.

---

[265] EKMR, Entscheidung vom 18.03.81– *McVeigh u.a./Vereinigtes Königreich*; Siemen, S. 83 ff.
[266] EKMR, Entscheidung vom 18.03.81 – *McVeigh u.a./Vereinigtes Königreich*, § 230.
[267] EKMR, Entscheidung vom 04.10.62 – *G.W./.BRD*.
[268] Ellger, S. 133 f.

In der Sache *Census Regulations*[269] hat die Kommission allein das Sammeln von Informationen als ausschlaggebend dafür angesehen, ob ein Eingriff in den Schutzbereich vorliegt. Die Kommission bestätigt in dieser Entscheidung zudem, dass auch eine offene Datenerhebung eine Verletzung des Rechts auf Privatleben darstellen kann. Der Sache lag eine britische Volkszählung zugrunde, gegen welche sich der Beschwerdeführer mit der Auffassung wandte, durch das Ausfüllen des Erhebungsbogens in seinem Recht gem. Art. 8 I EMRK beeinträchtigt zu sein. Der britische Census Regulations Act verlangt, dass die jeweiligen Hausvorstände Fragen hinsichtlich des Alters, Geschlechts, der Adresse, des Berufes etc. beantworten sollte.[270]

In der Sache *Malone*[271] ging es um die verdeckte Aufzeichnung des Briefverkehrs und der Telekommunikation. Der Beschwerdeführer wurde der Hehlerei verdächtigt, weswegen sein Telefonanschluss über mehrere Jahre hinweg überwacht worden war. Da der Beschwerdeführer den Eingriff mangels nachträglicher Information über die Datenerhebung nicht nachweisen konnte, war schon die Existenz eines solchen fraglich. Dennoch bejahte der Gerichtshof eine Beeinträchtigung, da allein die Möglichkeit der geheimen Überwachung, welche durch die geltenden Gesetze und die Praxis gegeben war, für einen Eingriff ausreiche.[272] Dies ist auch nur im Sinne des Betroffenen, da dieser – sofern er mit der Möglichkeit einer Überwachung rechnen muss – sein Privatleben nur noch gehemmt ausüben kann, d.h. er wird am Telefon nicht mehr frei sprechen können und sich ständig fragen müssen, was er preisgeben möchte. Allerdings hat sich der Gerichtshof dann einer weiteren Umgrenzung des Rechts auf Privatleben entzogen, indem er zwar sowohl die Registrierung der Daten als auch die

[269] EKMR, Entscheidung vom 06.10.82 – *Census Regulations*; Siemen, S. 83 ff.
[270] vgl. Kübler, S. 34 f.
[271] EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*; Siemen, S. 86 ff.
[272] EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, § 64.

Überwachung als Verletzung des Art. 8 I EMRK ansah, diese jedoch nur pauschal sowohl dem Recht auf Achtung des Privatlebens als auch der Korrespondenz zuordnete, ohne eine genaue Abgrenzung vorzunehmen. Genau diese Vorgehensweise kritisierte jedoch Richter Pettiti. Dieser erkannte die Gefährlichkeit der aufkommenden Informationstechniken und schlug daher vor, die Datenschutzkonvention des Europarats als Maßstab für den Umgang mit personenbezogenen Daten heranzuziehen. Besonders die Länder, welche der DSK beigetreten seien, müssten ihre Verpflichtungen sowohl aus der EMRK als auch aus der DSK erfüllen. [273]

Leider hat sich der Gerichtshof auch in der Sache *Leander*[274] einer klaren Aussage entzogen. Ein Schifffahrtsmuseum hatte den Beschwerdeführer als Techniker für seine Lagerräume, welche sich in einem militärischen Sperrgebiet befanden, eingestellt. Wenige Tage nach der Einstellung wurde er jedoch unter Hinweis auf eine erfolgte Sicherheitsüberprüfung durch die Polizei entlassen. Der Beschwerdeführer wandte sich mit der Bitte um Auskunft an die Polizei. Die Auskunft wurde ihm jedoch verweigert, ebenso die Möglichkeit einer Stellungnahme. Die dagegen eingelegte Beschwerde an die Regierung blieb erfolglos. Der EGMR sah in der Speicherung und Weitergabe der Daten einen Eingriff, sofern ein Bezug zum Privatleben vorhanden gewesen ist und bezog sich hierfür auf einen vorangegangenen Bericht der Kommission, welcher wiederum auf eine eigene unveröffentlichte Entscheidung verwies[275], wonach die Aufbewahrung und Weiterleitung einer Akte an ein Gericht ein datenschutzrechtliches Problem sei,

[273] EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, Sondervotum des Richters Pettiti.
[274] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*; Siemen, S. 88 f.
[275] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 46; EKMR, Bericht vom 17.05.85 - *Leander./.Schweden*, § 54 mit Verweis auf die unveröffentlichte Entscheidung der EKMR vom 07.05.81, App. Nr. 8334/78.

welches in den Schutzbereich des Art. 8 I EMRK falle.[276] Allerdings würde dies vom Inhalt der jeweiligen Akte abhängen.[277]

Im Gegensatz zum Malone-Urteil des Gerichtshofs hat die Kommission im Fall *Hilton*[278] allein deswegen einen Eingriff abgelehnt, weil die Beschwerdeführerin nicht nachweisen konnte, dass der Secret Service Informationen über sie gesammelt hatte und aufbewahrte. In dieser Angelegenheit ging es um die Ablehnung einer Bewerbung der Beschwerdeführerin als Reporterin bei der BBC. Die Beschwerdeführerin hatte erst Jahre später erfahren, dass die Ablehnung angesichts einer Sicherheitsüberprüfung erfolgt war, welche ergeben hatte, dass sie während ihrer Universitätszeit Mitglied der Schottisch-Chinesischen Gesellschaft gewesen war. Verwunderlich ist jedoch angesichts der Entscheidung der Kommission, dass sie einen Eingriff aufgrund der Unkenntnis der Beschwerdeführerin von einer möglichen Verletzung ablehnt, jedoch kein Auskunftsrecht gewährt bzw. dieses – sofern es bereits von der Regierung gewährt worden war – nicht problematisiert. Ferner hatte die Kommission – äußerst verhalten – eine Sicherheitsüberprüfung nicht per se als Eingriff angesehen, sondern vielmehr nur, wenn die Sicherheitsüberprüfung auf Informationen aus dem Bereich des Privatlebens beruht.[279]

In den Sachen *Lundvall*[280] und *Reyntjens*[281] machte sich die Kommission zum ersten Mal die Auswirkungen der Sammlung von Daten klar. Der Beschwerdeführer Lundvall war säumiger Steuerzahler und als solcher mit Namen, Anschrift und seiner persönlichen Identifikationsnummer in ein spezielles Verzeichnis

[276] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 48.
[277] EKMR, Bericht vom 17.05.85 – *Leander./.Schweden,* § 56.
[278] EKMR, Entscheidung vom 06.07.88 – *Hilton./.Vereinigtes Königreich*; Siemen, S. 94.
[279] EKMR, Entscheidung vom 06.07.88 – *Hilton./.Vereinigtes Königreich*.
[280] EKMR, Entscheidung vom 01.12.85 – *Lundvall./.Schwede;* Siemen*, S. 92.*
[281] EKMR, Entscheidung vom 09.09.92 – *Reyntjens./.Belgien*; Siemen, S. 93.

aufgenommen worden. Hierbei ist hinzuzufügen, dass es in Schweden üblich war, Daten einer Person mit einer Identifikationsnummer zu versehen, um mit deren Hilfe in kürzester Zeit umfassende Datenabgleiche durchführen zu können. Die Kommission kam zwar zu dem Schluss,

> *„it is therefore conceivable that the use of personal data in different registers and the matching of such registers could raise an issue under Art. 8 of the Convention"*[282]*,*

jedoch verneinte sie letztlich die Zulässigkeit der Beschwerde, da der Beschwerdeführer durch die Verwendung einer solchen Identifikationsnummer nicht beschwert sei. Im Gegensatz zum Fall Lundvall wurde in der Sache *Reyntjens* der Schutzbereich trotz der gleichen Qualität der Daten als nicht eröffnet angesehen unter Hinweis darauf, dass bei Verwendung einer persönlichen Identifikationsnummer ein wesentlich schnellerer Datenabgleich durchführbar wäre. Der Beschwerdeführer hatte sich gegenüber der Polizei geweigert, im Rahmen einer Routinekontrolle seine „carte d'identité" vorzulegen. Die Kommission hat hier sehr zurückhaltend entschieden, obwohl sie bereits die Gefahren einer Vernetzung erkannt hatte.[283]

Obwohl der Gedanke des Datenschutzes bis dato bereits Einzug in die Rechtsprechung hielt, wurde bislang eine Bedrohung nur in den Handlungen (Erfassung oder Sammlung) oder im Ort der Aufbewahrung (Akte) und zum Teil auch in der Vernetzung der Daten gesehen, jedoch nicht in der alleinigen Existenz der das Privatleben betreffenden Daten.[284] Auch wurde der Datenschutz bis dahin nicht als eigenständiger Aspekt des Rechts auf Achtung

[282] EKMR, Entscheidung vom 11.12.85, DR 45, 121 (130) – *Lundvall./.Schweden*.
[283] So auch Frowein, in: Frowein/Peukert, Art. 8 EMRK, Rn. 5.
[284] So auch Siemen, S. 90.

des Privatlebens angesehen, so dass für die Bejahung eines Eingriffs immer ein Bezug zum Privatleben erforderlich war.[285]

Da biometrische Merkmale auch medizinische Daten enthalten, erfolgt nun eine Auseinandersetzung mit Entscheidungen zu medizinischen Daten.

So hat die Kommission in der Sache *L./.BRD*[286] medizinische Daten dem Schutzbereich des Art. 8 I EMRK unterstellt und darauf hingewiesen, dass der Datenschutz seit der Leander-Rechtsprechung einhellig als vom Schutzbereich des Art. 8 EMRK umfasst anzusehen sei. Die Beschwerdeführerin hatte kritisiert, dass man das zur Feststellung ihrer strafrechtlichen Verantwortlichkeit im Rahmen eines Strafverfahrens gefertigte Gutachten auch für ein nachfolgendes zivilgerichtliches Verfahren zur Feststellung der Prozessbefugnis verwendet hatte. Statt jedoch genauer auf den Schutzbereich einzugehen, stellte die Kommission fest, dass das Gutachten für die Durchführung eines ordnungsgemäßen Gerichtsverfahrens erforderlich gewesen sei und zudem der Berichterstatter die alleinige Einsicht in das Gutachten erhalten habe, weswegen ein Eingriff abzulehnen sei. Dabei ist anzumerken, dass die Kommission damit die Rechtfertigung des Eingriffs vorweggenommen und bereits in der Eingriffsprüfung Verhältnismäßigkeitserwägungen angestellt hat. Dennoch ist die Entscheidung der Kommission im Ergebnis nachvollziehbar, da das Gutachten sowohl im Strafprozess als auch im Zivilprozess der alleinigen Feststellung der Prozessführungsbefugnis bzw. Verantwortlichkeit und damit dem gleichen Zweck diente. Es wäre mit unnötigen Kosten verbunden, wollte man ein erneutes Gutachten für die gleiche Angelegenheit herstellen.

---

[285] So auch Siemen, S. 95.
[286] EKMR, Entscheidung vom 13.10.88 – *L./.BRD*, Siemen, S. 98.

Auch der Gerichtshof hat sich bereits mit medizinischen Daten befasst und erklärt:

> *„the protection of personal data ["not least/particularly"] medical data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Art. 8 of the Convention".*[287]

In den bezeichneten Urteilen *Z./.Finnland*[288] und *M.S./Schweden*[289] ging es um die Weitergabe klinisch erhobener medizinischer Daten an staatliche Stellen. In beiden Entscheidungen hat der EGMR zwar medizinische Daten als vom Schutzbereich des Art. 8 EMRK als erfasst angesehen; im ersten Urteil ist er jedoch gar nicht auf den Schutzbereich eingegangen; vielmehr hat er gleich den Eingriff begründet und diesbezüglich entschieden, dass gerade bei der Zur-Verfügung-Stellung an einen größeren Personenkreis eine Beeinträchtigung vorliege. Demgegenüber ist der Gerichtshof in der Sache *M.S./Schweden* erstmals auf die DSK eingegangen, indem er feststellte, dass medizinische Daten dem Art. 6 DSK unterfallen würden und damit problemlos – gerade wegen ihrer Schutzbedürftigkeit – dem Schutzbereich des Art. 8 I EMRK zugeordnet werden könnten. In diesem speziellen Fall erachtete der EGMR insbesondere das Vertrauensverhältnis zwischen Arzt und Patient für wichtig.

Der Gerichtshof hat auch in der Entscheidung *Y.F./Türkei* den menschlichen Körper als intimsten Aspekt des Privatlebens verstanden.[290] Dies zeigt sich auch in seinen zahlreichen Entscheidungen, wonach die psychische und physische Integrität

[287] EGMR, Urteil vom 25.02.97 – *Z./.Finnland,* § 95*;* EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*, § 41.
[288] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*; Siemen, S. 98 ff.
[289] EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*; Siemen, S. 98 ff.
[290] EGMR, Urteil vom 22.07.03 – *Y.F./Türkei*, § 33.

des Individuums geschützt wird.[291] Hierzu gehört auch die Entnahme von Blut sowie zwangsweise durchgeführte erkennungsdienstliche Maßnahmen, die richtigerweise als Eingriff zu qualifizieren sind[292], auch wenn die körperliche Belastung i.E. gering sein mag.[293] Gerade deshalb sind auch Urinproben erfasst, werden jedoch meist gerechtfertigt sein.[294]

Aufgrund der aufkommenden Datenschutzdiskussion erließen der EGMR und die EKMR vermehrt Entscheidungen zur Erhebung, Verarbeitung und Speicherung von Daten.

So ging es in der Sache *Lupker*[295] um polizeiliche Maßnahmen gegen eine Gruppe von Hausbesetzern. Aus den Unterlagen der Führerschein- und der Passbehörde hatte die Polizei ein Buch mit Verdächtigen zusammengestellt, welche sie in diversen Geschäften zur Identifizierung der Gruppe vorzeigten. Die Beschwerdeführerin, eine der Verdächtigen, fühlte sich dadurch in ihrem Recht aus Art. 8 I EMRK verletzt. Die Kommission hat keinen Eingriff in das Privatleben angenommen, da die Bilder nicht in einer die Privatsphäre verletzenden Art und Weise aufgenommen worden seien. Zudem seien die Aufnahmen ursprünglich mit Einwilligung der Betroffenen in die Unterlagen gelangt und danach ausschließlich zur Identifizierung von Straftätern verwendet worden. Eine öffentliche Zur-Verfügung-Stellung sei nicht erfolgt. Diese Entscheidung der Kommission ist jedoch im Vergleich zu den bisherigen Entscheidungen oberflächlich. Zunächst wurden die Fotos zwar nicht der Öffentlichkeit zur Verfügung gestellt, aber doch der Öffentlichkeit

---

[291] EGMR, Urteil vom 12.06.03 – *van Kück./.BRD*, § 69; EGMR, Urteil vom 26.03.85 – *X und Y./. Niederlande*, § 22; EGMR, Urteil vom 25.03.93 – *Costello Roberts./.Vereinigtes Königreich*, § 34.
[292] Frowein, in: Frowein-Peukert, 2009, Art. 8 EMRK, Rn. 8.
[293] EKMR, Entscheidung vom 13.12.79, DR 18, 155 (156) – *X./.Österreich.*; Frowein, in: Frowein-Peukert, 2009, EMRK, Art. 8 Rn. 8.
[294] S. Peters, S. 157.
[295] EKMR, Entscheidung vom 07.12.92 – *Lupker./.Niederlande*; Siemen, S. 103 f.

preisgegeben. Wirklich unbedacht ist jedoch letztlich die Feststellung der Kommission, die Bilder seien mit Willen der Betroffenen aufgenommen worden. Weder bei der Führerschein- noch bei der Passbehörde noch bei der Polizei gelangen Bilder mit Willen des Betroffenen zu den Unterlagen. Auch wenn man den „Wunsch" nach einem und damit das Wollen eines Führerscheins noch nachvollziehen kann, obgleich auch dies wegen der bürokratischen Zwänge äußerst diskussionswürdig ist, so erfolgen doch weder die Beantragung eines Passes noch die Bilder bei der Polizei freiwillig. Wenn man darüber hinaus die entsprechenden Fotos aus der Pass- und der Führerscheinbehörde zur strafrechtlichen Ermittlung verwendet, so ist dies ein grober Verstoß gegen den Zweckbindungsgrundsatz.

Allerdings ist klarzustellen, dass die Kommission dann in der Sache *Arnaud Campion./.Frankreich*[296] den Zweckbindungsgrundsatz doch zumindest erkannt und anerkannt hat. Zwar hat sie einen Eingriff in das Recht auf Privatleben durch das Fotografieren in einer Radarfalle nicht als Eingriff in Art. 8 I EMRK angesehen. Dennoch hat sie unterstrichen, dass es entscheidend sei, ob die Aufnahmen veröffentlicht oder für andere Zwecke verwendet werden.

Doch bereits vor der Entscheidung Arnaud Campion./.Frankreich hat die Kommission erkannt, dass ein Eingriff erheblich davon abhänge, ob bereits beschaffte Daten der nachträglichen Verarbeitung unterliegen. So hat sie in *Friedl* den Eingriff nur unter Hinweis darauf verneint, dass keine nachfolgende Verarbeitung stattgefunden hat.[297] Der Beschwerdeführer war bei einer Demonstration fotografiert worden; außerdem wurden seine Personalien festgehalten. Die Regierung hat auf die Klage des

[296] EKMR, Entscheidung vom 06.09.95 – *Arnaud Campion./.Frankreich*; Siemen, S. 106 f.
[297] EKMR, Entscheidung vom 19.05.94 – *Friedl./.Österreich*, § 49; Siemen, S. 104 ff.

Beschwerdeführers hin zugesichert, dass die fotografierten Personen anonym geblieben und deren Daten nicht elektronisch verarbeitet worden seien, der Beschwerdeführer insbesondere nicht durch Datenverarbeitung identifiziert worden sei. Die Kommission hat der Begründung der Regierung geglaubt und daher einen Eingriff abgelehnt. Die Entscheidung ist ein Anzeichen dafür, dass die Kommission nun umdenkt und die Datenverarbeitung als wichtiges Kriterium dafür heranzieht, ob ein Eingriff vorliegt oder nicht.[298]

Einen weiteren Ansatzpunkt für die Bejahung eines Eingriffs sah die Kommission in der Speicherung und Verarbeitung von sensiblen Informationen. Der Beschwerdeführer *Tsavachidis*[299] hat eine Verletzung des Art. 8 I EMRK gerügt, da er durch den griechischen Geheimdienst wegen seiner religiösen Tätigkeiten im Zusammenhang mit den Zeugen Jehovas überwacht worden war. Die Kommission hat einen Eingriff bejaht, da es um die Speicherung und Verarbeitung von Informationen über religiöse Tätigkeiten ging, welche zwar in der Öffentlichkeit ausgeübt worden waren, aber doch – gerade aufgrund des religiösen Hintergrunds – dem Privatleben zuzuordnen sind. Zudem seien die erlangten Informationen das Ergebnis einer geheimen Überwachungsaktion gewesen.[300] Trotz der fortschreitenden Integrierung des Rechts auf Schutz persönlicher Daten in Art. 8 I EMRK gab es drei Kommissionsmitglieder – Herndl, Conforti und Bîrsan –, welche aufgrund der freien Zugänglichkeit der Informationen und dem damit einhergehenden Bezug zur Öffentlichkeit eine Verletzung des Art. 8 I EMRK verneinten.[301]

---

[298] Siemen, S. 106.
[299] EKMR, Bericht vom 28.10.97 –*Tsavachidis./.Griechenland*; Siemen, S. 107 f.
[300] EKMR, Bericht vom 28.10.97 –*Tsavachidis./.Griechenland*, § 48.
[301] EKMR, Bericht vom 28.10.97 –*Tsavachidis./.Griechenland*, Partly Concurring mostly dissenting opinion of MM K. Herndl, B. Conforti and C. Bîrsan.

Ebenso wie die Kommission hatte auch der EGMR Fälle zur Erhebung, Verarbeitung und Speicherung von Daten zu entscheiden.

Richtungsweisend war insbesondere das Urteil *Amann*[302]. Der Beschwerdeführer importierte geschäftlich Enthaarungsgeräte in die Schweiz. Durch seine Werbung erreichte er auch eine Kundin in der sowjetischen Botschaft in Bern, welche daraufhin telefonisch ein Gerät bestellte. Dieses Gespräch wurde vom Polizeidienst der Bundesanwaltschaft abgehört, woraufhin über den Beschwerdeführer eine Karteikarte im Sicherheitsregister angelegt wurde, worin er als Kontaktperson zur sowjetischen Botschaft aufgeführt wurde. Der Beschwerdeführer ersuchte um Einsichtnahme in dieses Register, erhielt jedoch nur geschwärzte Textpassagen, woraufhin er Beschwerde gegen das Abhören des Telefons, das Anlegen und Führen der Karteikarte einlegte. Der Gerichtshof sah das Speichern von Daten vom Schutzbereich des Art. 8 I EMRK umfasst. Grundlegend war jedoch der Verweis auf die DSK. Zwar hatte der EGMR bereits im Urteil *M.S./Finnland* auf die DSK Bezug genommen;[303] allerdings setzt er sich nun erstmals in der materiellen Prüfung des Art. 8 I EMRK mit der DSK auseinander und erkennt den Schutz des Einzelnen bei der automatischen Verarbeitung seiner Daten als Zweck der Konvention an.[304] Nach über 15 Jahren geht der EGMR damit auf den Vorschlag des Richters Pettiti im Urteil Malone, die DSK als Maßstab für den Umgang mit personenbezogenen Daten heranzuziehen,[305] ein.

---

[302] EGMR, Urteil vom 16.02.00 – *Amann./.Schweiz;* Siemen, S. 110 ff.
[303] EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*; Siemen, S. 98 ff.
[304] EGMR, Urteil vom 16.02.00 – *Amann./.Schweiz,* § 65.
[305] EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, Sondervotum des Richters Pettiti.

In der Sache *Rotaru*[306] hat der Gerichtshof die systematische Sammlung und Speicherung von Informationen als Kriterium dafür herangezogen, dass die Informationen in den Schutzbereich des Art. 8 I EMRK fallen, auch wenn die Informationen ursprünglich frei verfügbar und öffentlich zugänglich waren. Dem Beschwerdeführer wurden in einem Gerichtsverfahren im Rahmen der Beweisführung Informationen über seine politischen Aktivitäten vorgehalten, die vom ehemaligen rumänischen Geheimdienst gesammelt worden waren und später in den Bestand des heutigen Geheimdienstes aufgenommen wurden. Obwohl diese Informationen letztlich falsch waren, wurden sie nicht gelöscht. Eine Klage gegen die weitere Verwendung war nur bedingt erfolgreich, so dass der Beschwerdeführer mit der Beschwerde gegen die weitere Verwahrung und mögliche Verwendung der falschen Informationen vorging. Die Regierung war der Ansicht, der Beschwerdeführer habe durch seine politischen Aktivitäten konkludent auf sein Recht auf „Anonymität" verzichtet, weswegen es sich um öffentliche Informationen gehandelt habe.[307] Der Gerichtshof führte hierzu aus:

> *„Moreover, public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities."*[308]

Auch im Urteil *P.G. und J.H.*[309] wertet der Gerichtshof die systematische Sammlung von personenbezogenen Daten als Eingriff in Art. 8 I EMRK. Die Beschwerdeführer waren verdächtig, einen Überfall auf einen Geldtransporter zu planen, weswegen verschiedene Überwachungsmaßnahmen angeordnet wurden.

---

306 EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*; s. auch Siemen, S. 112 f.
307 EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, § 42.
308 EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien,* § 43.
309 EGMR, Urteil vom 25.09.01 – *P.G. und J.H../Vereinigtes Königreich*; Siemen, S. 114 ff.

Nach der Festnahme wurden die Gespräche der Beschwerdeführer in ihren Zellen abgehört, aufgezeichnet und es wurde anschließend ein Stimmenvergleich mit den während der Überwachung gemachten Tonbandaufnahmen durchgeführt. Die Regierung bezweifelte hinsichtlich der letzteren Maßnahme einen Eingriff in Art. 8 I EMRK, da die Stimme nicht dem Privatleben zuzuordnen, sondern ein äußerliches und damit öffentliches Merkmal sei. Außerdem hätten die Beschwerdeführer aufgrund der besonderen Situation nicht damit rechnen können, dass ihnen Privatsphäre zugebilligt würde.[310] Der Gerichtshof hat entschieden, dass die Erwartung der Person, welche diese an die Privatsphäre stellt, einen bedeutenden Faktor darstelle.[311] Ausschlaggebend war jedoch die systematische und dauerhafte Aufzeichnung der Daten. Der Gerichtshof folgte damit nicht den Ausführungen der Regierung, sondern sah in der Aufzeichnung der Stimme eine Verletzung des Art. 8 I EMRK.[312]

Die Vorhersehbarkeit der Aufnahme und Verbreitung von Informationen ist auch in der Sache *Peck*[313] Anknüpfungspunkt für die Bejahung des Eingriffs. Der Beschwerdeführer hatte nachts im öffentlichen Raum versucht, sich die Pulsadern aufzuschneiden. Während des Selbstmordversuchs war er nicht gefilmt worden, allerdings zuvor mit dem Messer in der Hand. Der Betreiber der öffentlichen Überwachungskamera hat das Filmmaterial an TV-Sender weitergegeben, welche die Ausschnitte veröffentlichten, allerdings ohne die Identität des Beschwerdeführers hinreichend unkenntlich zu machen. Der Gerichtshof entschied, dass es nicht darauf ankomme, ob es sich um eine geheime oder offene

310 EGMR, Urteil vom 25.09.01 – *P.G. und J.H../Vereinigtes Königreich*, § 54.
311 EGMR, Urteil vom 25.09.01 – *P.G. und J.H../Vereinigtes Königreich*, § 57.
312 *„The Court concludes therefore that the recording of the applicant's voices (…) discloses an interference with their right to respect for private life (…)",* vgl. EGMR, Urteil vom 25.09.01 – *P.G. und J.H../Vereinigtes Königreich*, § 60.
313 EGMR, Urteil vom 28.01.03 – *Peck./.Vereinigtes Königreich*; Siemen, S. 117 f.

Maßnahme gehandelt habe. Vielmehr komme es darauf an, ob Personen systematisch gefilmt oder die Aufnahme dauerhaft gespeichert werden. Hier ging es allerdings dem Beschwerdeführer in erster Linie nicht um die Speicherung, sondern vielmehr um die Weitergabe an die TV-Sender. Der Gerichtshof sieht daher insbesondere die Verbreitung durch die Medien als ausschlaggebend für einen Eingriff an, da der Beschwerdeführer damit von nun an einer sehr viel stärkeren Beobachtung ausgesetzt sein würde. Zudem sei zu beachten, dass die Videoaufnahme für den Beschwerdeführer nicht im Geringsten vorhersehbar war. Der Gerichtshof vertritt damit wieder einmal die Ansicht, dass der Schutz der Privatsphäre nicht an der Wohnungstür ende, sondern dass der Einzelne auch das Recht habe, sich in der Öffentlichkeit ohne Beobachtung bewegen zu können.[314]

Im Fall *Perry*[315] war ebenfalls die heimliche Videoüberwachung Gegenstand des Verfahrens. Der Beschwerdeführer war von der Polizei festgenommen worden, hatte sich jedoch einer Gegenüberstellung widersetzt. Daraufhin wurde er polizeilich geladen und beim Eintritt in die Dienststelle von einer eigens justierten Überwachungskamera zum Zwecke der Identifizierung aufgenommen. Nachdem sich der Beschwerdeführer erneut einer Gegenüberstellung widersetzte, griff die Polizei auf das Überwachungsmaterial zurück und konnte so den Beschwerdeführer als Täter identifizieren. Der Gerichtshof sah in der Verwendung einer Überwachungskamera per se keinen Eingriff.[316] Da die Kamera jedoch besonders eingestellt worden war und die Aufnahmen zudem auch Zeugen und beteiligten Personen im Gerichtsverfahren gezeigt worden waren, handelte es sich nach dem Gerichtshof um eine Maßnahme von ganz anderer Qualität.

---

[314] EGMR, Urteil vom 28.01.03 – *Peck./.Vereinigtes Königreich*, § 59 ff.; Siemen, S. 118 f.

[315] EGMR, Urteil vom 17.07.03 – *Perry./.Vereinigtes Königreich*.

[316] EGMR, Urteil vom 17.07.03 – *Perry./.Vereinigtes Königreich*, § 40.

In der Sache *S. and Marper./.Vereinigtes Königreich* beanstandeten die Beschwerdeführer, dass die Behörden deren Fingerabdrücke, DNA-Proben und DNA-Profile auch nach dem Strafverfahren aufbewahrt haben, obwohl dieses mit einem Freispruch endete bzw. eingestellt wurde. Sie verlangten daher die Löschung. Der EGMR hat hierzu ausführlich Stellung genommen. Danach sind sowohl Fingerabdrücke als auch DNA-Proben als auch DNA-Profile personenbezogene Daten i. S. d. DSK.[317] Im Anschluss daran hat der EGMR zwischen Fingerabdrücken und DNA differenziert. Hinsichtlich der DNA hat der EGMR darauf hingewiesen, dass die Besorgnis des Einzelnen über die mögliche zukünftige Verwendung der DNA durchaus berechtigt sei. Die DNA enthalte viele sensible Informationen über den Einzelnen, einschließlich Informationen über die Gesundheit sowie den genetischen Code des Betroffenen und seiner Verwandten. Des Weiteren erlaube die Verarbeitung der DNA-Profile den Behörden den Zugriff auf die ethnische Herkunft; solche Informationen würden dann im polizeilichen Ermittlungsverfahren auch tatsächlich genutzt werden. Der EGMR sieht folglich in der Einbehaltung der DNA-Profile und des DNA-Materials eine Beeinträchtigung von Art. 8 I EMRK.[318] Hinsichtlich der Fingerabdrücke wendet der EGMR die Vorgaben an, welche er in Bezug auf Fotografien und Stimmmuster gemacht hat. Der Gerichtshof sah in diesem Fall v.a. in der Speicherung der Fingerabdrücke in nationalen Datenbanken eine Beeinträchtigung des Rechts auf Privatleben.[319]

Aufgrund der inzwischen ergangenen Rechtsprechung zum Umgang mit Daten, insbesondere seit dem Urteil *Amann,* kann der Datenschutz mittlerweile als eigenständiges Element des Art. 8 I

[317] EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, § 68.
[318] EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, § 70 ff.
[319] EGMR, Urteil vom 04.12.08 – *S. &Marper./.Vereinigtes Königreich*, § 84 ff.

EMRK angesehen werden.[320] In der Sache *Amann* hat der EGMR erstmals die DSK als Kriterium für den Schutzbereich herangezogen. Später hat er die jeweiligen Eingriffe nach der Art der Erhebung und Verarbeitung, der Qualität der Daten sowie der Aufbewahrung bewertet, allesamt Kriterien der zwischenzeitlich vorhandenen Datenschutzregelungen. Zwar wird ein Bezug zum Privatleben noch gefordert, dieser ist nach dem Gerichtshof allerdings bereits durch die Qualität des Eingriffs, bspw. durch eine lange Aufbewahrung, oder die Erwartungshaltung des Betroffenen gegeben. So sind bislang keine umfassenden Regelungen zum Datenschutz ausgearbeitet worden, aber dennoch wird das Bestreben ersichtlich, das Individuum vor staatlichen Eingriffen zu schützen.[321]

Allerdings kann aus dem Recht auf Achtung des Privatlebens kein der deutschen Rechtsprechung vergleichbares Recht auf Achtung des informationellen Selbstbestimmungsrechts abgeleitet werden.[322]

Manche Stimmen aus der Literatur[323] sehen dies allerdings anders seit der Rechtsprechung *Pretty*[324]. Eine Britin, welche an einer unheilbaren Nervenkrankheit litt, konnte ihrem Leben selbst kein Ende bereiten und bat um aktive Sterbehilfe durch ihren Mann. Sie beantragte daher bei den Behörden Straffreiheit für ihren Mann, was jedoch abgelehnt wurde. Der Gerichtshof verwies zunächst auf seine vorangegangen Rechtsprechung, wonach vom Recht auf Privatleben auch die physische und psychische Integrität sowie das Recht, mit anderen Menschen in Verbindung zu treten und seine

320 So auch Siemen, S. 130; Breitenmoser, S. 48 und 245; Grabenwarter, § 22 Rn. 10; Tettinger, in: Tettinger/Stern, Art. 7 GRC, Rn. 14 f.
321 Vgl. Kübler, S. 37.
322 So auch Ellger, S. 138 f.; Sule, S. 75.
323 So z.B. Siemen, S. 75 f., Unger, S. 132 und 136; Mähring, in: EuR 1991, 369 (373).
324 EGMR, Urteil vom 29.04.02 – *Pretty./.Vereinigtes Königreich*; Siemen, S. 76 f.

eigene Persönlichkeit zu entwickeln, erfasst seien. Dann stellte er fest:

> *„Although no previous case has established as such any right to self-determination as being contained in Art. 8 of the Convention, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees"*[325]

Hierdurch sehen sich die Stimmen in der Literatur bestätigt.

Es stellt sich die Frage, ob auch die Rechtsprechung zum Recht am eigenen Bild diesen Eindruck bestätigt. In der Sache *Schüssel*[326] hat der EGMR ausdrücklich ein Recht am eigenen Bild anerkannt und dem Privatleben zugeordnet.[327] Die Veröffentlichung von Bildberichten kann daher einen Eingriff darstellen. Allerdings kann es entscheidend sein, ob die Person bei einer privaten oder öffentlichen Betätigung abgebildet wurde.[328] Der Bekanntheitsgrad ist bei der Frage des Eingriffs noch nicht von Bedeutung und findet erst auf der Rechtfertigungsebene Beachtung.[329] Die Abbildung, welche auf einem Polizeirevier gemacht wird, ist ebenso geschützt wie die Abbildung in der Öffentlichkeit.[330] Nach den Rechtsprechungsorganen nicht geschützt ist die bloße Beobachtung in der Öffentlichkeit, da hierbei kein Schutz zu erwarten ist. Erst wenn eine systematische oder dauerhafte Aufzeichnung von dieser Betätigung gemacht wird, ist ein Eingriff anzunehmen.[331] Gerade bei Personen der Öffentlichkeit wird

---

325 EGMR, Urteil vom 29.04.02 – *Pretty./.Vereinigtes Königreich*, § 61.
326 EGMR, Urteil vom 21.02.02 – *Schüssel./.Österreich*.
327 EGMR, Urteil vom 21.02.02 – *Schüssel./.Österreich*, § 2.
328 So Neukamm, S. 211.
329 EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, §§ 50 ff.
330 EGMR, Urteil vom 25.09.01 – *P.G. und J.H./.Vereinigtes Königreich*, § 57; EGMR, Urteil vom 17.07.03 – *Perry./.Vereinigtes Königreich*, §§ 38, 40; EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, § 53.
331 EGMR, Urteil vom 17.07.03 – *Perry./.Vereinigtes Königreich*, § 38; EGMR, Urteil vom 28.01.03 – *Peck./.Vereinigtes Königreich,* § 59; EKMR.

angenommen, dass auch diese auf den Schutz ihres Privatlebens in der Öffentlichkeit vertrauen dürfen.[332] Mit dem Urteil *Caroline von Hannover*[333] hat sich der EGMR gegen die frühen Entscheidungen der Kommission gewandt, wonach weder Fotos eines Demonstranten noch die Aufbewahrung von Akten einen Eingriff darstellten.[334] Der EGMR hat damit letztlich bereits die bloße Existenz der Daten dem Schutz des Art. 8 I EMRK unterstellt. Der EGMR geht in der von Hannover-Rechtsprechung sogar noch weiter und verlangt eine positive Verpflichtung des Staates zum Schutz der Privatsphäre des Einzelnen. Dementsprechend können Maßnahmen erforderlich sein, die der Achtung der Privatsphäre dienen.[335]

Durch das Recht am eigenen Bild sind nicht nur Äußerlichkeiten einer Person geschützt, sondern auch Elemente, die sich auf die Identität einer Person beziehen.[336] Infolgedessen müssten davon auch – gerade wegen dieses Schutzes – sämtliche biometrischen Merkmale umfasst sein.

Des Weiteren hat die Rechtsprechung anerkannt, dass der Einzelne ein Recht hat, Beziehungen zu anderen Menschen und zu seiner Umwelt aufzubauen sowie sein Leben – ohne Einmischung von außen – frei zu gestalten, mithin ein Recht auf freie Gestaltung der Lebensführung.[337]

Es mag letztlich zwar sein, dass der EGMR ein Recht auf informationelle Selbstbestimmung in Form eines Rechts auf freie

---

[332] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, §§ 51, 69.
[333] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*.
[334] EKMR, Entscheidung vom 12.10.73 – *X./.Vereinigtes Königreich*; EKMR, Bericht vom 19.05.94 – *Friedl./.Österreich*, §§ 49 ff.; S. auch Neukamm, S. 215.
[335] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, § 57.
[336] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, § 50; Frenz, § 4 Rn. 1197.
[337] s. EKMR, Bericht vom 12.07.77 – *Brüggemann und Scheuten./.BRD*, § 55; s. auch Grabenwarter, § 22 Rn. 13.

Gestaltung der Lebensführung und auf Schutz der Selbstdarstellung[338] in gewissem Maße anerkannt hat, jedoch ist dies keinesfalls mit der deutschen Ausprägung des informationellen Selbstbestimmungsrechts vergleichbar.

2. EINSCHRÄNKUNGEN DES RECHTS NACH ART. 8 II EMRK

Trotz oder gerade aufgrund des weiten Schutzbereichs versucht die Rechtsprechung diesen auf der Rechtfertigungsebene einzuschränken.

Gem. Art. 8 II EMRK darf in das Recht auf Achtung des Privatlebens nur eingegriffen werden, „soweit der Eingriff gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig ist für die nationale oder öffentliche Sicherheit, für das wirtschaftliche Wohl des Landes, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten, zum Schutz der Gesundheit oder der Moral oder zum Schutz der Rechte und Freiheiten anderer".

Zum einen verlangt Art. 8 II EMRK, dass der Eingriff „gesetzlich vorgesehen" sein muss; es muss also im innerstaatlichen Recht eine gesetzliche Grundlage bestehen.[339] Der EGMR hat in der Sache *Kopp*[340] entgegen der Ansicht der schweizerischen Regierung entschieden, dass das Abhören und andere Formen der Überwachung einen schweren Eingriff in Art. 8 I EMRK darstellen würden, der nur aufgrund einer präzisen gesetzlichen Grundlage möglich ist. Der Beschwerdeführer, ein Anwalt, war im Rahmen eines Ermittlungsverfahrens gegen seine Frau telefonisch

[338] So bspw. Grabenwarter, § 22 Rn. 11, der in der Rechtsprechung Peck [§ 60] und Caroline von Hannover [§ 50] das Recht, selbst zu bestimmen, in welcher Art und Weise man sich in der Öffentlichkeit darstellen und wahrgenommen werden möchte, erkennen will.
[339] Meyer-Ladewig (2006), Art. 8 Rn. 38.
[340] EGMR, Urteil vom 25.03.98 – *Kopp./.Schweiz*; Siemen, S. 142.

überwacht worden. Der Beschwerdeführer machte geltend, dass dadurch sein Zeugnisverweigerungsrecht in seiner Eigenschaft als Anwalt missachtet worden sei. Die schweizerische Regierung war jedoch der Ansicht, das Zeugnisverweigerungsrecht hätte nur dann auf den Beschwerdeführer Anwendung gefunden, wenn zwischen dem Telefonat und der Ausübung seines Anwaltsberufes ein Zusammenhang bestanden hätte.[341] Ebenso ließ die Kommission in der Sache *Hewitt und Harman*[342] eine Beschwerde zu, da das geheime Überwachen und Sammeln von Informationen über die Beschwerdeführerinnen nicht auf einer gesetzlichen Grundlage basierten.[343] Auch in der Sache *Sciacca*[344] forderte der Gerichtshof hinsichtlich der Veröffentlichung von Fotos einer Angeklagten eine gesetzliche Grundlage.[345] Unter dem Aspekt „Qualität des Gesetzes" verlangte der Gerichtshof die Regelung ausreichender Sicherheiten gegen Missbrauch. So hat der EGMR in der Sache *Huvig* festgestellt, dass der französische Gesetzgeber nicht mit hinreichender Klarheit die Reichweite und das Ermessen des Ermittlungsrichters – also die gesetzlichen Voraussetzungen einer Abhörmaßnahme – geregelt habe, da weder die möglichen Adressaten des Gesetzes noch die fraglichen Delikte noch die zeitliche Dauer festgelegt worden seien.[346] Auch in der Sache *Malone* hat der Gerichtshof festgestellt, dass die Eingriffe nicht gesetzlich vorgesehen waren.[347]

Vom Gerichtshof heißt „gesetzlich vorgesehen" auch, dass das innerstaatliche Recht die in Art. 8 I EMRK garantierten Rechte vor

---

341 EGMR, Urteil vom 25.03.98 – *Kopp./.Schweiz*, § 72; Siemen, S. 142.
342 EKMR, Entscheidung vom 09.05.89 – *Hewitt und Harmann./.Vereinigtes Königreich*.
343 EKMR, Entscheidung vom 09.05.89 – *Hewitt und Harmann./.Vereinigtes Königreich*, §§ 40 f.; Breitenmoser, S. 76 f.
344 EGMR, Urteil vom 11.01.05 – *Sciacca./.Italien*.
345 EGMR, Urteil vom 11.01.05 – *Sciacca./.Italien*, § 30.
346 EGMR, Urteil vom 24.04.90 – *Huvig./.Frankreich,* § 34; Frowein, in: Frowein-Peukert, Art. 8-11 Rn. 6.
347 EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, § 80.

willkürlichen Eingriffen schützen muss.[348] Willkür kann nur dann ausgeschlossen werden, „wenn das Gesetz für den Bürger zugänglich und vorhersehbar ist“[349]. „Zugänglich“ wiederum bedeutet, dass der Bürger in hinreichender Art und Weise erkennen kann, welche Vorschrift auf den gegenständlichen Fall anwendbar ist und welchen Inhalt die Norm hat.[350] Der Gerichtshof hat die Zugänglichkeit regelmäßig dann bejaht, wenn der Rechtsakt veröffentlicht wurde.[351]

„Vorhersehbar“ ist ein Gesetz, welches so bestimmt ist, dass der Bürger sein Verhalten danach ausrichten kann.[352] Des Weiteren müssen Rechtsakte die Umstände, unter denen ein Eingriff zulässig ist, klar und deutlich beschreiben, so dass diese den rechtsstaatlichen Bestimmtheitsanforderungen genügen. Gerade bei geheimen Maßnahmen sind die Anforderungen an das Gesetz sehr hoch; der Gerichtshof verlangt, dass das Gesetz die Voraussetzungen und das Verfahren des Eingriffs sowie Vorkehrungen gegen Missbrauch bestimmt.[353] In der Sache *U./.BRD* verlangte der EGMR daher die Angabe der Art der Straftaten und die Beschreibung der Personen, gegen die eine Überwachungsmaßnahme gerichtet ist;[354] Des Weiteren verlangte der Gerichtshof gerade für den Fall, dass Daten für die Strafverfolgung und Prävention genutzt werden, detaillierte Regelungen betreffend den Anwendungsbereich sowie bestimmte

---

348 EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, § 67; Siemen, S. 144.
349 So Siemen, S. 144 unter Verweis auf EGMR, Urteil vom 20.05.99 – *Rekvényi./.Ungarn*, § 59.
350 EGMR, Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich,* § 87; Grabenwarter § 18 Rn. 10; Siemen, S. 145.
351 EGMR, Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich*, § 87; Siemen, S. 145.
352 EGMR, Urteil vom 26.04.79 – *Sunday Times I./.Vereinigtes Königreich*, § 49; EGMR, Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich*, § 88; Mayer-Ladewig (2011), Art. 8 Rn. 103; Siemen, S. 145.
353 EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 51; Unger, S. 134; Breitenmoser, S. 75; Grabenwarter, § 22 Rn. 35.
354 EGMR, Urteil vom 02.09.10 – *U./.BRD*, § 65.

Sicherungsvorkehrungen, wie bspw. hinsichtlich des Zugangs Dritter zu den Daten, Maßnahmen zur Sicherstellung der Richtigkeit der Daten sowie Regelungen zur Löschung.[355] Vorhersehbarkeit bedeutet jedoch nicht, dass eine Person genau erkennen können muss, wann Abhörmaßnahmen möglich sind, so dass sie ihr Verhalten anpassen kann, sondern nur, unter welchen Voraussetzungen und auf welche Art und Weise eine Maßnahme vorgenommen werden kann.[356] Problematisch sind jedoch die Gesetze, welche einen Bewertungsspielraum einräumen. Der Gerichtshof verlangt, dass in einem solchen Gesetz der Umfang des Spielraums bestimmt sein muss.[357] Da gerade bei Ermessensentscheidungen das Missbrauchspotential sehr hoch ist, verlangt die Rechtsprechung u.a. Regelungen über die kontrollierenden Stellen, die Art und Weise der Kontrolle, die Dauer und die Gründe für eine Kontrolle[358] sowie Vorschriften über den Anwendungsbereich und die Art und Weise der Ermessensausübung, um sowohl dem Richter den Spielraum vorzugeben als auch dem Betroffenen einen Mindestschutz zu garantieren.[359] Neben den Rechtsakten müssen auch Weisungen und die Verwaltungspraxis berücksichtigt werden, soweit deren Inhalt veröffentlicht wurde.[360] So hatte der EGMR in der Sache *Leander* die entsprechende Vorschrift („Personnel Control Ordinance"), welche die Weiterleitung von im Polizeiregister gespeicherten Informationen erlaubt, als vorhersehbar angesehen. Trotz weitem Ermessen hinsichtlich der Art der gespeicherten Informationen enthielt die Verordnung detaillierte Vorschriften

[355] EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, § 99.
[356] EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, § 67; Siemen, S. 147.
[357] EGMR, Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich,* § 88; s. auch EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 51; Siemen, S. 146.
[358] EGMR, Urteil vom 24.09.92 – *Herczegfalvy./.Österreich*, § 91; EGMR, Urteil vom 04.07.00 – *Niedbala./.Polen*, § 81.
[359] EGMR, Urteil vom 21.10.96 – *Domenichini./.Italien*, § 33.
[360] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 51; EGMR, Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich*, § 88.

über das Sammeln, die Verarbeitung und die Weitergabe der Informationen. Es waren die Empfänger-Behörden, die Regelungen über das Verfahren sowie die Umstände, welche bei einer Weitergabe zu beachten sind, geregelt.[361] Ebenso hat der EGMR in der Sache *M.S./Schweden* die Übermittlung der Daten von der Klinik an die Sozialversicherungsstelle als ordnungsgemäß angesehen. Obwohl die entsprechende Übermittlungsvorschrift vorsieht, dass nur Daten, welche auch tatsächlich verlangt worden sind, übermittelt werden dürfen, haben die Kliniken weit über das Anforderungsgesuch hinausgehende Daten übermittelt. Der Gerichtshof hat jedoch entschieden, dass der Umfang der Übermittlungsverpflichtung von der Relevanz der Informationen abhinge; der Wortlaut des Gesuchs sei unwesentlich.[362] Anders hat der EGMR in der Sache *Rotaru* entschieden. Die Rechtsgrundlage, auf welche sich die Regierung berief, gestattete es den Behörden, Daten zu sammeln, zu speichern und zu benutzen, welche Bedeutung für die nationale Sicherheit haben. Der Gerichtshof bemängelte jedoch die Vorhersehbarkeit der Rechtsgrundlage, da die Grenzen der Befugnisse und der Verarbeitung nicht festgelegt worden waren. Insbesondere seien weder die Art der Informationen noch eine Zweckbestimmung noch das Verfahren noch die Aufbewahrung noch die Rechte der Betroffenen geregelt worden.[363] Des Weiteren verlangt der Gerichtshof die Benennung der zugriffsberechtigten Personen sowie Löschungsregelungen.[364]

Die Liste der legitimen Zwecke ist abschließend und aufgrund des Ausnahmecharakters der Vorschrift eng auszulegen.[365] Andererseits hat der EGMR bisher keine abschließenden

[361] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, §§ 52, 55; Siemen, S. 146.
[362] EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*, § 37; Siemen, S. 146 f.
[363] EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, § 57; Siemen, S. 149; Grabenwarter, § 22 Rn. 35.
[364] EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien,* § 57; Siemen, S. 149 f.
[365] EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, § 47.

Definitionen vorgenommen, weshalb den Mitgliedstaaten ein großer Bewertungsspielraum zusteht. Eine Eingrenzung findet daher meist erst auf der Verhältnismäßigkeitsebene statt.[366] Es stellt sich daher die Frage, ob die legitimen Ziele überhaupt beschränkend wirken. Der Gerichtshof hat in der Sache *Z./.Finnland*[367] Zweifel geäußert, ob die Maßnahmen (Bekanntgabe des Namens und der medizinischen Informationen) einem legitimen Grund gem. Art. 8 II EMRK dienen.[368] Der Ehemann der Beschwerdeführerin hatte mehrere Sexualstraftaten begangen und dabei die betroffenen Frauen der Ansteckung mit dem HI-Virus, mit dem er infiziert war, ausgesetzt. Die Beschwerdeführerin machte in der Hauptverhandlung von ihrem Zeugnisverweigerungsrecht Gebrauch, infolgedessen die medizinischen Unterlagen der Beschwerdeführerin beschlagnahmt und den Ermittlungsakten beigefügt wurden. Die Beschwerdeführerin wandte sich gegen die Beschlagnahme der Unterlagen, die Veröffentlichung dieser Unterlagen bereits nach zehn Jahren und die Nennung ihres Namens sowie entsprechender Details im Urteil, da die sie betreffenden Daten keine Bedeutung für das Strafverfahren ihres Mannes hätten. Durch die Zweifel des Gerichts lässt sich zumindest vermuten, dass die Aufzählung der legitimen Gründe nicht nur ein hohles Gebilde ist.[369]

Art. 8 II EMRK verlangt weiter, dass der Eingriff „in einer demokratischen Gesellschaft notwendig ist“. Der Eingriff ist notwendig, „wenn ein dringendes gesellschaftliches Bedürfnis (…) für die Grundrechtseinschränkung angenommen wird und die

[366] Siemen, S. 151.
[367] Siemen, S. 152.
[368] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*, § 77.
[369] Siemen, S. 151 f.

Maßnahme verhältnismäßig zum legitimen Ziel ist".[370] Hinsichtlich der Auswahl des Mittels und der Einschätzung, ob der Einsatz dieses Mittels gerechtfertigt ist, kommt den Behörden ein großer Beurteilungsspielraum zu.[371] Dieser ändert sich entsprechend den Umständen[372] und je nach Rechtfertigungsziel[373].[374] Je schwerwiegender der Eingriff oder je sensibler der Bereich, desto enger ist der Beurteilungsspielraum.[375] Auf der anderen Seite rechtfertigen die Verhinderung von Straftaten oder Handlungen zum Schutz der nationalen Sicherheit Grundrechtsbeeinträchtigungen in höherem Maße, als es bspw. Handlungen zum Schutz des wirtschaftlichen Wohls vermögen.[376] Eine unterschiedliche Gewichtung kann auch aufgrund von Eingriffshandlungen oder entsprechend dem Adressatenkreis vorgenommen werden; so maßen die Rechtsprechungsorgane dem Kampf gegen Terroristen einen größeren Stellenwert bei als Ermittlungen gegen einen „harmlosen" Delinquenten.[377] Aufgrund des möglichen Missbrauchs darf ein Eingriff außerdem nur dann als „notwendig" in einer „demokratischen Gesellschaft" angesehen werden, wenn in der Rechtsgrundlage hinreichende Garantien zur Absicherung vorgesehen sind.[378] Das Bedürfnis für solche Sicherheitsvorkehrungen ist umso größer, wenn die Daten automatisch verarbeitet und für polizeiliche Zwecke genutzt

[370] So Siemen, S. 153 und st. Rspr. des EGMR, u.a. Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich*, § 97 und Urteil vom 26.03.87 – *Leander./.Schweden*, § 58.
[371] Siemen, S. 154 f.
[372] EGMR, Urteil vom 28.11.84 – *Rasmussen./.Dänemark*, § 40.
[373] EGMR, Urteil vom 26.04.79 – *Sunday Times./.Vereinigtes Königreich*, § 59; EGMR, Urteil vom 22.10.81 – *Dudgeon./.Vereinigtes Königreich*, § 52.
[374] Siemen, S. 155.
[375] Vgl. bis hierher Siemen, S. 154 ff.
[376] Breitenmoser, S. 79.
[377] EKMR, Bericht vom 18.03.81 – *McVeigh u.a./.Vereinigtes Königreich*, §§ 230 f.
[378] EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, § 81.

werden.[379] Der Gerichtshof hat dabei umfangreiche Überprüfungsmöglichkeiten.[380]

In der Sache *X./.BRD* hat die Kommission entschieden, dass es im Interesse der nationalen Sicherheit und zur Verhütung von Straftaten notwendig ist, Akten anzulegen, Fingerabdrücke zu nehmen sowie Fotoaufnahmen zu fertigen. Die Aufbewahrung in manuellen Akten sei daher keine große Bedrohung für den Einzelnen.[381] Gleichermaßen entschied die Kommission im Fall *Friedl*, in dem die Daten ebenfalls nur in einer einfachen Verwaltungsakte gespeichert worden waren. Die Vernehmung des Beschwerdeführers sei notwendig gewesen, um beurteilen zu können, ob eine Anklage erhoben wird.[382] Hinsichtlich des Ziels „Schutz der nationalen Sicherheit" nimmt der Gerichtshof einen weiten Spielraum bei der Auswahl der Mittel an;[383] Zudem kann es der Schutz der nationalen Sicherheit gebieten, persönliche Daten zu sammeln, sie an andere staatliche Stellen weiterzugeben und dem Betroffenen die Information darüber zu versagen, da eine nachträgliche Benachrichtigung u. U. zur „Aufdeckung der Arbeitsweise und Beobachtungsfelder der Geheimdienste führen und möglicherweise sogar zur Identifizierung ihrer Agenten beitragen" könnte.[384] Der Gerichtshof wertet das Interesse des Staates an der Verbrechensbekämpfung höher als die Rechte des Einzelnen. Heutzutage wird diese Gewichtung aufgrund der technischen Modifikationen, insbesondere der Vernetzung der Datenbanken, nicht mehr bestehen bleiben können.[385]

---

379 EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, § 103.
380 Mayer-Ladewig (2006), Art. 8 Rn. 42, 44, 45a.
381 EKMR, Bericht vom 18.03.81, DR 25, 15 (50) – *McVeigh u.a./Vereinigtes Königreich*; Siemen, S. 157.
382 EKMR, Bericht vom 19.05.94 – *Friedl./.Österreich*, § 66; Siemen, S. 158.
383 EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 59; Grabenwarter § 22 Rn. 38.
384 EGMR, Urteil vom 06.09.78 – *Klass u.a./.BRD*, § 58; EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 59; Grabenwarter, § 22 Rn. 36.
385 Siemen, S. 159.

Andererseits verleitet die Bedrohung durch den Terrorismus die Rechtsprechungsorgane immer wieder zu etwas großzügigeren Verhältnismäßigkeitsprüfungen. So hielt die Kommission in der Sache *McVeigh* die Durchsuchung der Verdächtigen und das Abnehmen der Fingerabdrücke für gerechtfertigt. Auch die Aufbewahrung sei nicht unverhältnismäßig, obwohl kein Verdacht für die Begehung einer Straftat vorlag. Für die Kommission reicht es aus, dass die Aufbewahrung der Akten der Verhinderung terroristischer Akte dient.[386] Anderer Ansicht war das Kommissionsmitglied Klecker, welcher die Durchsuchung für angemessen hielt, den Einbehalt der Akten jedoch nicht als gerechtfertigt ansah, v.a. wenn sich der Verdacht gegen den Betroffenen nicht erhärtet hat. Auch während der Prüfung habe es keine Tatsachen gegeben, welche den Verdacht gestützt hätten.[387] Ähnlich beurteilte die Kommission die Situation in der Sache *A, B, C und D./.BRD*. Die Beschwerdeführer waren verdächtig, terroristische Propaganda verteilt und mit der Baader-Meinhof-Gruppe in Verbindung gestanden zu haben. Die Kommission hatte daher die Aufbewahrung von Daten über den tatsächlichen Bedarf hinaus für gerechtfertigt gehalten.[388] Gleichwohl betont der EGMR, dass staatliche Maßnahmen nicht die Demokratie untergraben dürften, weswegen angemessene und effektive Sicherungen zum Schutz des Betroffenen vorhanden sein müssen.[389] Obwohl das Urteil *Leander* hinsichtlich der Anerkennung des Schutzes von Informationen als fortschrittlich gilt, so erstreckt sich dies nicht auf die Rechtfertigungsebene. Der Gerichtshof hat zwar auch hier Maßnahmen zum Schutz vor Missbrauch gefordert. Da die schwedischen Vorschriften aber nach Meinung des EGMR

[386] EKMR, Entscheidung vom 04.10.62 – *G.W./.BRD*; Siemen, S. 159 f.
[387] EKMR, Bericht vom 18.03.81 – *McVeigh u.a../.Vereinigtes Königreich*, Dissenting Opinion of Mr. Klecker; Breitenmoser, S. 241.
[388] EKMR, Entscheidung vom 13.12.79, DR 18, 176 f. (180) – *A, B, C und D./.BRD*.
[389] EGMR, Urteil vom 06.09.78 – *Klass u.a./.BRD*, §§ 48 ff.; EGMR, Urteil vom 24.04.90 – *Kruslin./.Frankreich,* §§ 34 ff.; Grabenwarter § 22 Rn. 39.

ausreichenden Schutz vorsahen, sah der EGMR den Eingriff als gerechtfertigt an.[390] Lediglich die Richter Pettiti und Russo warnten im Zuge dieser Entscheidung vor der elektronischen Vernetzung zwischen den Polizeiregistern.[391] Diese Entscheidungen machen deutlich, dass die Straßburger Organe die terroristische Bedrohung als ernst zu nehmende Gefahr betrachten.[392] Die Bedrohung hat sich seit den 70er Jahren nicht verringert, sondern nur gewandelt. Es ist folglich zum Schutz der nationalen Sicherheit erforderlich, die Ermittlungsmethoden anzupassen. Eingriffsbefugnisse müssen daher mit den technischen Möglichkeiten mitwachsen, um dem Staat eine Chance gegen die terroristische Bedrohung einzuräumen.[393] Indes darf ein Staat für den Kampf gegen den Terrorismus nicht zu jeder Maßnahme greifen. Dies beurteilt sich vielmehr „nach allen Umständen des Falles (…), wie Art, Umfang und Dauer der möglichen Maßnahme, die für ihre Anordnung erforderlichen Gründe, die für ihre Zulassung, Ausführung und Kontrolle zuständigen Behörden und die Art der im nationalen Recht vorgesehenen Rechtsbehelfe“[394].

Dem Schutz besonders sensibler Daten, wie bspw. medizinischen Daten, hat der EGMR besondere Bedeutung zuerkannt.[395] So stellte er im Fall *Z./.Finnland* fest, dass die Vertraulichkeit der Informationen nicht nur dem Schutz der Privatsphäre des Einzelnen dient, sondern auch dem Vertrauen in die medizinischen Berufe. Ein Patient darf nicht davon abgehalten werden, sich medizinische Hilfe zu sichern, weil er die Veröffentlichung seiner Daten befürchtet. Daher sei dem

390 EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 67; Siemen, S. 163.
391 EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, Partially dissenting opinion of Jugdes Pettiti und Russo.
392 So auch bereits in EGMR, Urteil vom 28.10.94 – *Murray./.Vereinigtes Königreich*, §§ 92 ff.
393 So auch Siemen, S. 164.
394 EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, §§ 49 f.
395 Siemen, S. 165.

Schutzbedürfnis des Einzelnen Vorrang gegenüber der Verfolgung von Straftaten einzuräumen.[396] Sollte dennoch ein Eingriff in das Recht des Betroffenen erforderlich sein, so müssten ausreichende Garantien gegen Datenmissbrauch vorhanden sein. Der Gerichtshof erkennt an – entsprechend Art. 9 DSK –, dass Ausnahmen und Einschränkungen zur Bekämpfung von Straftaten auch zu Lasten der sensiblen Daten gem. Art. 6 DSK gehen können.[397] Eine Weitergabe von Daten ohne die Einwilligung des Betroffenen sei hingegen nur unter engen Voraussetzungen möglich.[398] Der EGMR kommt dann zu dem Schluss, dass eine Verschlusszeit von nur zehn Jahren und die Offenlegung der persönlichen und medizinischen Daten der Beschwerdeführerin unverhältnismäßig waren.[399] Anderer Ansicht war Richter de Meyer, nach dessen Ansicht medizinische Daten dauerhaft unter Verschluss gehalten werden müssten.[400] In der Sache *M.S./Schweden* bejahte der Gerichtshof hingegen die Verhältnismäßigkeit aufgrund zahlreicher Schutzvorkehrungen gegen Missbrauch, insbesondere waren sämtliche Zugriffsberechtigte zum vertraulichen Umgang mit den Daten verpflichtet, deren Nichtbeachtung zivil- oder strafrechtliche Folgen nach sich gezogen hätte. Nach Ansicht des EGMR blieb den Behörden mangels anderweitiger Informationsquelle keine andere Möglichkeit als die Beschaffung der Daten von den Kliniken.[401] Ebenso urteilte die Kommission in der Sache *L./.BRD*, wonach die vertrauliche Behandlung durch den Berichterstatter und der Verwendungszweck der Daten den Eingriff rechtfertigen

[396] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*, §§ 95 ff.; Grabenwarter § 22 Rn. 39; Siemen, S. 165.
[397] EGMR; Urteil vom 25.02.97 – *Z./.Finnland*, § 97; Siemen, S. 165.
[398] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*, §§ 95 ff.; Mayer-Ladewig (2006), Art. 8 Rn. 11.
[399] EGMR, Urteil vom 25.02.97 – *Z./.Finnland,* §§ 112 f.
[400] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*, Partially Dissenting opinion of Judge de Meyer; Siemen, S. 166.
[401] EGMR, Urteil vom 27.08.97 – *M.S../.Schweden*, § 42; Siemen, S. 166 f.

würden.[402] Freilich lassen sich aus den Urteilen keine allgemeinen Prinzipien für die Rechtmäßigkeit einer Maßnahme ableiten, jedoch sind die Anforderungen an die staatlichen Maßnahmen überaus hoch.[403]

Im Rahmen der Verhältnismäßigkeitsprüfung achten die Rechtsprechungsorgane besonders darauf, ob geeignete Schutzmaßnahmen des Staates vorhanden sind. Der Staat hat folglich zum Schutz des Betroffenen sinnvolle und angemessene Maßnahmen zu treffen.[404] So hat der EGMR im Fall *Leander* die Überwachung durch das Parlament sowie durch unabhängige Instanzen als ausreichend angesehen, wodurch einem Missbrauch vorgebeugt würde und damit ein Ausgleich für die Geheimhaltung der Datensammlung geschaffen wäre. Da es sich im Fall *Leander* um eine geheime Überwachungsmaßnahme gehandelt hatte, waren aufgrund der Missbrauchsgefahr besonders hohe Anforderungen hinsichtlich der Schutzmaßnahmen zu erfüllen.[405] Ebenso hat die Kommission im Fall *Census Regulations 1981* die Verhältnismäßigkeit bejaht, da die Formulare streng vertraulich behandelt und die Antworten nur für Statistiken benötigt wurden; Daten wie Name und Anschrift seien nicht in die elektronische Datenverarbeitung aufgenommen worden. Die Verschlusszeit der Erhebungsbögen von 100 Jahren wurde ebenfalls von der Kommission entsprechend positiv gewürdigt.[406] Indessen hat der Gerichtshof in der Sache *Peck* die Veröffentlichung des Videomaterials als unverhältnismäßig angesehen, da keinerlei Versuche zum Schutz des Privatlebens des Beschwerdeführers

[402] EKMR, Entscheidung vom 13.10.88 – *L./.BRD*.
[403] Siemen, S. 167.
[404] EGMR, Urteil vom 21.02.90 – *Powell und Rayner./.Vereinigtes Königreich,* § 41; EGMR, Urteil vom 19.02.98 – *Guerra u.a./Italien,* § 58; Grabenwarter § 22 Rn. 53.
[405] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 60; Siemen, S. 174.
[406] EKMR, Entscheidung vom 06.10.82, DR 30, 239 (240) – *Census Regulations*; Siemen, S. 174 f.; Ellger, S. 137.

unternommen worden waren.[407] Zu den weiteren Pflichten des Staates gehört die Bereitstellung der Möglichkeit, sich durch Rechtsbehelfe gegen Beeinträchtigungen wehren zu können, mithin durch verfahrensrechtliche Garantien.[408] Auch wenn sie erst in Pkt. C. I. näher erörtert werden, so sind diese Garantien doch mit dafür ausschlaggebend, ob der Staat innerhalb seines Beurteilungsspielraums gehandelt hat. Des Weiteren ist der Aspekt der Information des Betroffenen nicht zu vernachlässigen. Zwar verneinte der EGMR einen grundsätzlichen Anspruch auf nachträgliche Benachrichtigung, da damit der langfristige Zweck der Ermittlungsmaßnahme gefährdet werden könnte und die Aufdeckung der Arbeitsweise und der Beobachtungsfelder des Geheimdienstes einschließlich der möglichen Identifizierung der Agenten riskiert würde. Dennoch erinnert er an das Urteil des deutschen Bundesverfassungsgerichts vom 15.12.1970, wonach der Betroffene nach Abschluss einer Ermittlungsmaßnahme über diese informiert werden muss, sofern dies ohne Gefährdung des Ermittlungszwecks möglich ist.[409] Ein gänzlicher Ausschluss der nachträglichen Benachrichtigung kommt hingegen nicht in Betracht, da man damit nach Ansicht von *Breitenmoser* gegen die grundsätzliche Unschuldsvermutung verstoßen würde. Die nachträgliche Benachrichtigung diene letztlich auch dem Image der Strafverfolgungsorgane, welche damit dem Verdacht, grundlose Ermittlungen anzustellen, begegnen würden. Für die Benachrichtigung spricht auch, dass der Betroffene nur so die Möglichkeit erhält, die Maßnahme anzugreifen, was wiederum der Rechtsstaatlichkeit Ausdruck verleiht.[410]

---

[407] EGMR, Urteil vom 28.01.03 – *Peck./.Vereinigtes Königreich*, § 85; Siemen, S. 175.
[408] EGMR, Urteil vom 26.03.85 – *X und Y./.Niederlande*, § 27; EGMR, Urteil vom 27.05.04 – *Connors./.Vereinigtes Königreich*, §§ 83, 92 ff.; Mayer-Ladewig (2006), Art. 8 EMRK, Rn.2a.
[409] EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, § 58; Schrepfer, S. 59.
[410] Breitenmoser, S. 197 f.

In der Sache *Van der Velden./.Niederlande* hat der EGMR die Beschwerde eines Verurteilten wegen Erhebung und Speicherung seiner DNA-Daten noch mit der Begründung zurückgewiesen, dass die DNA-Aufzeichnungen in den letzten Jahren einen wertvollen Beitrag zur Strafverfolgung geliefert haben. Zudem ging der EGMR damals noch davon aus, dass eine solche Speicherung in der DNA-Datei schließlich auch von Nutzen für den Betroffenen sei, insbesondere um ihn bei künftigen Straftaten von jeglichem Verdacht freizusprechen.[411] Allerdings gestalteten sich die gesetzlichen Bedingungen im Fall *S.&Marper./.Vereinigtes Königreich* wesentlich anders, so dass der EGMR dazu ausführlicher Stellung nahm. So stellte sich der EGMR die Frage, ob es gerechtfertigt sei, wenn DNA- und Fingerabdruckdaten gespeichert bleiben, obwohl die Betroffenen entweder freigesprochen oder das Verfahren eingestellt wurde. Des Weiteren stellte sich die Frage, ob die dauerhafte Speicherung der Daten gerechtfertigt ist.[412] Der EGMR führte hierzu aus:

> *„In this respect, the Court is struck by the blanket and indiscriminate nature oft he power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offende; fingerprints and samples may be taken from a person of any age (...), which includes minor or non-imprisonable offences. The retention is not time-limited. (...) Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database*

[411] EGMR, Urteil vom 07.12.06 – *Van der Velden./.Niederlande*.
[412] EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, §§ 106, 114.

or the materials destroyed (...); in particular, there is no provision for independent review (...)".[413]

Des Weiteren hat der EGMR festgestellt, dass nicht-verurteilte Betroffene ebenso sehr stigmatisiert werden wie verurteilte Personen. Überdies hat der verantwortliche Staat jedweden Beurteilungsspielraum überschritten, so dass davon auszugehen ist, dass die weitergehende Speicherung nicht als „notwendig in einer demokratischen Gesellschaft" angesehen werden kann.[414]

Zusammenfassend lässt sich damit sagen, dass die Straßburger Organe die Verhältnismäßigkeit im Wesentlichen von den getroffenen Vorkehrungen gegen Missbrauch abhängig machen.[415]

Natürlich hat der EGMR weitere Urteile[416] zum Recht auf Privatsphäre, insbesondere im Bereich des Schutzes persönlicher Daten, gefällt, welche jedoch nicht mehr besprochen werden, da diese im Wesentlichen die gleichen Inhalte wie die vorgenannten haben oder für die nachfolgende Untersuchung nicht von Bedeutung sind.

3. ZUSAMMENFASSUNG DER RECHTSPRECHUNG ZU ART. 8 EMRK

Da die Rechtsprechung zu Art. 8 EMRK recht umfangreich ausgefallen ist, wird diese zunächst in ihren wesentlichen Zügen zusammengefasst, bevor eine Betrachtung der ePass-Regelungen und der Prüm-Regelungen anhand der Rechtsprechung vorgenommen wird.

---

413 So EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich,* § 119.
414 EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, §§ 122, 125.
415 So Siemen, S. 176.
416 So z.B. EGMR, Urteil vom 01.07.08 – *Liberty u.a./.Vereinigtes Königreich*; EGMR, Urteil vom 12.05.00 – *Khan./.Vereinigtes Königreich*; EGMR, Urteil vom 09.06.09 – *Kvasnica./.Slovakei*; EGMR, Urteil vom 18.05.10 – *Kennedy./.Vereinigtes Königreich*; EGMR, Urteil vom 27.04.10 – *Ciubotaru./.Moldavien*; EGMR, Urteil vom 02.12.08 – *K.U./.Finnland*; EGMR, Urteil vom 10.03.09 – *Bykov./.Russland*; EGMR, Urteil vom 03.04.07 – *Copland./.Vereinigtes Königreich*.

Betrachtet man die vorangestellte Rechtsprechung, so kommt man zu dem Ergebnis, dass dem Schutz der persönlichen Daten mehr und mehr Bedeutung zugemessen wird. War anfangs in der Rechtsprechung ein direkter Bezug zum Privatleben erforderlich, sei es durch die Entstehung der Bilder, den Aufenthaltsort des Betroffenen oder den Inhalt der Daten, so haben die Rechtsprechungsorgane nun weitere Kriterien entwickelt.

Die Kommission entschied je nach Art und Weise der Informationsbeschaffung, der Qualität der Daten sowie der beabsichtigten Verwendung über das Vorliegen eines Eingriffs. Der Kommission reicht schon das Sammeln von Daten aus, wobei auch eine offene Erhebung eine Verletzung des Art. 8 I EMRK herbeiführen kann.[417] Auch die Aufbewahrung und Weiterleitung einer Akte an ein Gericht kann eine Beeinträchtigung darstellen, was jedoch vom Inhalt der jeweiligen Akte abhängt, insbesondere wenn es um Verbindungen oder Handlungen des Individuums geht. Weitere Anhaltspunkte für das Vorliegen eines Eingriffs sind die nachträgliche Datenverarbeitung und die damit möglicherweise verbundene Zweckänderung[418] sowie eine möglicherweise nachfolgende Vernetzung der Daten[419]. Auch die Speicherung und Verarbeitung von Informationen stellen einen Eingriff dar, wobei jedoch durch den Inhalt der Daten ein Bezug zum Privatleben vorliegen muss. Ebenso können geheime Überwachungen zu einer Beeinträchtigung führen.[420] Besonders wichtig sind sensible Daten (medizinische, religiöse, etc.), da

[417] EKMR, Entscheidung vom 06.10.82, DR 30, 239 (240) – *Census Regulations*.
[418] S. Siemen, S. 106 f. unter Bezugnahme auf EKMR, Entscheidung vom 19.05.94 – *Friedl./.Österreich*.
[419] EKMR, Entscheidung vom 01.12.85, DR 30, 239 (240) – *Lundvall./.Schweden*.
[420] EKMR, Entscheidung vom 28.10.97 – *Tsavachidis./.Griechenland*, § 48.

durch deren Vorliegen eine beträchtlich hohe Eingriffsqualität erreicht wird.[421]

Keine Beeinträchtigung stellen nach der Kommission hingegen die Aufbewahrung kriminalpolizeilicher Akten, v.a. wenn diese der Verhinderung terroristischer Straftaten dient,[422] oder die Verwendung von Identifikationsnummern aufgrund der Möglichkeit des erleichterten Datenabgleichs dar[423]. Auch wenn Fotos ursprünglich mit Willen des Betroffenen gemacht worden sind und diese nun zur Identifizierung von Straftätern genutzt werden, sei dies keine Beeinträchtigung.[424] Später hat die Kommission dann allerdings den Zweckbindungsgrundsatz anerkannt, auch wenn sie letztlich das Fotografieren in einer Radarfalle nicht als Eingriff gewertet hat.[425]

Während die Kommission für die Bejahung eines Eingriffs den Nachweis der Datenerhebung fordert[426], reicht dem Gerichtshof die latente Möglichkeit der Überwachung durch entsprechende Gesetze, Maßnahmen etc. aus.[427]

Natürlich ist nicht zu vergessen, dass die Kommission bereits seit 1998 nicht mehr existiert, weswegen die Kommission ihre Entscheidungen nicht mehr an die technischen Fortschritte anpassen konnte.

Der Gerichtshof hat eine Reihe von Anhaltspunkten für das Vorliegen eines Eingriffs entwickelt. Als Kriterien für die Bejahung eines Eingriffs hat er zunächst in der Sache *Rotaru* die

---

421 EKMR, Entscheidung vom 13.10.88 – *L./.BRD*; EKMR, Entscheidung vom 28.10.97 – *Tsavachidis./.Griechenland*, § 48.
422 Siemen, S. 157 unter Bezugnahme auf EKMR, Entscheidung vom 04.10.62 – *G.W./.BRD*.
423 EKMR, Entscheidung vom 09.09.92 – *Reyntjens./.Belgien*, § 2.
424 EKMR, Entscheidung vom 07.12.92 – *Lupker./.Niederlande*, § 5.
425 EKMR, Entscheidung vom 06.09.95 – *Campion./.Frankreich*.
426 EKMR, Entscheidung vom 06.07.88 – *Hilton./.Vereinigtes Königreich*.
427 EGMR, Urteil vom 02.08.84 – *Malone./.Vereinigtes Königreich*, § 64.

systematische Sammlung und Speicherung angesehen, in der nachfolgenden Sache *P.G. und J.H.* sowie in *Peck* jedoch entweder die systematische Sammlung oder die dauerhafte Aufzeichnung für einen Eingriff ausreichen lassen.[428] Wenn Daten systematisch gesammelt und gespeichert werden, so stellt dies nach Ansicht des Gerichtshofes – entgegen der Kommission – auch dann eine Beeinträchtigung dar, wenn die Informationen ursprünglich frei verfügbar und zugänglich waren.[429] Die öffentliche Überwachung durch technische Hilfsmittel ist grundsätzlich der Beobachtung durch eine andere Person, bspw. einen Passanten, gleichzusetzen. Dies gilt jedoch dann nicht, wenn Hilfsmittel eingesetzt werden, die menschliche Schwächen bei der Wahrnehmung oder dem Erinnerungsvermögen ausgleichen oder sogar übersteigen, v.a. durch Speicherung von Verhaltensweisen, wie es bspw. bei der Videoüberwachung oder einer Tonbandaufnahme der Fall ist, d.h. bei Aufzeichnung des Materials.[430] Dem „Beobachten" steht das bloße Abhören gleich. Auch die Weiterleitung oder Zur-Verfügung-Stellung von Daten im Zusammenhang mit dem Inhalt dieser Daten kann einen Eingriff darstellen, auch wenn diese Daten nur einem begrenzten Personenkreis bekanntgemacht werden.[431] Ebenso haben die Speicherung und Verarbeitung von Daten Eingriffsqualität.[432] Außerdem hat der Gerichtshof festgestellt, dass mit der Dauer der Aufbewahrung die steigende Privatheit der Informationen einhergeht;[433] auch öffentliche Handlungen werden zunehmend privater, wenn sie dokumentiert und für lange Zeit aufbewahrt werden.[434] Hinsichtlich der Dauer der Aufbewahrung

[428] S. auch EGMR, Urteil vom 02.09.10 – *U./.BRD*, § 44.
[429] EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, §§ 46, 63.
[430] so EGMR, Urteil vom 17.07.03 – *Perry./.Vereinigtes Königreich*, §§ 38, 40 f.; Urteil vom 28.01.03 – *Peck./.Vereinigtes Königreich*, § 59; vgl. auch Siemen, S. 127.
[431] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*.
[432] EGMR, Urteil vom 16.02.00 – *Amann./.Schweiz*, § 70.
[433] Vgl. Siemen S. 124.
[434] So auch Siemen, S. 124 f.

hat die Kommission im Fall *Williams./.Vereinigtes Königreich* festgestellt, dass eine Frist von elf Monaten für die Speicherung von DNA nicht unangemessen ist, sofern die Daten in einem Mordfall benötigt würden.[435] Ebenso ist die Erwartungshaltung einer Person an die Privatsphäre in die Erwägung einzubeziehen.[436] Seit der Rechtsprechung zu *Amann* ist zusätzlich die DSK ein wichtiges Kriterium bei der Frage des Vorliegens einer Beeinträchtigung.[437] Allerdings wird die DSK in diesem Abschnitt nur indirekt einbezogen, da sie in Pkt. II. besondere Beachtung findet.

Entgegen der engen Sicht der Kommission, welche inhaltlich einen Bezug zum Privatleben fordert, sieht der Gerichtshof bereits in der Qualität des Eingriffs, bspw. in einer langen Aufbewahrungsdauer, oder der Erwartungshaltung den Bezug zum Privatleben.

Der Gerichtshof unterstellt ferner medizinische Daten dem Schutzbereich des Art. 8 EMRK.[438] Zudem ist die psychische und physische Integrität des Individuums geschützt, d.h. die Entnahme von Blut, erkennungsdienstliche Maßnahmen sowie Urinproben beeinträchtigte den Einzelnen in seinem Recht auf Privatleben. Das Recht am eigenen Bild ist ebenfalls vom Schutzbereich des Art. 8 I EMRK umfasst, wobei allerdings entscheidend ist, ob die Person bei einer privaten oder öffentlichen Betätigung abgebildet wurde.[439] Dabei sind nicht nur Äußerlichkeiten geschützt, sondern auch Teile der Identität der Person wie der Name oder die

[435] EKMR, Entscheidung vom 01.07.92 – *Williams./.Vereinigtes Königreich*; Siemen, S. 136.
[436] EGMR, Urteil vom 25.09.01 – *P.G. und J.H./Vereinigtes Königreich,* § 57; EGMR, Urteil vom 17.07.03– *Perry./.Vereinigtes Königreich*, § 41.
[437] EGMR, Urteil vom 16.02.00 – *Amann./.Schweiz*, § 65.
[438] EGMR, Urteil vom 25.02.97 – *Z./.Finnland*, §§ 88, 93; EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*; § 41.
[439] EGMR, Urteil vom 21.02.02 – *Schüssel./.Österreich*, § 2; EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, §§ 50, 69.

Stimme.[440] Auch hat der Staat die positive Verpflichtung, zum Schutz des Einzelnen tätig zu werden.[441]

Der EGMR hat auch explizit zur Verwertung von DNA und Fingerabdrücken Stellung genommen und festgestellt, dass es sich um sensible personenbezogene Daten handelt, welche Informationen über die Gesundheit und auch über Verwandtschaftsbeziehungen sowie über die ethnische Herkunft enthalten. Auch stelle die Speicherung der Daten in nationalen Datenbanken eine Beeinträchtigung dar.

Die Rechtfertigung der Beeinträchtigungen beurteilt sich anhand Art. 8 II EMRK.

Die Rechtsprechung verlangt, dass ein Eingriff gesetzlich vorgesehen sein muss, d.h. dass eine präzise gesetzliche Grundlage vorhanden sein muss, welche auch Regelungen zur Absicherung vor Missbrauch enthält.[442] Dabei müssen sowohl die Reichweite des Ermessens als auch die möglichen Adressaten einer Maßnahme als auch die fraglichen Delikte als auch die zeitliche Dauer der Maßnahme festgelegt sein.[443] Des Weiteren muss ein Schutz vor willkürlichen Maßnahmen vorgesehen sein; dies kann dadurch erreicht werden, dass das Gesetz zugänglich und vorhersehbar ist. Zugänglich bedeutet, dass der Bürger mit hinreichender Sicherheit erkennen kann, welche Vorschrift anwendbar ist und welchen Inhalt die Norm hat; dies geschieht regelmäßig durch Veröffentlichung der Vorschrift. Vorhersehbar ist ein Gesetz, welches so hinreichend bestimmt ist, dass der Einzelne sein Verhalten danach ausrichten kann, d.h. er muss

---

[440] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, § 50.
[441] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, § 57.
[442] S. u.a. EGMR, Urteil vom 25.03.98 – *Kopp./.Schweiz, § 72.*; EGMR, Urteil vom 09.05.89 – *Hewitt und Harman./.Vereinigtes Königreich*, §§ 40 f.; EGMR, Urteil vom 11.01.05 – *Sciacca./.Italien,* § 30.
[443] EGMR, Urteil vom 24.04.90 – *Huvig./.Frankreich,* §§ 34 f.

erkennen können, welche Voraussetzungen für einen Eingriff gegeben sein müssen, welches Verfahren hierfür erforderlich ist sowie die Aufbewahrungsfrist und die Vernichtung der Daten. Ebenso sollten die Art der Straftaten und der betroffene Personenkreis beschrieben sein. Auch Sicherungsmaßnahmen bei der Nutzung von Daten zu Präventionszwecken sind erforderlich, d.h. es sollte der Zugang Dritter geregelt sein, ebenso wie die Sicherstellung der Integrität und Richtigkeit der Daten.[444] Bei einem Ermessensspielraum muss der Umfang des Ermessens bestimmt werden. Auch sind Regelungen zur kontrollierenden Stelle, Art und Weise der Kontrolle, Dauer und Gründe der Kontrolle anzugeben. Für alle angesprochenen Punkte können auch Weisungen und die Verwaltungspraxis herangezogen werden, sofern diese öffentlich gemacht wurde. Vereinzelt verlangte der Gerichtshof, dass auch die Rechte des Betroffenen und die Art der Information geregelt werden.[445]

Art. 8 II EMRK benennt die legitimen Zwecke, aufgrund derer eine Einschränkung des Rechts auf Privatleben möglich ist.

Weiter verlangt Art. 8 II EMRK, dass der Eingriff „in einer demokratischen Gesellschaft notwendig ist"; dies ist der Fall, wenn ein dringendes gesellschaftliches Bedürfnis für die Einschränkung angenommen wird und die Maßnahme verhältnismäßig ist. Dabei kommt den staatlichen Stellen ein Beurteilungsspielraum zu, wobei es Folgendes zu beachten gilt: Je privater der Eingriff ist, desto enger ist dieser Spielraum; dies gilt besonders in sensiblen Bereichen oder bei schwerwiegenden Eingriffen. Andererseits ist der Beurteilungsspielraum weiter, je gewichtiger das legitime Ziel ist; auch der Adressatenkreis ist für die Beurteilung des Spielraums maßgeblich. Ein Eingriff kann nur dann „notwendig in einer

[444] EGMR, Urteil vom 04.12.08, *S. & Marper./.Vereinigtes Königreich*, § 99; EGMR, Urteil vom 02.09.10 – *U./.BRD*, § 65.
[445] EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, § 57.

demokratischen Gesellschaft“ sein, wenn ausreichende Garantien gegen Missbrauch ergriffen wurden. Die Sicherheitsvorkehrungen müssen höher ausfallen, wenn Daten automatisch verarbeitet werden bzw. wenn diese von polizeilichen Behörden genutzt werden.[446] Die Kommission hat hierzu entschieden, dass das Anlegen von Akten, die Abnahme von Fingerabdrücken und die Aufnahme von Fotos sowie die generelle Sammlung und Weitergabe von Informationen zur Verhütung von Straftaten notwendig sei, insbesondere bei manuellen Akten;[447] dies diene auch dazu, zukünftige Straftaten aufzudecken. Dabei kann es der Schutz der nationalen Sicherheit gebieten, den Betroffenen über die vorhandenen Daten vorerst nicht zu informieren,[448] wobei dies natürlich spätestens dann nachgeholt werden sollte, wenn eine Information ohne Gefährdung des Ermittlungszwecks möglich ist. Auch die Aufbewahrung der Akten über den tatsächlichen Bedarf hinaus kann gerechtfertigt sein.[449] Daraus ergibt sich, dass sowohl der EGMR als auch die Kommission den Kampf gegen den Terrorismus und die Bekämpfung von Straftaten als ernste Aufgabe ansehen und den Umständen nach eine Ausweitung des Beurteilungsspielraumes zulassen; dabei wird jedoch nicht außer Acht gelassen, dass beide Ziele nicht jede Maßnahme rechtfertigen. Hinsichtlich der Verwendung sensibler Daten ist dem Schutzbedürfnis des Einzelnen grundsätzlich Vorrang vor der Verfolgung von Straftaten zu gewähren. In Ausnahmesituationen ist natürlich auch hier eine Beeinträchtigung möglich, allerdings müssen dann ausreichende Garantien gegen Missbrauch gegeben sein (z.B. Verpflichtung zum vertraulichen Umgang, rechtliche Folgen bei Nichtbeachtung) und der Betroffene sollte seine

[446] EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich*, § 103.
[447] EKMR, Bericht vom 19.05.94 – *Friedl./.Österreich*, § 66; EKMR, Bericht vom 18.03.81 – *McVeigh u.a./.Vereinigtes Königreich*, § 232.
[448] EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, §§ 57 f.
[449] EKMR, Entscheidung vom 13.12.79, DR 18, 176 (180 f.) – *A.B,C und D./.BRD*; EKMR, Bericht vom 18.03.81 – *McVeigh u.a./.Vereinigtes Königreich*, § 229.

Einwilligung erteilt haben. Speziell in Bezug auf DNA- und Fingerabdruck-Daten ist im Rahmen der Abwägungen zur Rechtfertigung auch zu berücksichtigen, wie schwerwiegend das Delikt ist, wie alt die Betroffenen sind, ob die Speicherung zeitlich limitiert ist und welche Möglichkeiten für den Betroffenen bestehen, die Daten aus den Datenbanken entfernen zu lassen.[450]

4. VERGLEICH DER RECHTSPRECHUNG MIT DEN EPASS-REGELUNGEN UND DEM PRÜMER RATSBESCHLUSS

Im Folgenden soll nun die Rechtsprechung mit den ePass-Regelungen und dem Prümer Ratsbeschluss verglichen werden.

a) BEWERTUNG DES EPASSES ANHAND DER RECHTSPRECHUNG

Nach den vorgenannten Kriterien der Rechtsprechung stellt der ePass[451] eine Beeinträchtigung des Rechts auf Achtung des Privatlebens dar.

Der ePass verarbeitet biometrische Daten, welche allein durch ihren persönlichen Inhalt einen Bezug zum Privatleben aufweisen. Die Art der Daten, nämlich biometrische Bilddateien, ist von hoher Qualität, d.h. auch von hoher Eingriffsqualität. Die Daten werden im ePass aufgezeichnet und gespeichert. Die dazwischengeschaltete technische Aufbereitung der Daten für den ePass bzw. die Ausweiskontrolle stellen außerdem eine nachträgliche Datenverarbeitung dar. Hinzu kommt, dass gem. Art. 4 III i.V.m. Art. 7 II des Schengener Grenzkodexes[452] eine Überprüfung zusätzlicher Sicherheitsmerkmale erfolgen kann. Nach Art. 7 II des Schengener Grenzkodexes kann die Echtheit des

[450] EGMR, Urteil vom 04.12.08 – *S. & Marper./.Vereinigtes Königreich,* §§ 118 f.
[451] Konsolidierte Fassung, s. Dokument 2004R2252-DE-26.06.2009-001.001.
[452] Konsolidierte Fassung, s. Dokument 2006R0562-DE-05.04.2010-003.002.

Passes überprüft werden, ggf. auch durch Abfrage einer Datenbank, welche Daten über gestohlene, missbräuchlich verwendete, abhanden gekommene und für ungültig erklärte Dokumente enthält, d.h. es ist die Sachfahndung der einschlägigen nationalen und internationalen Datenbanken abzufragen, mithin also das Schengener Informationssystem und die nationalen Datenbanken – in Deutschland das INPOL. Ferner können über Art. 7 II des Schengener Grenzkodexes auch Daten abgefragt werden bezüglich der Frage, ob eine Person eine „tatsächliche, gegenwärtige und erhebliche Gefahr für die innere Sicherheit, die öffentliche Ordnung, die internationalen Beziehungen der Mitgliedstaaten oder die öffentliche Gesundheit" darstellt; diese Abfrage erfolgt ebenfalls über die Ausweisnummer. Auch wenn hier keine biometrischen Merkmale eingegeben werden bzw. kein biometrischer Abgleich erfolgt, sondern die Abfrage allein anhand der Ausweisnummer vorgenommen wird, so stellt dies doch eine Zweckänderung gegenüber den Zwecken des Art. 4 III lit. a) und b) ePass-Verordnung dar, auch wenn dies im weitesten Sinne der Verfolgung von Straftaten zuzurechnen ist. Ferner stellte der Gerichtshof fest, dass eine Speicherung und Verarbeitung von Daten auch dann einen Eingriff darstellen, wenn die Informationen ursprünglich frei verfügbar und zugänglich waren. Ähnlich verhält es sich beim ePass. Das Gesichtsbild ist öffentlich zugänglich und kann von jedem wahrgenommen werden. Auch werden Fotos seit einiger Zeit fast tabulos im Internet verbreitet. Dennoch bedeutet dies nicht, dass der Wert des Bildes sinkt, denn spätestens mit der Speicherung eines Fotos und der Sammlung von Informationen – wie hier Daten über Größe, Augenfarbe etc. – ist ein Bereich der Privatsphäre überschritten, der an Profilbildung grenzt. Der Gerichtshof hat zudem in mehreren Entscheidungen das Recht am eigenen Bild dem Schutz der Privatsphäre unterstellt.[453] Ferner ist

[453] EGMR, Urteil vom 21.02.02 – *Schüssel./.Österreich*, § 2; EGMR, Urteil vom 24.06.04

im Unterschied dazu, ob jemand an einer Person vorbeigeht und deren Gesicht betrachtet, mit der Aufnahme des Fotos und der Speicherung auf einem Dokument eine Aufzeichnung verbunden, welche Gelegenheit gibt, die Person näher zu betrachten und weitere Merkmale der Person zu entdecken, was zur Einschätzung darüber führen kann, ob die Person an einer Krankheit leidet oder welchen Charakter sie hat (Mimik).

Diskussionswürdig ist allein die Frage, ob die Person bei einer privaten oder öffentlichen Tätigkeit abgebildet ist, denn dementsprechend stellt sich die Frage, ob eine Einwilligung des Betroffenen vorliegt. Die Beantragung eines Ausweises selbst ist privat. Andererseits erfolgt die Beantragung, um eine öffentliche Ausweispflicht beim Grenzübertritt erfüllen zu können. Bei Privatpersonen wird man von einer privaten Betätigung ausgehen müssen, da diese ihrem Privatleben zuzuschreiben ist, ebenso wie die Tatsache, ob jemand auf Reisen geht oder nicht. Eine Einwilligung kann daher unterstellt werden. Wichtig ist nach dem Gerichtshof auch die Erwartungshaltung des Betroffenen bei der Ausweiskontrolle. Der Betroffene geht nur davon aus, dass seine Identität und die Echtheit des Ausweises überprüft werden. Dass auch eine Überprüfung der Datenbanken hinsichtlich des Vorliegens einer Gefahr in seiner Person stattfindet, erwartet dieser nicht. Des Weiteren handelt es sich bei den biometrischen Daten mitunter auch um solche, welche medizinische, ethnische und religiöse Informationen erkennen lassen, sei es durch ein Kopftuch, die Hautfarbe oder durch eine Brille. Sowohl diese Daten als auch Informationen wie Name, Anschrift, Größe, Augenfarbe etc. stellen personenbezogene Daten dar, welche gerade aufgrund ihres Bezugs zum Privatleben dem Art. 8 I EMRK unterfallen und deren Speicherung und Verarbeitung einen Eingriff in Art. 8 I EMRK bedeuten. Gerade, da es sich bei den

– *Caroline von Hannover./.BRD*, § 50.

biometrischen Daten auch um sensible Daten handelt, ist eine erhöhte Eingriffsqualität vorhanden. Dabei wurde von EGMR bereits explizit festgestellt, dass Fingerabdrücke personenbezogene Daten sind, welche Gesundheitsinformationen und Daten über die ethnische Herkunft enthalten.

Art. 8 Abs. 2 EMRK verlangt, dass ein Eingriff gesetzlich vorgesehen sein muss. Mit der Verordnung 2252/2004 (einschließlich der Änderung durch die Verordnung 444/2009) liegt eine gesetzliche Grundlage vor, welche im Amtsblatt veröffentlicht und damit zugänglich gemacht wurde. Diese Verordnung ist außerdem unmittelbar anwendbar und gilt daher auch im nationalen Bereich. Allerdings stellt sich zum einen die Frage, ob ausreichende Garantien gegen Missbrauch vorhanden sind und zum anderen, ob die Maßnahmen vorhersehbar sind. Zur Absicherung vor Missbrauch der biometrischen ePass-Daten wurden zahlreiche Sicherheitsvorkehrungen getroffen, u.a. beginnt dies damit, dass nur die zuständigen Behörden mit den biometrischen Daten befasst sind, d.h. nur die entsprechenden Meldeämter sowie eine Druckerei (Art. 3 II der Verordnung). Im weiteren Verlauf haben auf die Daten nur Polizeibehörden, Grenzbeamte, Zollbeamte und die Meldeämter Zugriff, da nur diese die entsprechenden Zugangsdaten besitzen. Alle Behörden dürfen auf die Daten nur im Rahmen ihrer Befugnisse zugreifen. Die Meldeämter dürfen darauf zugreifen, um die Anträge zu bearbeiten und mögliche Berichtigungen vorzunehmen bzw. um die Identität des Ausweisinhabers zu überprüfen. Die Druckereien dürfen nur zur Erstellung des Passes darauf zugreifen. Im Übrigen werden die Fingerabdruckdaten im Passregister sofort nach Erstellung des Ausweises gelöscht, nicht so aber die Passfotos. Die Polizeibehörden, Grenzbeamten und Zollbeamten dürfen ebenfalls nur nach Maßgabe des Gesetzes, also zu den Zwecken des Art. 4 III i.V.m. Art. 7 II Schengener Grenzkodex darauf zugreifen.

Allerdings wird der Zugriff auf die Passregister durch nationales Recht oft erheblich erweitert, indem Polizeibehörden auch im Falle der Ermittlung nationaler Straftaten (bspw. Verkehrsstraftaten) Zugriff auf die Datenbank nehmen. Da diese Verwendungsmöglichkeit in einem anderen Gesetz (Passgesetz) steht, ist für den Bürger eine Verbindung nicht immer nachvollziehbar, insbesondere wird ihm dies nicht bei der Beantragung mitgeteilt. Dieser Eingriff wird umso schwerwiegender, als es sich um biometrische Daten und damit um eine Grundlage für einen automatisierten Abgleich handelt. Anzumerken ist jedoch, dass auch die ePass-Verordnung in Deutschland in das Passgesetz übernommen wurde, weshalb der Bürger durch Einsicht in dieses Gesetz alle Verwendungsmöglichkeiten erkennen könnte. In anderen Ländern kann dies jedoch wieder anders sein.

Fraglich ist daher weiter, ob weitere Zugriffsrechte auf das biometrische Foto überhaupt im Sinne einer Einheitlichkeit erlaubt sein sollen und ob eine entsprechende Regelung auf europäischer Ebene nötig ist. Dies lässt sich nur mit dem Subsidiaritätsprinzip des Art. 5 II EUV beantworten. Befürwortet werden kann demnach eine staatliche Regelung, sofern das europäische Recht vorschreibt, dass für den Bürger eine Klarheit gegeben ist, die keinen Zweifel an der Verwendung des Fotos lässt, da ansonsten das Ziel der Subsidiarität, nämlich die Bürgernähe nationaler Entscheidungen, nicht erreicht würde. Damit lässt sich auch gleich die zweite Frage beantworten, nämlich ob die Maßnahmen vorhersehbar sind. Auch wenn mit der Überprüfung der Datenbanken nach dem Schengener Grenzkodex sowie aufgrund der Abgleichmöglichkeit durch Polizeibehörden – hinsichtlich der Frage des Vorliegens einer von dem Betroffenen ausgehenden Gefahr – eine Zweckänderung verbunden ist, so ist dies dennoch vorhersehbar, da Art. 4 III auf Art. 7 II Schengener

Grenzkodex verweist und ein Abgleich zum Zwecke der Verfolgung von Verkehrsstraftaten im Passgesetz geregelt ist. Es ist lediglich fraglich, in welchen Fällen eine solche Überprüfung stattfindet. Art. 7 II des Schengener Grenzkodex bspw. stellt dies in das Ermessen der durchführenden Beamten (vgl. Wortlaut „auf nicht systematischer Grundlage"). Hier müssen dann der Umfang des Ermessens, Art und Weise der Kontrolle, Dauer und Gründe für die Kontrolle bestimmt sein. Die Art und Weise wird bereits durch Art. 7 II Schengener Grenzkodex bestimmt, d.h. durch Abfrage der einschlägigen internationalen und nationalen Datenbanken. Die Dauer ergibt sich aus der Natur der Sache und wird daher nur kurzwährend sein. Der Umfang des Ermessens und die Gründe für die Kontrolle ergeben sich aus der polizeilichen Praxis, welche nach der Rechtsprechung ebenfalls ausreicht.

Die Verwendung des ePasses und der darauf enthaltenen biometrischen Daten erfolgt zum Zwecke der Verfolgung von Straftaten und damit zur Aufrechterhaltung der öffentlichen Ordnung. Die Verwendung des ePasses dient außerdem der Erleichterung der Abwicklung des Binnenverkehrs. Dieser Aspekt ist ebenfalls im Rahmen der Aufrechterhaltung der öffentlichen Ordnung zu beachten, da nur so eine ordnungsgemäße Abwicklung des Flugverkehrs möglich ist. Im Bereich der Verfolgung von Straftaten dient der ePass v.a. der Aufdeckung von Fälschungen. Auch sollen mögliche Straftaten im Vorfeld bekämpft werden, insbesondere im Bereich der Terrorismusbekämpfung. Aus diesem Grund dient der ePass auch der Wahrung der nationalen Sicherheit.

Ferner muss der Eingriff „in einer demokratischen Gesellschaft notwendig sein", d.h. die Verwendung des ePasses samt seiner biometrischen Daten muss verhältnismäßig sein. Für die Beurteilung sind sowohl die Privatheit des Eingriffs, der Adressatenkreis und das Vorhandensein ausreichender Garantien

als auch das legitime Ziel maßgeblich. So hat der Gerichtshof in Angelegenheiten zur Verhütung von Straftaten oder zum Schutz der nationalen Sicherheit – wie hier vorliegend – einen größeren Beurteilungsspielraum angenommen. Auf der anderen Seite handelt es sich hier um biometrische Daten, deren hohes Maß an Privatheit nicht zu unterschätzen ist. Der Adressatenkreis ist klar bestimmt, nämlich jeder, der einen ePass beantragt, wird beeinträchtigt. So wird niemand diskriminiert, d.h. jeder wird gleich behandelt, da die Situation eines jeden gleich ist. Durch den großen Adressatenkreis sind jedoch auch Schutzmaßnahmen zu Gunsten des Einzelnen erforderlich. So bestehen zahlreiche Sicherheitsmaßnahmen in Bezug auf den ePass, welche die Datensicherheit gewährleisten. Dabei wurden technische und organisatorische Maßnahmen getroffen. In Pkt. 5.2 der Entscheidung der Kommission vom 28.06.2006 wurden Schutzmaßnahmen in Bezug auf Zugriffe (Basic Access Control und Extended Access Control, vgl. Teil C Pkt. A. III.) getroffen. Auch hat außer dem Inhaber kein anderer Zugang zum Pass, wodurch gleichzeitig ein Zugangsschutz sichergestellt wird. Zugriff auf die biometrischen Daten haben nur bestimmte Behörden, wobei zu berücksichtigen ist, dass die Fingerabdrücke gleich nach Ausgabe des Passes wieder gelöscht werden und das biometrische Foto nur im Rahmen der oben genannten Zwecke genutzt wird, d.h. der Behördenkreis ist auch hier wieder eingeengt. Des Weiteren wurden Maßnahmen getroffen, um ein Kopieren der Daten zu vermeiden (Passive Authentification und Active Authentification, vgl. Teil C, Pkt. A. III.). Fraglich ist nur, ob die Sicherungsmaßnahmen durch ein zusätzliches Passwort nicht besser geschützt würden und ob ein solches Passwort überhaupt erforderlich ist oder über den Umfang der erforderlichen Sicherungsmaßnahmen zu weit hinausgeht. Ein Passwort, das der Betroffene vor Abfrage seiner Daten einzugeben hat, würde die Sicherheit in Bezug auf unbefugtes Auslesen der Daten durchaus

erhöhen. Um den Bürger besser zu schützen, sollte diese Möglichkeit auch in Erwägung gezogen werden, insbesondere deshalb, weil ein Auslesen der Daten durch Unbefugte möglich ist und dies bisher nicht behoben werden konnte. Die Sicherheitsvorkehrungen haben auch deshalb so hoch zu sein, da die Daten automatisch verarbeitet werden. Ferner sollte der Betroffene eine Belehrung über den Umgang mit dem ePass erhalten, um diesen vor Beschädigung, Missbrauch, etc. schützen zu können. Auch gibt es leider keine Vorschriften, welche die strafrechtliche und disziplinarrechtliche Verantwortlichkeit im Fall einer unrechtmäßigen Behandlung bzw. eines Missbrauchs regeln. Befindet sich der Passinhaber bspw. in Deutschland, so gibt es hierzu ausreichend Sicherungsmöglichkeiten. Dies ist aber von den Mitgliedstaaten zu regeln und kann divergieren. Insbesondere wird der ePass nicht nur in den Mitgliedstaaten der EU verwendet, sondern auch in Drittländern, weshalb fraglich ist, ob diese Länder entsprechende Vorkehrungen vorsehen. Da die Mitgliedstaaten in diesem Fall die Verantwortung für eine ordnungsgemäße Rechtssetzung per Einzelermächtigung auf die Europäischen Organe abgegeben hat, sind die Europäischen Organe m.E. auch verpflichtet, bei Erlass einer Rechtsvorschrift für die Einhaltung europäischer Normen zu sorgen, notfalls durch Abkommen mit Drittstaaten. Ferner ist zu berücksichtigen, dass die Kommission bereits entschieden hat, dass die Abnahme von Fingerabdrücken und die Aufnahme von Fotos sowie die generelle Sammlung und Weitergabe von Informationen zur Verhütung von Straftaten und um zukünftige Straftaten aufzudecken notwendig sind.[454] Auch den Schutz vor terroristischen Bedrohungen sah die Kommission als ernste Aufgabe an. Letztlich geht es beim ePass um nichts anderes. Es sollen Straftaten im Bereich der Ausweisdelikte aufgeklärt und es soll vor terroristischen Straftaten geschützt

[454] EKMR, Bericht vom 19.05.94 – *Friedl./.Österreich*, § 66.

werden. Wenn dabei schon die erkennungsdienstliche Behandlung zulässig ist, bei der Fotos und Fingerabdrücke aufgenommen und auf lange Zeit gespeichert werden, dann muss ein kurzer 1:1-Abgleich erst recht angemessen sein. Da es sich bei den biometrischen Daten um einen Grenzbereich zu den sensiblen Daten handelt, ist eine Unverhältnismäßigkeit nicht von vornherein gegeben. Doch auch wenn dies so wäre, so wären Ausnahmesituationen, etwa im Sinne der legitimen Ziele des Art. 8 Abs. 2 EMRK, durchaus vorstellbar. Der ePass unterscheidet sich vom vorhergehenden Ausweis durch seine biometrischen Merkmale, aber auch durch mehr Schutzvorkehrungen. Die biometrischen Merkmale – und das wird häufig vergessen – dienen auch dem Schutz des Einzelnen vor Missbrauch, da ein anderer den Ausweis nicht wird benutzen können. Ferner spricht für den ePass auch die Tatsache, dass durch die angeglichenen Mindestsicherheitsstandards eine reibungslosere und einfachere Kontrolle durch die Grenzbeamten gewährleistet wird. Auf der anderen Seite ist zu berücksichtigen, dass bereits Kinder ab zwölf Jahren einen biometrischen Reisepass verwenden. Allerdings hat auch hier wiederum der Betroffene bzw. der Erziehungsberechtigte alleinigen Zugriff auf die Daten und die Speicherung ist auf die Lebensdauer des Passes limitiert.

Problem des ePasses sind also einzig und allein die mangelnden Schutzvorkehrungen, welche durchaus noch verbesserungswürdig sind. Letztlich wird aber die Befolgung der DSK dafür entscheidend sein, ob der ePass tatsächlich Art. 8 EMRK verletzt, da die DSK vom Gerichtshof – zu Recht – bei der Beurteilung der Verletzung des Art. 8 EMRK herangezogen wird.

b) BEWERTUNG DES PRÜMER RATSBESCHLUSSES ANHAND DER RECHTSPRECHUNG

Gleiches gilt für den Prümer Ratsbeschluss, der einen Austausch von DNA- und Fingerabdruck-Daten vorsieht. Beide fallen damit in den Schutzbereich des Art. 8 I EMRK. Durch die Art der Daten (DNA und Fingerabdruck) wird ein unmittelbarer Bezug zum Privatleben hergestellt.

Der Kommission hat entschieden, dass eine nachträgliche Datenverarbeitung bspw. i.S.e. Weiterleitung einer Akte an ein Gericht einen Eingriff darstellen kann.[455] Entscheidend ist hierfür der Inhalt der Akte. Inhalt der Akte wäre in diesem Fall, dass ein Fingerabdruck/Handabdruck bzw. eine DNA-Spur mit der eines Betroffenen übereinstimmt. Dabei handelt es sich um eine Verbindung zum Betroffenen und aufgrund des Charakters eines biometrischen Merkmals sogar um eine sehr individuelle Verbindung. Eine nachträgliche Datenverarbeitung findet nur insofern statt, als die Daten zunächst einer Person bzw. Spur zugeordnet und anschließend im Prozess verwendet werden. Eine Speicherung der Daten in der Datei eines anderen Mitgliedstaates ist vom Wortlaut des Prümer Ratsbeschlusses nicht vorgesehen. Allerdings kann ein Eingriff bereits in der dezentralen Vernetzung der einzelnen Dateien gesehen werden, vgl. Art. 7 II und 12 III Durchführungsbeschluss zum Prümer Ratsbeschluss. Des Weiteren wird auch aufgrund der Speicherung und der Verarbeitung der Daten ein Eingriff angenommen. Aufgrund der biometrischen Eigenschaft der Daten stellen diese einen Bezug zum Privatleben her. Ebenso ist die DNA, auch wenn es sich nur um nicht-codierte DNA handelt, ein Teil des Betroffenen und damit ein Teil seines Privatlebens, vielmehr sogar seiner höchsten Intimsphäre. Nach

[455] EKMR, Bericht vom 19.05.94 – *Friedl./.Österreich*, § 49.

Ansicht der Kommission wäre daher eine Beeinträchtigung gegeben.

Auch nach Auffassung des Gerichtshofes müsste ein Eingriff bejaht werden.

In der Bereitstellung der DNA- und der Fingerabdruck-Daten zum Abgleich liegt bereits eine Beeinträchtigung. Spätestens, wenn die Daten bzw. die dazugehörigen personenbezogenen Daten aufgrund eines Treffers weitergeleitet werden, wird ein weiterer Eingriff vorgenommen. Es ist vollkommen irrelevant, dass diese Daten nur entsprechend ermächtigten Behörden bekanntgemacht werden (vgl. Art. 27 Prümer Ratsbeschluss) bzw. nur besonders ermächtigte Beamte Zugriff darauf haben (vgl. Art. 30 II lit. a) S. 1 Prümer Ratsbeschluss), da mit der Bereitstellung der Daten gewissermaßen die Kontrolle über diese Daten aus der Hand gegeben wird. Bereits durch die Speicherung und die maschinelle Aufbereitung der Daten bzw. die Nutzung der Daten wird das Recht des Betroffenen auf Privatleben beeinträchtigt. Durch die maschinelle Verarbeitung werden die Fingerabdrücke deutlicher, so dass die Minutien besser zutage treten. Bei der DNA-Analyse wird sogar zunächst eine Vervielfältigung des Materials vorgenommen. Erst danach werden die benötigten Daten durch Verwendung eines DNA-Profils minimiert. Des Weiteren werden die Daten für eine gewisse Dauer gespeichert. Wenn der Gerichtshof „dauerhaft“ meint, so ist darunter nicht „für immer“ zu verstehen, sondern ein „Zeitraum von einer gewissen Länge“. Die DNA- und daktyloskopischen Daten werden für einen gewissen Zeitraum gespeichert. Die Länge ist meistens abhängig von der Schwere des Delikts, wobei dies wiederum von Staat zu Staat differiert; manche Staaten speichern solche Daten generell für einen bestimmten Zeitraum, unabhängig von der begangenen Straftat. Auch in Deutschland findet bspw. nach Ablauf gewisser Fristen nur eine dahingehende Prüfung statt, ob die Daten noch

erforderlich sind (s. Teil C. Pkt. I.). Wird dies bejaht, so bleiben die Daten weiterhin gespeichert. Von einer dauerhaften Speicherung und damit auch von einer Beeinträchtigung des Art. 8 I EMRK kann daher ausgegangen werden. In Großbritannien stellt die Aufbewahrung der Daten sogar ein noch größeres Problem dar, weil dort eine Frist zur Überprüfung der Erforderlichkeit gar nicht vorgesehen ist. Auch hier sollte eine einheitliche Festlegung erfolgen, wann eine Überprüfung erforderlich ist. Eine Verlagerung dieses Problems auf die nationale Ebene lässt den Mitgliedstaaten zu viel Spielraum und führt dazu, dass die Staaten unbegrenzt Daten speichern können. Ohne Frage kann der Zeitraum bei den Mitgliedstaaten verbleiben, wobei jedoch vom europäischen Gesetzgeber zumindest eine bestimmte Spanne anzugeben ist. Ein Bezug zum Privatleben wird sowohl durch die lange Aufbewahrungsdauer als auch durch die Qualität des Eingriffs hergestellt. Die Qualität des Eingriffs beruht auf dem Umstand, dass es sich um biometrische Daten und damit um persönliche Eigenschaften des Betroffenen handelt. Diese Daten werden staatenübergreifend abgeglichen, was die Eingriffsqualität noch erhöht. Ferner sind die Datenbanken im Rahmen des Prümer Ratsbeschluss miteinander vernetzt, um den Datenabgleich überhaupt durchführen zu können. Dies bedeutet natürlich auch, dass der Abgleich entsprechend einfach durchzuführen ist und es dadurch zu einer erhöhten Abfragequote kommt. Allerdings ist bei dem Aspekt der Vernetzung nicht zu verachten, dass diese natürlich auch zu schnelleren Ermittlungserfolgen führt. Die Frage, ob es sich bei den DNA-Daten um medizinische Daten handelt bzw. ob aus den Fingerabdruck-Daten medizinische Informationen ausgelesen werden können, ist hierfür dann nicht mehr relevant und wird wohl weiterhin streitig sein. Letztlich berührt aber sowohl die Entnahme der DNA als auch die Abnahme der daktyloskopischen Daten die physische und psychische Integrität, weswegen bereits bei der Abnahme/Entnahme ein

Eingriff vorliegt und damit auch bei Anwendung des Art. 7 Prümer Ratsbeschluss, d.h. bei einem Ersuchen um Gewinnung und Untersuchung molekulargenetischen Materials. In der Entscheidung *Caroline von Hannover* hat der Gerichtshof auch Teile der Identität einer Person unter den Schutz des Art. 8 I EMRK gestellt.[456] Biometrische Daten sind unmittelbar identitätsbezogen, da gerade der Fingerabdruck und die DNA einmalig sind. Ferner wurde vom EGMR explizit festgestellt, dass DNA-Material, DNA-Profile und Fingerabdrücke personenbezogene Daten sind, welche nicht nur Gesundheitsinformationen und Daten über die ethnische Herkunft enthalten, sondern auch durch Ähnlichkeiten im DNA-Profil Verwandtschaftsbeziehungen erkennen lassen. Es ist bereits in einigen Staaten, u.a. auch in Deutschland, erlaubt, Daten über das Geschlecht einer Person zu verarbeiten.

Die Beeinträchtigung durch den Abgleich und die Übermittlung der Daten ist gesetzlich vorgesehen durch Art. 3 I, II, 4 I, II 9 I, II Prümer Ratsbeschluss. Der Prümer Ratsbeschluss wirkt zwar nicht unmittelbar, dennoch sind seine Ziele verbindlich und dementsprechend in nationales Recht umzusetzen. Zumindest aber liegt mit dem Umsetzungsgesetz eine Rechtsgrundlage für den Eingriff vor. Des Weiteren sind durch die Vorgabe die Regelungen vorhersehbar. Ebenso ist die Einrichtung einer solchen Datei in Art. 2 I Prümer Ratsbeschluss angeordnet. Der Prümer Ratsbeschluss wurde im Amtsblatt der EU veröffentlicht; ebenso wurden die nationalen Umsetzungsakte national veröffentlicht.

Der Prümer Ratsbeschluss enthält auch Regelungen zur Absicherung vor Missbrauch. So sind bspw. umfangreiche Protokollierungsvorschriften enthalten, wonach jede nichtautomatisierte Übermittlung (Art. 30 I) und jede

[456] EGMR, Urteil vom 24.06.04 – *Caroline von Hannover./.BRD*, § 50

automatisierte Übermittlung (Art. 30 II) mit bestimmten vorgegebenen Angaben protokolliert werden muss. Diese Protokolle können von den Datenschutzbehörden kontrolliert werden. Da der Prümer Ratsbeschluss Ermessensvorschriften enthält, müssen nach der Rechtsprechung die Reichweite des Ermessens, die möglichen Adressaten, die fraglichen Delikte sowie die zeitliche Dauer der Maßnahme festgelegt sein. Letztlich bedeuten das Vorliegen dieser Voraussetzungen sowie die Festlegung der Aufbewahrungsfristen und die Ausgestaltung des Verfahrens, dass die Maßnahmen vorhersehbar sind. In Art. 4 I und 9 I Prümer Ratsbeschluss wird lediglich bestimmt, dass die Anfragen nur im Einzelfall und nach Maßgabe des innerstaatlichen Rechts erfolgen dürfen. Der Ermessensspielraum wurde hierbei nicht festgelegt. Dieser verbleibt vielmehr bei den Mitgliedstaaten und kann je nach Mitgliedstaat unterschiedlich ausfallen, weswegen eine Vorhersehbarkeit nicht gegeben ist. Dies gilt auch dann, wenn durch das Umsetzungsgesetz der Ermessenspielraum eingegrenzt wurde, denn letztlich verbleibt die Umsetzung des Ratsbeschlusses bei den Ländern. Ob ein Einzelfall vorliegt, müssen die Behörden und die zuständigen Beamten im Rahmen ihrer Ermessensausübung bestimmen.

Die möglichen Adressaten sind genau festgelegt. Die Zuständigkeit der Behörden wird in Art. 27 Prümer Ratsbeschluss eingegrenzt. Die zum Abruf ermächtigten Staaten sind nur die Mitgliedstaaten der EU. Die zeitliche Dauer des Abrufs ist regelmäßig begrenzt, u.a. durch Art. 14 II Durchführungsbeschluss bzw. durch die Schwedische Initiative, auf welche in Erwägungsgrund 10 des Prümer Ratsbeschlusses verwiesen wird. Problematisch ist dagegen das Fehlen eines Straftatenkataloges. Es bleibt damit schließlich den Mitgliedstaaten überlassen, aufgrund welcher Delikte sie einen Abruf vornehmen. Aufgrund der Verschiedenartigkeit der Voraussetzungen je nach Mitgliedstaat kann von Vorhersehbarkeit

für den Einzelnen keine Rede sein. Wird ein Straftatenkatalog festgelegt, dürfte dies auch einen Ermessensspielraum festlegen. Ein Straftatenkatalog ist damit unabdingbar für die Vorhersehbarkeit der Maßnahmen. Aufbewahrungsfristen wurden ebenfalls nicht festgelegt. Auch dies wird unausgesprochen den Mitgliedstaaten überlassen und kann daher von Staat zu Staat variieren.

Weniger Anlass zur Kritik bietet die Ausgestaltung des Verfahrens. Dieses ist in den Art. 3, 4, 5, 9 und 10 Prümer Ratsbeschluss sowie in den Durchführungs-bestimmungen ausreichend festgelegt worden, so dass der Einzelne sich danach richten kann.

Aufgrund der Kritikpunkte zu großer Ermessensspielraum, fehlender Straftatenkatalog und fehlende Angabe der Aufbewahrungsdauer sind die Maßnahmen mangels Vorhersehbarkeit nicht gerechtfertigt. Es reicht auch nicht aus, wenn diese Regelungen erst im Umsetzungsakt getroffen werden, da damit zu viele Variablen gegeben wären. Da der Abgleich staatenübergreifend erfolgt, müsste eigentlich ein gemeinsamer Straftatenkatalog vorliegen, damit ein deutscher Betroffener vor dem Abgleich geschützt ist, wenn er in einem anderen Staat eine Tat begangen hat, die nach deutschem Recht nicht strafbar ist. Zudem können die Tatbestandsmerkmale variieren. Allerdings stellt sich die Frage, ob ein Betroffener vor einer Verurteilung in einem anderen Land geschützt ist, wenn er dort eine Straftat begeht, die nach deutschem Recht nicht strafbar ist. Ein solcher Schutz kann jedoch nicht angenommen werden. Wenn jemand in ein anderes Land kommt, muss er auch dessen Regeln einhalten: „Unwissenheit schützt vor Strafe nicht“. Da diese Punkte nicht im Prümer Ratsbeschluss geregelt wurden, ist nicht anzunehmen, dass die Umsetzungsakte dementsprechende Regelungen enthalten, wie man bereits an der deutschen Umsetzung feststellen kann. Ferner sind bei Ermessensvorschriften Regelungen zur Kontrollstelle, Art

der Kontrolle, Dauer und Gründe der Kontrolle anzugeben. Regelungen zur Kontrollstelle finden sich in Art. 31 I S. 3 Prümer Ratsbeschluss i.V.m. den nationalen Bestimmungen, welche aus der Umsetzung der Datenschutzrichtlinie rühren. Die Art der Kontrolle ist in Art. 30 III und V Prümer Ratsbeschluss geregelt. Allerdings fehlen in Bezug auf staatenübergreifende Übermittlungen Einwirkungsbefugnisse. Hierzu reichen die umgesetzten Bestimmungen der Datenschutzrichtlinie 95/46/EG nicht mehr aus. Da die Vernetzung der Systeme auf unbestimmte Dauer vorgenommen wird, ist davon auszugehen, dass auch die Kontrolle von Dauer ist und nicht nur für die Anfangszeit gilt, insbesondere da hierzu nichts erwähnt wurde. Die Gründe für die Kontrolle wurden in Art. 30 III S. 2 Prümer Ratsbeschluss aufgeführt, nämlich die Kontrolle des Datenschutzes und die Sicherstellung der Datensicherheit.

Lässt man die vorhergehenden Punkte außer Acht, kann man zumindest das Vorhandensein eines legitimen Zwecks bejahen. Der Abgleich von DNA- und Fingerabdruckdaten dient der Aufklärung und Vorbeugung von Straftaten und damit einem legitimen Zweck des Art. 8 II EMRK. Aufgrund dessen dienen die Maßnahmen auch zur Aufrechterhaltung der öffentlichen und nationalen Sicherheit, insbesondere da der Prümer Ratsbeschluss im Hinblick auf die Verhinderung von schweren Straftaten geschaffen wurde, welche die öffentliche Ordnung beeinträchtigen könnten.

Der Eingriff ist „in einer demokratischen Gesellschaft notwendig“, wobei dennoch einige Lücken vorhanden sind.

Für die Maßnahmen des Prümer Ratsbeschlusses ist ein dringendes gesellschaftliches Bedürfnis anzunehmen. Die Kommission hat in Bezug auf manuelle Akten entschieden, dass die Abnahme von daktyloskopischen Daten sowie die generelle

Sammlung und Weitergabe von Informationen für die Verhütung von Straftaten, insbesondere zur Aufdeckung zukünftiger Straftaten, notwendig sind.[457] Es ist unbestreitbar, dass die automatisierte Verarbeitung von Daten eine größere Eingriffsqualität hat als die manuelle Datenverarbeitung. Allerdings muss dies auch im Zusammenhang mit der heutigen Technologie gesehen werden. Die Entscheidung zu *McVeigh* und der Bericht zu *Friedl* stammen aus einer Zeit, als die Fingerabdruckdateien noch manuell abgelegt wurden. Seit ein paar Jahren werden diese jedoch automatisiert verarbeitet. Dies ist auch erforderlich, um dem Bedürfnis einer schnelleren und effizienteren Aufklärung von Straftaten nachzukommen. Auch der grenzüberschreitende Austausch von Daten entspricht dem Wandel der Zeit. Durch Schengen sind die Grenzen heutzutage offen, weswegen Straftäter länderübergreifend einfacher agieren können. Eine Zusammenarbeit ist daher notwendig; ebenso die Vernetzung und Automatisierung von Datenbanken, da nur so eine schnelle und effiziente Aufklärung von Straftaten gesichert ist.

Ob die Regelungen zum Schutz vor Missbrauch ausreichend sind, ist zweifelhaft. Wie bereits erwähnt, gibt es ausführliche Protokollierungsvorschriften, vgl. Art. 30 Prümer Ratsbeschluss. Hinzu kommt, dass nur besonders ermächtigte Beamte Zugriff auf die Daten haben, Art. 30 II lit. a) S. 1 Prümer Ratsbeschluss. Datenschutzbehörden haben Kontrollbefugnisse, vgl. Art. 30 III und V Prümer Ratsbeschluss. Ferner gibt es die Möglichkeit, Schadensersatz geltend zu machen oder sonstige Abhilfe gerichtlich durchzusetzen, vgl. Art. 31 I S. 3 Prümer Ratsbeschluss. Der unrichtig übermittelnde Mitgliedstaat kann sich einer Haftung auch nicht entziehen, vgl. Art. 31 II Prümer Ratsbeschluss. Allerdings fehlen Vorschriften zur strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit. Diese Lücke kann nur

[457] Siemen, S. 157.

durch mitgliedstaatliche Vorschriften geschlossen werden, weswegen man mit Abweichungen rechnen muss. Solche Abweichungen sind aber nicht gerechtfertigt. Wenn bereits die staatenübergreifende Übermittlung geregelt wird, so sollten auch umfassende Vorschriften für den Fall vorhanden sein, in dem eine Übermittlung nicht rechtmäßig durchgeführt wurde. Dazu gehört auch die strafrechtliche und disziplinarrechtliche Verantwortlichkeit. Natürlich gilt wiederum der Grundsatz der Subsidiarität, wonach die Regelung den Mitgliedstaaten vorbehalten bleiben soll. Allerdings stellt sich auch hier wiederum die Frage, ob es ausreicht, wenn die Mitgliedstaaten dies regeln, insbesondere hinsichtlich des „OB“. Dies würde wiederum zu divergierenden Regelungen führen. Wäre das „OB“ bereits vom Prümer Ratsbeschluss festgelegt worden, so wäre es kein Problem, das „WIE“ den Mitgliedstaaten zu überlassen. Allerdings muss sich der Betroffene darauf verlassen können, Ansprüche gegen denjenigen zu haben, der seine Daten falsch verarbeitet. Nur dies würde auch der Abschreckung vor Missbrauch dienen. Zu erwähnen ist jedoch auch, dass Art. 29 Prümer Ratsbeschluss i.V.m. dem Durchführungsbeschluss Vorschriften zur Verhinderung des Missbrauchs durch Dritte vorschreibt, nämlich indem bestimmte Datensicherungsmaßnahmen festgelegt werden. Lässt man die fehlenden Missbrauchsregelungen hinsichtlich der strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit außer Betracht, ist der Abruf/Abgleich von Daten zumindest verhältnismäßig. Da von der Rechtsprechung die oben genannten legitimen Ziele als sehr gewichtig eingestuft werden, insbesondere wenn es um die Bekämpfung von terroristischen Straftaten geht, kommt den Behörden ein großer Beurteilungsspielraum darüber zu, wie sie diese Taten bekämpfen können. Auch wenn der Adressatenkreis aus allen Mitgliedstaaten der EU besteht, so ist er im Endeffekt dennoch sehr klein gehalten durch Art. 27 Prümer Ratsbeschluss. Zu beachten ist weiterhin, dass der Prümer

Ratsbeschluss ungeachtet aller Mängel immerhin eigene Datenschutzvorschriften enthält, ohne deren Umsetzung die Inbetriebnahme des grenzüberschreitenden Austauschs nicht zulässig ist, Art. 25 II Prümer Ratsbeschluss. Im Endeffekt ist es aufgrund der fortschreitenden Technisierung und zur Förderung der legitimen Ziele gerechtfertigt, einen grenzüberschreitenden Datenaustausch vorzunehmen, welcher darüber hinaus in einer Schritt-für-Schritt-Übermittlung besteht.

5. FAZIT

Der ePass und die Prümer Regelungen unterfallen dem Schutzbereich des Art. 8 I EMRK.

Daten werden sowohl durch den ePass als auch durch den Prümer Ratsbeschluss verarbeitet. Da es sich um biometrische Daten handelt, welche dem Menschen unmittelbar zuzuordnen sind, handelt es sich um Daten mit hoher Eingriffsqualität. Hinzu kommt beim Austausch nach dem Prümer Ratsbeschluss, dass es sich um einen staatenübergreifenden Austausch handelt, welcher die Eingriffsqualität nochmals erhöht. Sowohl beim ePass als auch gemäß dem Prümer Ratsbeschluss findet eine nachträgliche Datenverarbeitung in Form einer technischen Aufbereitung der biometrischen Daten statt. Im Weiteren unterscheidet sich die Art der Beeinträchtigung. Beim ePass wird der Passinhaber durch die Speicherung und Verarbeitung beeinträchtigt, auch wenn bspw. sein Gesichtsbild ursprünglich frei verfügbar und zugänglich war, was insbesondere daher rührt, dass der Gerichtshof das Recht am eigenen Bild schützt und der Betroffene hier bei einer privaten Tätigkeit abgebildet wurde. Eine weitere Beeinträchtigung entsteht durch die Erwartung, dass der Passinhaber durch den Ausweis nur verifiziert wird bzw. dass sein Ausweis auf Fälschungsmerkmale hin überprüft wird. Dass es nicht so ist, zeigt Art. 4 III Pass-

Verordnung i.V.m. Art. 7 II Schengener Grenzkodex. Ferner lässt der ePass aufgrund des Gesichtsbildes medizinische und ethnische Informationen erkennen. Beim Prümer Ratsbeschluss hingegen wird ein Eingriff insbesondere auch aufgrund der Bereitstellung bzw. Weiterleitung der Informationen an eine andere Behörde angenommen, was mit dem Inhalt der Daten zusammenhängt; diese lassen aufgrund ihres biometrischen Charakters eine Verbindung zum Betroffenen zu. Außerdem ist mit der Bereitstellung bzw. Weiterleitung der Daten immer auch ein Kontrollverlust verbunden, was beim ePass nicht passieren kann, da dieser ständig im Besitz des Passinhabers bleibt. Ebenso ergibt sich eine Beeinträchtigung aufgrund der dezentralen Vernetzung der Daten und der Dauerhaftigkeit der Speicherung. Im Übrigen ist sowohl durch die Entnahme der DNA als auch durch die Abnahme der daktyloskopischen Daten die physische und psychische Integrität verletzt.

Diese Eingriffe sind sowohl hinsichtlich des ePasses in der ePass-Verordnung als auch hinsichtlich des Prümer Ratsbeschlusses in demselben gesetzlich vorgesehen. Z. T wurden Maßnahmen gegen Missbrauch geschaffen. So wurde beim ePass der Zugriff allein auf die relevanten Behörden beschränkt, wohingegen beim Prümer Ratsbeschluss Protokollierungs- und Kontrollvorschriften vorhanden sind. Beim ePass sind die Maßnahmen aufgrund der gesetzlichen Festlegung vorhersehbar. Auch der automatisierte Abgleich mit dem Passregister ist im Passgesetz vorgesehen. Dies kann man jedoch beim Prümer Ratsbeschluss nicht behaupten. Im Prümer Ratsbeschluss wurde der Ermessensspielraum vielmehr den Mitgliedstaaten überlassen. Problematisch ist insbesondere das Fehlen eines Straftatenkatalogs, welcher das Ermessen hinsichtlich der Art der Delikte eingrenzt. Daran ändert auch das Subsidiaritätsprinzip nichts. Da aufgrund des Charakters als Ermessensvorschrift auch Kontrollmaßnahmen vorgesehen sein

müssen, liegt im Fehlen einer Einwirkungsbefugnis der Kontrollstellen beim grenzüberschreitenden Datenverkehr eine Lücke vor. Man könnte vielleicht argumentieren, dass hinsichtlich der Vorhersehbarkeit beim ePass die polizeiliche Praxis ausreicht und dies daher auch beim Prümer Ratsbeschluss der Fall sein muss. Dies ist aber nicht vergleichbar. Wenn die Beamten der Grenzkontrolle den ePass auf Fälschungsmerkmale überprüfen sowie eine Datenbank-Überprüfung vornehmen, Unregelmäßigkeiten feststellen und aufgrund dessen eine weiteren Überprüfung der Person vornehmen, so sind dies Unregelmäßigkeiten, welche eng begrenzt sind und hinsichtlich deren mit der Zeit eine gewisse polizeiliche Routine und damit Praxis entsteht. Beim Prümer Ratsbeschluss ist dies nicht so. So schreiben schon Art. 3 I und 9 I Prümer Ratsbeschluss vor, dass ein Abruf nur „im Einzelfall" zu erfolgen hat, d.h. es ist immer wieder von neuem eine Abwägung vorzunehmen, welche fallspezifisch ist und keine Routine entstehen lässt. Somit wäre der Eingriff beim Prümer Ratsbeschluss schon mangels einer vorhersehbaren Rechtsgrundlage nicht gerechtfertigt.

Ungeachtet dessen verfolgen sowohl der ePass als auch der Austausch nach dem Prümer Ratsbeschluss die legitimen Ziele der Aufrechterhaltung der öffentlichen Sicherheit und der nationalen Sicherheit.

Der ePass und der Austausch nach dem Prümer Ratsbeschluss sind zur Verhütung von Straftaten notwendig, der ePass auch zum Schutz der nationalen Sicherheit. Da es sich um gewichtige Ziele handelt, billigt die Rechtsprechung den Staaten einen großen Beurteilungsspielraum zu. Bei beiden Rechtsakten ist der Adressatenkreis klar bestimmt. Allerdings besteht bei beiden ein Mangel an Sicherheitsvorkehrungen. So wurden zwar Protokollierungsvorschriften und Zugangsbeschränkungen festgelegt. Allerdings fehlen insbesondere Vorschriften zur

strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit, die nicht durch den Grundsatz der Subsidiarität gerechtfertigt sind. Hinsichtlich des ePasses könnte zudem die Sicherheit, welche ein Kriterium für die Rechtfertigung ist, durch ein Passwort, welches nur der Inhaber des Passes kennt, erhöht werden. Des Weiteren sollte der Inhaber eines Passes auch über den Umgang mit einem solchen und darüber belehrt werden, was im Verlustfall zu unternehmen ist. Ansonsten ist der ePass insbesondere auch wegen der gewichtigen Ziele gerechtfertigt, insbesondere da nur ein 1:1-Abgleich vorgenommen wird. Auch der Prümer Ratsbeschluss ist sicherlich ein sinnvoller Ansatz, da die automatisierte und grenzüberschreitende Übermittlung heutzutage Standard sein sollte. Gelungen sind auch die Vorschriften, wonach nur eine Schritt-für-Schritt-Übermittlung erfolgt und auch diese nur nach nationalen Vorschriften.

Sowohl der ePass als auch der Austausch nach dem Prümer Ratsbeschluss weisen noch kleine Lücken auf, welche erst behoben werden müssen, damit diese gerechtfertigt sind.

II. DIE DSK UND DIE EMPFEHLUNGEN DES MINISTERKOMITEES

Wie bereits unter Teil D. Pkt. A. III. erläutert, stellen die DSK sowie deren Zusatzprotokoll allgemeine Regelungen zum Datenschutz bereit, welche von den unverbindlichen Empfehlungen des Ministerkomitees ergänzt werden. Im Folgenden werden daher zunächst die Regelungen der DSK und der Empfehlungen zusammenfassend dargestellt und im nächsten Schritt wird ein Vergleich dieser materiellen Vorgaben mit den Prümer Regelungen und dem ePass vorgenommen.

1. DIE REGELUNGEN DER DSK UND DER EMPFEHLUNGEN

Die DSK sowie das Zusatzprotokoll zur DSK regeln den allgemeinen Datenschutz und ermöglichen einen weiten Beurteilungsspielraum der Behörden, welcher gerade durch viele Ausnahmen in Art. 3 und 9 DSK sowie durch noch mehr unbestimmte Rechtsbegriffe bedingt ist. Die Empfehlungen des Ministerkomitees ergänzen die Konventionen. Im Folgenden werden daher zunächst beide Komponenten ausführlich dargestellt, um sowohl eine Basis für die nachfolgende Analyse des ePasses und des Prümer Ratsbeschlusses zu haben und die Grundlagen der DSK und der Empfehlungen R (87) 15 und (92) 1 zu erfassen als auch das Zusammenspiel von DSK und den beiden vorgenannten Empfehlungen zu erkennen.

a) ALLGEMEINE BESTIMMUNGEN

Die DSK ist gem. Art. 3 DSK nur anwendbar auf die automatische Verarbeitung von personenbezogenen Daten, es sei denn, der Geltungsbereich wurde von einem Vertragsstaat gem. Art. 3 Abs. 2c) DSK auf Dateien erweitert, welche personenbezogene Daten

nicht automatisch verarbeiten.[458] In diesem Fall kann ein Staat auch bestimmen, dass die Erweiterung nur für bestimmte Arten von Dateien gilt, vgl. Art. 3 Abs. 3 DSK. Allerdings gibt es auch umgekehrt die Möglichkeit, bestimmte Arten von automatisierten Dateien von den Bestimmungen der DSK auszunehmen, sofern diese Dateien nicht auch im jeweiligen innerstaatlichen Recht Datenschutzvorschriften unterliegen, vgl. Art. 3 Abs. 2 a) DSK. So hat bspw. Lettland die Anwendung der DSK hinsichtlich Dateien ausgeschlossen, die von öffentlichen Institutionen zum Zwecke der Sicherheit und im Strafrechtsbereich errichtet wurden; ebenso hat Malta die Anwendung hinsichtlich Dateien ausgeschlossen, die zum Zwecke der öffentlichen Sicherheit, der Verteidigung oder der Staatssicherheit errichtet worden sind.[459] Die Rec. R (87) 15 schließt sich hinsichtlich des Anwendungsbereichs an die DSK an und eröffnet den Anwendungsbereich für die Sammlung, Speicherung, Nutzung und Übermittlung von persönlichen Daten, welche automatisch verarbeitet werden, allerdings nur in Bezug auf polizeiliche Daten. Die Rec. R (87) 15 soll damit insbesondere die aufgrund der Ausnahmeregelung des Art. 9 Abs. 2 DSK entstandene Lücke schließen. Daten, welche hingegen für verwaltungstechnische Zwecke gesammelt werden, also bspw. Protokolldaten, sollen, sofern möglich, in einer separaten Datei gespeichert werden, da diese eigentlich nicht den Vorschriften für den Polizeibereich zu unterwerfen sind, vgl. Principle 3.3.

Art. 2 DSK enthält Begriffsbestimmungen. Der Datenbegriff in Art. 2 lit. a) DSK ist sehr weit gefasst[460] und erfasst „jede Information über eine bestimmte oder bestimmbare natürliche Person“. Damit

[458] So bspw. Frankreich, Spanien und Ungarn; diesbezügliche Bestimmung, s. auch Rec. R (87) 15 „Scope and definitions”.
[459] S. CoE, “Lists of declarations, reservations and other communications” zur DSK, einsehbar unter: http://conventions.coe.int/Treaty/Commun/ListeDeclarations.asp?NT=108&CM=&DF=&CL=ENG&VL=1.
[460] Henke, S. 69.

sind Daten ohne Personenbezug nicht erfasst, ebenso wenig wie juristische Personen.[461] Allerdings besteht gem. Art. 3 Abs. 2 b) DSK bzw. gem. Rec. R (87) 15 die Möglichkeit, die DSK auch auf Personengruppen, Vereinigungen etc. auszudehnen.[462] Bestimmbarkeit bedeutet, dass man eine Person anhand einfacher Methoden identifizieren kann. Aufwändige Verfahren hingegen sollten nicht erforderlich sein.[463] Was jedoch als aufwändiges Verfahren anzusehen ist, wurde weder im Explanatory Report noch in der DSK erwähnt.[464] *Henke* sieht einen Anhaltspunkt u.a. in der *Empfehlung des Europarates zum Schutz personenbezogener Daten für die Zwecke der wissenschaftlichen Forschung und Statistik vom 23.09.1983*[465]. Der Begriff der „personenbezogenen Daten" stimme mit der Definition der DSK überein. Allerdings sei nach Nr. 1.2 Satz 2 dieser Regelungen eine Person nicht „bestimmbar", sofern für die Identitätsfeststellung ein „unverhältnismäßige[r] Aufwand an Zeit, Kosten und Arbeitskraft" erforderlich wäre.[466] Die Bezugnahme auf die DSK im Explanatory Memorandum der Empfehlung R (83) 10 unter Nr. 19 ist ein Hinweis darauf, dass auch die DSK entsprechend dieser Vorgaben auszulegen ist.[467]

Unter „automatisierter Datei" wird gem. Art. 2 lit. b) DSK „jede zur automatischen Verarbeitung erfasste Gesamtheit von Informationen" verstanden. Damit ist nicht nur der Zusammenschluss von Daten an einem Ort gemeint; vielmehr sind darunter auch Informationen zu verstehen, welche geographisch

461 Henke, S. 69.
462 So bspw. Italien und Österreich.
463 Committee of Experts (CoE), Explanatory Report, ETS No. 108, Nr. 28; so auch Rec. R (87) 15 "Scope and definitions".
464 So auch Henke, S. 70.
465 Recommendation No. R (83) 10.
466 Henke, S. 70.
467 S. auch Henke, S. 70.

verteilt sind und zur Verarbeitung zusammengeschlossen werden.[468]

Des Weiteren ist die DSK – wie bereits festgestellt – auf die automatische Verarbeitung von Daten beschränkt. Art. 2 lit. c) DSK konkretisiert, was unter „automatischer Verarbeitung" zu verstehen ist, nämlich das „Speichern von Daten, das Durchführen logischer und/oder rechnerischer Operationen mit diesen Daten, das Verändern, Löschen, Wiedergewinnen oder Bekanntgeben von Daten". Der Europarat hat die Gefahren erkannt, die durch die Art der Verarbeitung entstehen, was sowohl mit der erheblich größeren Verarbeitungsgeschwindigkeit als auch der größeren Speicherkapazität als auch der Möglichkeit des Verbundes der Dateien und der damit einhergehenden Gefahr von Persönlichkeitsprofilen zusammenhängt.[469] Des Weiteren ist zu beachten, dass sämtliche Verarbeitungsmöglichkeiten nur im Zusammenhang mit automatisierten Verfahren der DSK unterfallen.[470] „Automatisiert" bedeutet hierbei jedoch nicht, dass es sich um computergestützte Verfahren handeln muss; vielmehr ist damit jeder automationsunterstützte Vorgang gemeint, d.h. auch digitale oder optische Verfahren. Auch muss nicht der gesamte Verarbeitungsvorgang automatisiert erfolgen; es reicht bereits eine teilautomatisierte Verarbeitung.[471] Auffällig ist, dass die Beschaffung von Daten von Art. 2 lit. c) DSK nicht erwähnt wird.[472] Die Beschaffung von Daten wird nur in Art. 5 lit. a) und Art. 12 DSK erwähnt, weshalb theoretisch auch nur diese Bestimmungen bei der Beschaffung von Daten zu beachten sind. Allerdings wird bei der Erfassung der manuell gesammelten Daten bereits ein automatisierter Verarbeitungsvorgang in Gang gesetzt,

[468] CoE, Explanatory Report, ETS No. 108, Nr. 30.
[469] Vgl. Henke, S. 78.
[470] Henke, S. 79.
[471] Vgl. hierzu Henke, S. 80.
[472] So Henke, S. 81 f.

so dass die Daten spätestens ab diesem Zeitpunkt von der DSK erfasst sind. Bei manuell gesammelten Daten wird man schwerlich die Gefahren herbeiführen können, welche der Europarat bei der Erstellung der DSK im Sinn hatte. Die „Bekanntgabe" von Daten wird auf zweierlei Weise von Art. 2 lit. c) DSK erfasst; zum einen versteht der Europarat darunter die Weitergabe von Informationen an eine Person und zum anderen die Ermöglichung der Kenntnisnahme der Informationen.[473]

Art. 2 lit. d) DSK konkretisiert die „verantwortliche Person". Hierunter sind jedoch nicht die ausführenden Stellen oder Personen zu verstehen, sondern die für die nach Art. 2 lit d) DSK zu treffenden Entscheidungen zuständigen Personen.[474] Hinsichtlich der Zuständigkeit nimmt die DSK auf das nationale Recht Bezug, da der Europarat der Auffassung war, dass jeder Staat geeignete Kriterien zur Bestimmung der Verantwortlichkeit besitzt.[475]

Rec. R (87) 15 konkretisiert des Weiteren den Begriff „for police purposes". Entsprechend der Definition in der Empfehlung sind davon alle Maßnahmen zur Verhütung und Verfolgung von Straftaten sowie zur Aufrechterhaltung der öffentlichen Ordnung erfasst.

Weitere Definitionen stellt die Rec. (92) 1 in Principle 1 bereit. Danach versteht man unter DNA-Analyse jegliches Verfahren zur Analyse von menschlicher oder sonstiger lebender DNA. Unter „samples" (dt. „DNA-Proben") sind sämtliche lebenden Substanzen zu verstehen, welche für die Zwecke der DNA-Analyse nutzbar sind. Des Weiteren ist unter „DNA file" (dt. „DNA-

[473] CoE, Explanatory Report, ETS No. 108, Nr. 31.
[474] So auch Rec. R (87) 15 "Scope and definitions".
[475] CoE, Explanatory Report, ETS No. 108, Nr. 32.

Identifizierungsmuster“) jegliche strukturierte Erfassung von Ergebnissen aus DNA-Analyse-Verfahren zu verstehen.

Gem. Art. 4 DSK verpflichten sich die Vertragsparteien, die erforderlichen Maßnahmen zur Umsetzung der DSK in ihrem innerstaatlichen Recht zu treffen. Dies schließt nach der Rec. R (87) 15 auch ein, dass eine manuelle Verarbeitung im Polizeibereich nicht stattfindet, sofern damit die Anwendbarkeit der Bestimmungen der Empfehlung umgangen werden soll.

b) QUALITÄT DER DATEN

Art. 5 DSK regelt die Datenqualität. Dabei soll Art. 5 DSK fundamentalen Datenschutzstandards gerecht werden; zum einen müssen die Informationen korrekt und erheblich sein und dürfen im Verhältnis zum Zweck nicht überspannt sein und zum anderen muss auch die Nutzung der Daten korrekt sein.[476]

(1) Die Rechtmäßigkeit der Datenbeschaffung und -verarbeitung

Nach Art. 5 lit. a) DSK müssen die Daten zunächst „nach Treu und Glauben und auf rechtmäßige Art und Weise beschafft sein und verarbeitet werden“. Der Ausdruck „nach Treu und Glauben“ soll bedeuten, dass die Person, deren Daten erhoben werden, zugestimmt oder zumindest Kenntnis von der Erhebung haben, mithin also an der Erhebung beteiligt sein sollte.[477] Dies soll den Betroffenen in die Lage versetzen, zu wissen, wann und von wem seine Daten erhoben werden, um später die in Art. 8 DSK garantierten Rechte durchsetzen zu können. Die Beschaffung sollte auf rechtmäßige Art und Weise geschehen, d.h. im Rahmen einer vorhandenen Rechtsgrundlage.

[476] CoE, Explanatory Report, ETS No. 108, Nr. 40.
[477] So Henke, S. 101.

In Konkretisierung der DSK hat die Rec. R (87) 15 Vorschriften zur Übermittlung von Daten geschaffen. Danach ist eine Übermittlung zwischen Polizeibehörden gem. Principle 5.1 nur zulässig, wenn legitime Interessen – innerhalb der rechtlichen Befugnisse – für eine solche Übermittlung vorliegen. Des Weiteren ist eine Übermittlung zu anderen öffentlichen Stellen wie bspw. Staatsanwaltschaften möglich, wenn die Voraussetzungen des Principle 5.2 vorliegen. Danach ist gem. Principle 5.2 i. lit a) erforderlich, dass eine klare gesetzliche (innerstaatliche) Verpflichtung („legal obligation") bzw. Ermächtigung („legal authorisation") vorliegen muss; allerdings ist auch eine Ermächtigung durch die Aufsichtsbehörde zulässig. Entsprechend dem Memorandum kann die Autorisierung gem. HS. 1 auch durch einen Richter erfolgen.[478] Principle 5.2 i. lit b) lässt eine Übermittlung auch dann zu, wenn die Daten unabdingbar für die Aufgabenerfüllung des Empfängers sind, sofern die Sammlung oder Verarbeitung beim Empfänger nicht mit der ursprünglichen Verarbeitung unvereinbar ist und sofern die rechtliche Verpflichtung des Übermittelnden dem nicht entgegensteht. Lit. b) erfordert damit als Ausnahmevorschrift von dem Erfordernis einer rechtlichen Grundlage eine Zweckbindung an die ursprünglich festgelegten Zwecke und nimmt damit auf Art. 5 lit. b) DSK Bezug. Des Weiteren ist eine Übermittlung ausnahmsweise auch dann zulässig, wenn gem. Principle 5.2 ii. lit. a) die Übermittlung im Einzelfall unzweifelhaft im Interesse des Betroffenen erfolgt und entweder der Betroffene eingewilligt hat oder Umstände vorliegen, welche die Vermutung für eine solche Einwilligung nahelegen; eine weitere Ausnahme sieht Principle 5.2 ii. lit. b) vor, wonach eine Übermittlung zulässig ist, wenn dies notwendig ist, um eine ernste und drohende Gefahr abzuwenden. Der absolute Ausnahmecharakter von Principle 5.2 ii. wird dadurch

[478] S. Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 60.

hervorgehoben, dass das Ministerkomitee zum einen von Ausnahme spricht („exceptionally“) und zum anderen einen Einzelfall verlangt („in a particular case“). Des Weiteren regelt Principle 5.6 die Zulässigkeit von Verbindungen zwischen Dateien und Online-Zugängen zu Dateien. Da die Vorschrift jedoch nur für Dateien mit verschiedenen Zwecken gilt, ist diese im Weiteren nicht anwendbar, denn diese Vorschrift wäre theoretisch nur bezüglich des Prümer Ratsbeschlusses anzuwenden, wobei hier jedoch nur Dateien vernetzt werden, welche jeweils zur Untersuchung und Verfolgung von Straftaten benutzt werden und damit den gleichen Zwecken dienen. Während Principle 5 die Übermittlung von Daten regelt, regelt Principle 2 die Sammlung von Daten. Principle 2.3 der Rec. R (87) 15 normiert die Zulässigkeit von Datensammlungen, welche aus technischen Überwachungsmaßnahmen bzw. anderen automatischen Mitteln resultieren; dies ist nur zulässig, sofern dies in speziellen Bestimmungen vorgeschrieben ist, mithin ist also nur ein hinreichend bestimmtes und zugängliches Gesetz erforderlich, welches ausreichend den Umfang sowie die Art und Weise der Maßnahme beschreibt und zugleich von adäquaten Sicherungsmaßnahmen gegen Missbrauch begleitet wird.[479] Principle 5.5 i. stellt Anforderungen an die Anfragen auf Übermittlung. Demnach sollen Anfragen die ersuchende Behörde sowie den Grund und den Zweck der Anfrage bezeichnen. Dies soll sicherstellen, dass eine Übermittlung zu Recht ausgeführt wird.[480] Des Weiteren sind bei der Übermittlung Sicherungsmaßnahmen nach Principle 5.5 iii. vorzusehen; die Daten dürfen demnach nicht für andere Zwecke verwendet werden, als in der Anfrage zur Übermittlung aufgeführt wurden. Eine Nutzung für andere Zwecke

[479] Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 46.
[480] Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 71.

sollte unter Beachtung der Principles 5.2 bis 5.4 von einer gesonderten Vereinbarung abhängig gemacht werden.

Auch in der Rec. (92) 1 wurden Regelungen zur Rechtmäßigkeit der Erhebung bzw. Verarbeitung aufgenommen. Nach Principle 4 ist eine Entnahme von Blut- oder Gewebeproben nur zulässig, sofern die Umstände durch innerstaatliches Recht festgelegt sind, wobei in manchen Staaten hierfür eine richterliche Genehmigung vorliegen muss. Sofern das innerstaatliche Recht die Entnahme von Proben ohne Einwilligung des Betroffenen zulässt, ist dies nur zulässig, sofern die Umstände des Falles eine solche Maßnahme rechtfertigen. Das Ministerkomitee hat in seinem Memorandum für letzteres verschiedene Fälle aufgezählt, unter denen eine Probenentnahme zulässig ist, so z.B.

- wenn ein dringender Tatverdacht vorliegt,
- bei schweren Verbrechen,
- wenn eine DNA-Analyse unabdingbar für die Ermittlung ist,
- wenn die Probe nicht mit Risiken oder beträchtlichen Schmerzen für den Betroffenen verbunden ist,
- wenn der Verhältnismäßigkeitsgrundsatz beachtet ist.

Viele Staaten differenzieren zudem nach dem Grad der Intimität des Probenmaterials, wobei an die Entnahme von Blut und Sperma hohe Anforderungen geknüpft werden. Da die Entnahme von Probenmaterial immer auch eine Beeinträchtigung des Rechts auf Privatleben gem. Art. 8 EMRK darstellt, seien – entsprechend dem Memorandum – insbesondere die Voraussetzungen des Art. 8 II EMRK zu beachten.[481] Aufgrund der fortschreitenden Technisierung hat das Ministerkomitee in Principle 8 letzter

[481] Committee of Ministers, Explanatory Memorandum zu Rec. (92) 1, Nr. 40 f.

Absatz auch die Einrichtung und den Betrieb einer DNA-Datei zum Zwecke der Untersuchung und Verfolgung von Straftaten unter einen Gesetzesvorbehalt gestellt.

(2) Speicherung zu festgelegten Zwecken und Zweckbindung

Nach Art. 5 lit. b) DSK müssen die Daten zum einen zu festgelegten Zwecken gespeichert werden und dürfen zum anderen nur zu den festgelegten Zwecken verwendet werden. Damit soll eine Speicherung für unbestimmte Zwecke verhindert werden. Die Bekanntgabe des Zwecks hat nach der Konvention spätestens mit Beginn des Speicherungsvorgangs zu erfolgen. Offensichtlich nicht erforderlich ist damit die Bekanntgabe des Zwecks bereits bei der Erhebung der Daten. Die OECD-Guidelines on the Protection of Privacy and Transborder Flows of Personal Data haben in Nr. 9 wohlweislich geregelt, dass bereits bei der Beschaffung der Daten der Zweck bekannt sein muss. Dies wäre auch sinnvoll gewesen, da der Schutz des Einzelnen eine möglichst frühzeitige Aufklärung verlangt, insbesondere da der Betroffene nur mit dieser Information wirklich entscheiden kann, ob und in welchem Umfang er Daten bekanntgibt.[482] Letztlich ist hierbei auch an Art. 5 lit. a) DSK zu denken, wonach die Daten „nach Treu und Glauben" beschafft werden müssen, worunter auch die Kenntnis vom späteren Verwendungszweck fällt.

Diese Lücke wird auch durch die Empfehlungen nicht vollständig geschlossen. Hinsichtlich der Sammlung der Daten enthält Principle 2 der Rec. R (87) 15 keine bestimmte Zweckangabe, ebenso wie Principle 3 zur Speicherung von Daten und Principle 4 zur Nutzung von Daten. Lediglich Principle 5.1 legt fest, dass eine Übermittlung nur zulässig ist, wenn legitime Interessen innerhalb des rechtlichen Aufgabenbereichs der Polizei für diese Übermittlung vorliegen. Dies grenzt die Zwecke zumindest für den

[482] Vgl. hierzu Henke, S. 103 f., Unger, S. 47.

Bereich der Übermittlung ein. Geht man jedoch nochmals an den Anfang der Empfehlung zum „Anwendungsbereich“, so ist dort festgelegt, dass die Empfehlung auf die Sammlung, Speicherung, Nutzung und Übermittlung von persönlichen Daten für polizeiliche Zwecke im Rahmen automatisierter Verarbeitung anzuwenden ist. Der Begriff „Polizeiliche Zwecke“ wird zwei Absätze weiter unten konkretisiert. Die gesamte Empfehlung ist damit nur für diese Zwecke anwendbar, mithin liegt also eine Zweckbestimmung vor.

Der Zweck der Rec. (92) 1 wird ebenfalls durch den Anwendungsbereich in Principle 2 bestimmt. Dieser sieht vor, dass die Sammlung von Proben und die DNA-Analyse nur für Zwecke der Identifikation im Rahmen der Untersuchung und Verfolgung von Straftaten zulässig ist. Auch die Verwendung für Forschungs- und statistische Zwecke wurde in Principle 3 Abs. 3 der Rec. (92) 1 für zulässig erklärt, sofern die Identität des Betroffenen nicht bestimmt werden kann, d.h. dass Namen und andere Hinweise zur Identifizierung vor der Nutzung für diese Zwecke beseitigt werden müssen. Die DSK verlangt, dass Daten nur zu den bekannten Zwecken verwendet werden dürfen. Ebenso verlangt Principle 3 Abs. 1 der Rec. (92) 1, dass die Analyse-Proben und die daraus gewonnenen Informationen nur für Fälle der Untersuchung und Verfolgung von Straftaten, jedoch nicht für andere Zwecke genutzt werden dürfen, es sei denn, der Betroffene wünscht, dass ihm die Informationen mitgeteilt werden. Ebenso verlangt Principle 3 Abs. 2 der Rec. (92) 1, dass Proben, welche für medizinische Zwecke gesammelt wurden, und die daraus gewonnenen Informationen nicht für Zwecke der Untersuchung und Verfolgung von Straftaten genutzt werden dürfen, außer es liegen Umstände vor, welche eine solche Ausnahme erlauben. Diese Umstände müssen jedoch ausdrücklich im nationalen Recht geregelt sein, bspw. bei

Einwilligung eines Patienten oder wenn sehr schwere Fälle vorliegen.[483]

Die zweite Voraussetzung, nämlich die Verwendung der Daten zum festgelegten Zweck, normiert den Zweckbindungsgrundsatz. Der Betroffene muss darauf vertrauen dürfen, dass seine Daten, welche er zur Speicherung freigegeben hat, nur zu den ihm bekannten Zwecken verwendet werden dürfen, es sei denn, er hat seine Zustimmung zu einer Zweckänderung gegeben.[484] Gerade aufgrund der Verarbeitung der Daten in automatisierten Dateien kann eine Zweckänderung hinsichtlich der Verwendung fatale Folgen für den Betroffenen nach sich ziehen; so besteht die Möglichkeit, dass seine Daten nun statt zur Verfolgung einer Straftat zur Erstellung eines vollumfänglichen Persönlichkeitsprofils genutzt werden oder dass seine DNA-Daten entgegen der gesetzlich eingeschränkten Verwendungsmöglichkeiten auch zur Erstellung eines Profils hinsichtlich seines Gesundheitszustandes oder seines Aussehen verwendet werden. Diesen Folgen versucht Art. 5 lit. b) DSK entgegenzuwirken. Allerdings wäre die Regelung nur vollständig, wenn die Bekanntgabe des Zwecks vor der Erhebung der Daten erfolgt, da zwischen der Erhebung der Daten und der Speicherung ein Zeitraum liegt, der eine Änderung des Zwecks und ferner auch eine manuelle Profilerstellung ermöglicht.

Nichtsdestotrotz ist in Art. 5 lit. b) DSK auch zu erkennen, dass selbst eine spätere Zweckänderung mit den bereits festgelegten Zwecken vereinbar sein – was jedoch ebenfalls einen erheblichen Beurteilungsspielraum zulässt – und sich an den Kriterien des Art.

[483] Committee of Ministers, Explanatory Memorandum zu Rec. (92) 1 Nr. 39.
[484] So Henke, S. 105.

5 lit. b) DSK messen lassen muss, d.h. auch der „neue“ Zweck muss festgelegt und rechtmäßig sein.[485]

(3) Inhaltliche Qualität der Daten

Art. 5 lit. c) und d) DSK regeln die inhaltliche Qualität der Daten. Nach Art. 5 lit. c) DSK müssen die Daten dem Speicherzweck entsprechen, „dafür erheblich sein und dürfen nicht darüber hinausgehen“. Damit sind sowohl die Arten der Daten als auch der Speicherumfang festgelegt worden. Die Daten müssen nicht nur im Rahmen des Speicherzwecks liegen, sondern auch dafür erforderlich sein. Der Einzelne soll somit vor nicht konkretisierten Datensammlungen geschützt werden.[486] Im Übrigen – und dies wird leider oft außer Acht gelassen – dient diese Vorschrift auch dem Nutzen des Datenverarbeiters. Vielfach wird von Anwendern der Datenschutz als lästig abgetan; dennoch dient der Datenschutz auch dem Schutz der Anwender und dem einfacheren Umgang mit Daten, d.h. die erforderlichen Speicherkapazitäten sind kleiner gehalten und aufgrund der geringeren Datenmenge sinkt auch das Risiko einer Überlastung des Speichersystems. Der Datenverarbeiter „muss“ demnach tatsächlich nur die Anzahl an Daten verarbeiten, die den Zwecken entspricht, was natürlich die Datenmengen und die damit verbundenen Kosten erheblich einschränkt.

Entsprechend der Vorschrift des Art. 5 lit. c) DKS verlangt Principle 2.1 der Rec. R 87 (15), dass die Sammlung von Daten für polizeiliche Zwecke auf solche Daten beschränkt werden muss, die für die Verhütung einer tatsächlichen Gefahr oder die Aufklärung von besonderen Straftaten notwendig sind. Ausnahmen hiervon sind nur zulässig, sofern diese im nationalen Recht speziell vorgesehen sind. Entsprechend dem Ministerkomitee soll Principle

[485] So auch Henke, S. 105.
[486] Vgl. Henke, S. 109.

2.1 die Grenzen des Art. 9 Abs.2 DSK bestimmen, welcher im Hinblick auf die Verfolgung von Straftaten Ausnahmen von Art. 5 lit. c) DSK zulässt. Principle 2.1 der Rec. R 87 (51) begrenzt damit die Sammlung von Daten auf das Notwendigste. Durch die Verwendung des Begriffs „tatsächliche Gefahr" soll ausgeschlossen werden, dass Daten bereits dann gesammelt werden, wenn nur die unbestimmte, spekulative Möglichkeit einer Gefahr gegeben ist, d.h. es muss ein begründeter Verdacht einer Straftat vorliegen.[487] Des Weiteren dürfen nach Principle 3.1, sofern möglich, nur korrekte Daten gespeichert werden und auch nur solche, welche sowohl zur Erfüllung der polizeilichen Aufgabe nach nationalem Recht als auch zur Erfüllung ihrer Pflichten nach internationalen Recht erforderlich sind. Dem Ministerkomitee war bei Zugrundelegung der Vorschrift bewusst, dass eine Speicherung zu polizeilichen Zwecken dauerhaft erfolgen würde.[488]

Nach Art. 5 lit. d) DSK müssen die Daten „sachlich richtig [sein] und wenn nötig auf den neuesten Stand gebracht" werden. Entgegen Art. 8 der OECD-Leitlinien, welcher zusätzlich noch die Vollständigkeit der Daten fordert, hat der Europarat hier eine Einschränkung vorgenommen, um die Datenverarbeiter nicht in erhöhtem Maße zu belasten und um der Möglichkeit vorzubeugen, dass vom Betroffenen wegen jeder Kleinigkeit Änderungen verlangt werden können.[489] Diese Überlegung ist auch richtig, wäre aber durch entsprechende Regelungen beim Recht auf Berichtigung abwendbar gewesen. Schließlich kann die Unvollständigkeit der Daten ebenfalls zu einem unrichtigen Verständnis vom Persönlichkeitsbild des Betroffenen führen. Allerdings ist davon auszugehen, dass unvollständige Daten

[487] Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 43.
[488] Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 50.
[489] S. Henke, S. 109 f.

unrichtig und damit ebenfalls vom Anwendungsbereich der DSK erfasst sind.[490]

In Anbindung an die Korrektheit der Daten, welche bereits in Principle 3.1 verlangt wird, fordert Principle 3.2 der Rec. R (87) 15, dass hinsichtlich der verschiedenen Datenkategorien nach Möglichkeit nach dem Grad der Richtigkeit und Zuverlässigkeit differenziert werden soll. Ebenso soll zwischen Daten, die auf Tatsachen basieren, und Daten, welche auf Meinungen und persönlichen Einschätzungen basieren, differenziert werden.

(4) Aufbewahrung der Daten

Art. 5 lit. e) DSK regelt die Aufbewahrung der Daten. Demnach müssen die Daten „so aufbewahrt werden, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern". Nach Meinung des Europarats bedeutet dies nicht, dass die Identifizierungsmerkmale unwiderruflich vom Namen des Betroffenen getrennt werden müssen, sondern nur, dass eine neuerliche Verlinkung nicht leicht wiederherstellbar sein darf.[491] Allerdings ist diese Interpretation des Europarats nicht mit dem Erforderlichkeitsgrundsatz vereinbar. Nach diesem dürfen Daten nämlich nur so lange gespeichert werden, wie sie erforderlich sind. Da die Datenverknüpfung allerdings wiederherstellbar ist, wenn auch unter Aufwendung erheblicher Mittel, genügt dies dem allgemein anerkannten Datenschutzgrundsatz nicht. Des Weiteren wird in Art. 5 lit. e) DSK der Zweckbindungsgrundsatz angesprochen. Wenn die Zwecke es demnach nicht mehr erfordern, dass die Daten weiter aufbewahrt werden müssen, warum sollte dann eine Verlinkung dennoch möglich bleiben? Letztlich würde dies dem Zweckbindungsgrundsatz zuwider laufen, denn bei einer erneuten

[490] Henke, S. 110.
[491] CoE, Explanatory Report, ETS No. 108, Nr. 42.

Verlinkung ist anzunehmen, dass sich auch der Zweck geändert hat, da der ursprüngliche Zweck aufgrund Zweckerreichung bereits erledigt ist. Wenn tatsächlich eine neuerliche Herstellung der Daten erforderlich ist, dann sind hierfür gewichtige Interessen erforderlich. Doch bei Vorliegen solcher Interessen greift Art. 9 DSK, weshalb eine Einschränkung der Interpretation durch den Europarat überhaupt nicht erforderlich ist. Aus diesem Grunde ist der Interpretation des Europarats nicht zu folgen.[492] Daher sollte eine Verlinkung nicht wieder möglich sein, alles andere wäre lediglich eine Sperre von unbestimmter Zeit. Der Grund für die Regelung ist schließlich, Missbrauch der Daten sowie die Anhäufung beträchtlicher Datenbestände zu verhindern, sei es durch den Datenverarbeiter selbst oder durch externe Stellen. Gerade hierfür ist es daher erforderlich, die Daten vollständig zu vernichten bzw. unwiderruflich zu anonymisieren.

Principle 7.1 der Rec. R (87) 15 fordert ausdrücklich eine Löschung der Daten, sofern diese für die Zwecke, für die sie gespeichert wurden, nicht länger notwendig sind. Damit entspricht Principle 7.1. im Wesentlichen Art. 5 lit. e) der DSK, allerdings mit der Maßgabe, dass eine Löschung vorzunehmen ist. Da mit der Löschung der Daten diese unwiderruflich verloren sind, hat das Ministerkomitee in Principle 7.1 Kriterien festgelegt, welche bei der Überlegung, ob die Daten gelöscht werden sollen, berücksichtigt werden müssen: die Notwendigkeit, Daten für die Feststellung eines Verbrechens in speziellen Fällen zurückzubehalten; eine endgültige richterliche Entscheidung; Rehabilitation; Gnadenerlasse, verbrauchte Verurteilungen; Alter des Betroffenen. Nach Principle 7.2 der Rec. R (87) 15 sollen Regelungen in Bezug auf feste Aufbewahrungszeiten für die verschiedenen Kategorien von Daten sowie regelmäßige Qualitätskontrollen in

[492] So im Ergebnis auch Henke, S. 107.

Übereinstimmung mit der Aufsichtsbehörde oder mit dem nationalen Recht festgelegt werden.

In Bezug auf die DNA-Daten wurde in Principle 8 Abs. 1 der Rec. (92) 1 empfohlen, DNA-Proben und anderes Körpergewebe nicht länger als bis zur endgültigen richterlichen Entscheidung des Falles, für den die Proben verarbeitet wurden, aufzubewahren, sofern die Zwecke für eine eventuelle neue Verwendung nicht denen entsprechen, für die sie gespeichert wurden. Entsprechend Principle 8 Abs. 1 sollen gem. Abs. 2 Maßnahmen ergriffen werden, damit die Ergebnisse der DNA-Analyse und die daraus gewonnenen Informationen gelöscht werden, wenn sie nicht länger notwendig sind. Allerdings wird in Satz 2 anerkannt, dass eine Löschung der Daten in speziellen Fällen nicht zweckmäßig ist, nämlich wenn jemand eines schweren Verbrechens gegen das Leben, die Integrität und die Sicherheit einer Person verurteilt worden ist. In diesem Fall sind dann strenge Aufbewahrungszeiten durch das nationale Recht festzulegen. Bei Verbrechen, die gegen die Sicherheit des Staates gerichtet sind, ist eine Einbehaltung der Proben, der Ergebnisse und der daraus erhaltenen Informationen sogar dann erlaubt, wenn der Betroffene nicht angeklagt oder verurteilt wurde. Allerdings sind auch in diesem Fall strenge Aufbewahrungsfristen festzulegen (vgl. Principle 8 Abs. 4). Ausnahmsweise ist eine Speicherung darüber hinaus außerdem dann zulässig, wenn der Betroffene dies erbittet (bspw. um bei weiteren Straftaten als Verdächtiger ausgeschlossen zu werden) oder wenn es sich um Spuren-DNA handelt, Principle 8 Abs. 3.

c) SENSIBLE DATEN

Art. 6 DSK schützt sensible Daten, also Informationen über die rassische Herkunft, politische Anschauungen oder religiöse oder andere Überzeugungen, Informationen über die Gesundheit und das Sexualleben. Solche Daten dürfen nach Art. 6 DSK nur

verarbeitet werden, wenn das innerstaatliche Recht einen geeigneten Schutz vorsieht. Der Ausdruck „innerstaatliches Recht" ist dabei weit zu verstehen; darunter fallen alle Bestimmungen oder Verwaltungsrichtlinien, solange der notwendige Schutz des Einzelnen sichergestellt ist.[493] Auf welche Weise der Schutz gewährleistet wird, bleibt den Staaten überlassen. Entscheidend ist die konkrete Verwendung der Daten; hiervon hängt die Geeignetheit des Schutzes ab, weshalb auch bei jedem Verarbeitungsvorgang eine gesonderte Prüfung vorgenommen werden sollte. Wenn man sich die Vorschrift des Art. 6 DSK genau ansieht, stellt man fest, dass das Sammeln der Daten nicht von Art. 6 DSK umfasst ist. Der Europarat ging seinerzeit davon aus, dass die manuell gesammelten Daten – entsprechend der Begründung zu Art. 2 lit. c) DSK – keine besonderen Gefahren bergen. Dies steht jedoch im Widerspruch zu seiner Meinung über sensible Daten. Gerade der Schutz dieser Daten sei besonders wichtig, weshalb es mit Art. 6 DSK auch eine dementsprechende Regelung gegeben habe.[494] Die OECD hatte damals einen solchen Schutz mit der Begründung abgelehnt, dass personenbezogene Daten nicht grundsätzlich sensibel seien, sondern dies mit der Art und dem Zweck der Verwendung sowie dem Gebrauch der Daten zusammenhänge und nicht von der Beschaffenheit einer Information abhängig sei.[495] Obwohl dem Europarat bei der Erstellung der DSK bekannt war, dass die OECD-Leitlinien keine dem Art. 6 DSK entsprechende Vorschrift enthielten, wollte er gewisse Arten von Daten einem besonderen Schutz unterstellen,

[493] CoE, Explanatory Report, ETS No. 108, Nr. 46.
[494] vgl. Henke, S. 113 ff.
[495] OECD-Guidelines on the protection of Privacy and Transborder Flows of Personal Data, Explanatory Memorandum Nr. 50, einsehbar unter www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html#guidelines; Henke, S. 112; Unger, S. 50.

da z.T. schon die Verarbeitung bestimmter Kategorien von Daten an sich zu Verletzungen der individuellen Rechte führen kann.[496]

Ebenso weit zu verstehen ist der Begriff der „Daten über die Gesundheit". Zur Zeit der Ausarbeitung der DSK wurde eine gesonderte Empfehlung auf dem Gebiet automatischer medizinischer Datenbanken entworfen und verabschiedet. Während diese Empfehlung den Schutz medizinischer Daten nur eingeschränkt gewährleistet, nämlich nur für solche in medizinischen Datenbanken, [497] ist Art. 6 DSK umfassender und schützt medizinische Daten auch in anderen Datenbanken.[498] Von Art. 6 DSK sind somit alle Informationen der Vergangenheit, der Gegenwart und der Zukunft, physisch oder psychisch, bezogen auf kranke, gesunde oder bereits verstorbene Menschen, geschützt. So sind auch Informationen erfasst, welche in Zusammenhang mit Alkoholmissbrauch und Drogenkonsum stehen.[499]

Von Art. 6 DSK sind ferner nicht nur Daten über die Rasse, die politische Anschauung und religiöse Überzeugungen geschützt, sondern auch sämtliche Tätigkeiten, welche mit der Ausübung dieser Anschauungen und Überzeugungen im Zusammenhang stehen.[500]

Art. 6 DSK ist nicht abschließend. In Übereinstimmung mit Art. 11 DSK können weitere sensible Daten bestimmt werden, deren Verarbeitung vorgeschrieben oder begrenzt wird. Der Grad der Sensibilität der Daten hängt dabei im Wesentlichen vom rechtlichen und soziologischen Hintergrund des Landes ab. So können Informationen im einen Land bereits für sich allein zu einem Risiko für den Persönlichkeitsbereich führen, wohingegen in

[496] CoE, Explanatory Report, ETS No. 108, Nr. 43; Henke, S. 113, 115.
[497] Recommendation Nr. R (81) 1.
[498] S. auch Henke, S. 117.
[499] CoE, Explanatory Report, ETS No. 108, Nr. 45.
[500] CoE, Explanatory Report, ETS No. 108, Nr. 44.

einem anderen Land weitere Umstände für eine Gefährdung hinzukommen müssen. Der Europarat hat dies anhand der Gewerkschaftszugehörigkeit deutlich gemacht.[501]

Auch Art. 6 DSK ist von der Ausnahmevorschrift des Art. 9 Abs. 2 DSK erfasst.

In Principle 2.4 der Rec. R (87) 15 wird die Sammlung von Daten über die Rasse, die religiöse Weltanschauung, das Sexualverhalten sowie über politische Meinungen oder die Zugehörigkeit zu Organisationen ebenfalls für unzulässig erklärt. Hierbei ist auffällig, dass – anders als bei Art. 6 DSK – bereits die Sammlung dieser Daten verboten wird. Eine Sammlung dieser Daten ist nur zulässig, wenn diese für eine bestimmte Untersuchung absolut notwendig ist. Der Ausdruck „particular inquiry" ist als generelle Begrenzung anzusehen. Eine solche Untersuchung muss auf Tatsachen basieren, welche den Schluss zulassen, dass eine schwere Straftat begangen worden ist oder begangen werden wird.[502]

d) DATENSICHERUNG

Gemäß Art. 7 DSK sind zum Schutz personenbezogener Daten, welche in automatisierten Dateien gespeichert sind, „geeignete Sicherungsmaßnahmen (…) gegen die zufällige oder unbefugte Zerstörung, gegen zufälligen Verlust sowie gegen unbefugten Zugang, unbefugte Veränderung oder unbefugtes Bekanntgeben" zu treffen.

Unter „Zerstörung" ist die Unbrauchbarmachung von Datenverarbeitungsanlagen sowie die „unrechtmäßige Vernichtung der Datenbestände" zu verstehen. Mit „zufälligem Verlust" ist die unabsichtliche Löschung gemeint. Durch

[501] CoE, Explanatory Report, ETS No. 108, Nr. 48.
[502] Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 48.

Maßnahmen zum Schutz gegen „unbefugten Zugang“ sollen der Zugang und der Zugriff durch Nichtberechtigte abgewehrt werden. Unter „unbefugten Veränderungen“ sind nicht legitimierte verändernde Eingriffe in die Soft- oder Hardware, aber auch unmittelbar in die gespeicherten Daten zu verstehen. Durch Maßnahmen zum Schutz gegen „unbefugte Bekanntgabe“ soll verhindert werden, dass nichtberechtigte Personen Zugriffsmöglichkeiten erhalten bzw. dass solchen Personen Daten weitergegeben werden.[503]

Der Europarat hat bei der Regelung der Datensicherung bedacht, dass Einwirkungen durch zufällige Ereignisse und Eingriffe durch Unbefugte nicht nur den Datenverarbeitungsvorgang beeinträchtigen, sondern auch den Schutz des Einzelnen. Demgemäß wird der Staat aufgefordert, den Datenverarbeitern entsprechende Pflichten zur Sicherung der Datenanlage und der Rechte des Einzelnen aufzuerlegen. Hierfür kommen physische Maßnahmen (gesicherte Türen etc.), organisatorische Maßnahmen (Vorschriften über Zugangsberechtigungen, diverse Richtlinien etc.) sowie technische Hilfsmittel (Verschlüsselung etc.) in Betracht.[504] Allerdings konnten aufgrund der sich verändernden technischen Gegebenheiten keine festen Regelungen getroffen werden; vielmehr wurde nur ein flexibler Rahmen festgelegt, der den Mitgliedstaaten die Möglichkeit gibt, auf technische Veränderungen zu reagieren.[505]

Hierbei sind für jede Datei spezielle Sicherheitsvorkehrungen unter Einbeziehung des Schadenspotentials der jeweiligen Datei zu treffen.[506] Dabei sind u.a. die Dauer der Speicherung, die Quantität der Daten, die Sensibilität, der Zweck der Verarbeitung sowie die

[503] zu diesem Absatz s. Henke, S. 122.
[504] Henke, S. 121 f.
[505] Henke, S. 123.
[506] CoE, Explanatory Report, ETS No. 108, Nr. 49.

daraus resultierenden Gefahren in die Überlegungen darüber einzubeziehen, welche Schutzmaßnahmen ergriffen werden müssen.[507]

Des Weiteren müssen die Sicherheitsvorkehrungen geeignet sein, d.h. die spezifische Funktion der Datei und deren Risiken müssen abgewogen werden.[508] Etwaige dadurch entstehende Kosten muss der Datenverarbeiter dulden. *Henke* sieht dies als Folge dessen, dass der Datenverarbeiter durch die Verarbeitung erst die Risiken schafft, weshalb er auch verpflichtet ist, entsprechende Maßnahmen zu ergreifen, auch wenn diese etwas mehr kosten.[509] Die Sicherheitsvorkehrungen müssen auf den gängigen Datenschutzmethoden basieren.[510]

Leider hat der Europarat auch hier versäumt, die Beschaffung der Daten in den Schutz des Art. 7 DSK aufzunehmen, weshalb bis zum Zeitpunkt der Speicherung zahlreiche Gefahren vorhanden sind, sei es durch unbefugten Zugang oder Zerstörung der Daten etc.[511]

Auch Principle 8 der Rec. R (87) 15 trifft eine Regelung zur Datensicherung. Danach hat die verantwortliche Person die notwendigen Maßnahmen zu treffen, um eine angemessene Sicherheit der Daten zu gewährleisten und unbefugten Zugang, Übermittlung oder Änderung zu verhindern. Dabei sind die verschiedenen Eigenschaften und Inhalte der Dateien zu berücksichtigen. Hinsichtlich des Begriffs „communication“ hat das Ministerkomitee im Besonderen die Übermittlung nach Principle 5 im Blick gehabt. Principle 8 wurde anders formuliert als Art. 7 DSK, so dass der Schutzumfang etwas geringer ist. So wurde

[507] Henke, S. 123.
[508] CoE, Explanatory Report, ETS No. 108, Nr. 49.
[509] Henke, S. 125.
[510] CoE, Explanatory Report, ETS No. 108, Nr. 49.
[511] So auch Henke, S. 126.

statt „Zerstörung“, „Verlust“ und „Veränderung“ in Principle 8 nur der Begriff „Änderung“ verwendet, d.h. Sicherungsmaßnahmen gegen Zerstörung und Verlust sind nicht erforderlich; eine „Änderung“ enthält sinngemäß die Überlegung, dass nach der Nutzung noch Daten vorhanden sind, was bei der „Zerstörung“ und dem „Verlust“ nicht mehr der Fall ist.

Die Empfehlung Rec. (92) 1 konkretisiert die Sicherheitsmaßnahmen in Bezug auf die Laboratorien und Institutionen, welche bei der DNA-Analyse beteiligt sind. Demnach sollen nach Principle 6 DNA-Analysen nur von Laboratorien ausgeführt werden, welche angemessene Einrichtungen und Erfahrungen haben. Die Mitgliedstaaten sollen sicherstellen, dass eine Liste aufgestellt wird, in welcher die zugelassenen Laboratorien oder Institutionen angegeben werden, welche die folgenden Kriterien erfüllen: hohes Wissen und Fachkenntnis, verbunden mit angemessenen Qualitätskontrollverfahren; wissenschaftliche Integrität; angemessene Sicherheit der Anlagen und der Untersuchungsmaterialien; angemessene Sicherheiten im Hinblick auf die Geheimhaltung; Gewährleistung, dass die Regelungen der Rec. (92) 1 eingehalten werden. Dabei spielt es letztlich keine Rolle, ob die Institutionen in privater oder öffentlicher Hand sind. Das Ministerkomitee kam zu dem Ergebnis, dass bei solchen in öffentlicher Hand zwar Zweifel an der Unabhängigkeit der Laboratorien aufkommen könnten; bei solchen in privater Hand könnte jedoch Befangenheit angenommen werden, wenn eine Person für eine Analyse bezahlt. Aus diesem Grund verlangt das Ministerkomitee wissenschaftliche Integrität.[512] Des Weiteren sollten die Mitgliedstaaten entsprechend Principle 10 der Rec. (92) 1 die nationale und internationale Standardisierung der DNA-Analyse-Methoden fördern.

[512] Committee of Ministers, Explanatory Memorandum zu Rec. (92) 1, Nr. 45.

e) AUSNAHMEN UND EINSCHRÄNKUNGEN NACH ART. 9 I, II DSK

Art. 9 DSK lässt entsprechend seinen Abs. 2 und 3 Ausnahmen von den Art. 5, 6 und 8 DSK zu. Da für die vorliegende Arbeit jedoch nur Art. 9 Abs. 2 DSK relevant ist, bleibt Abs. 3 außer Betracht.

Art. 9 Abs. 2 DSK lässt eine Abweichung zu, wenn „sie durch das Recht der Vertragspartei vorgesehen und in einer demokratischen Gesellschaft eine notwendige Maßnahme ist a) zum Schutz der Sicherheit des Staates, der öffentlichen Sicherheit (...) oder zur Bekämpfung von Straftaten; b) zum Schutz des Betroffenen oder der Rechte und Freiheiten Dritter".

Nach Art. 9 Abs. 2 DSK ist eine solche Abweichung jedoch nur möglich, sofern „sie durch das Recht der Vertragspartei vorgesehen ist", wohingegen Art. 9 Abs. 3 DSK eine Einschränkung nur durch Gesetz zulässt. Der Wortlaut des Art. 9 Abs. 2 DSK sagt bereits aus, dass eine Ermächtigungsgrundlage im nationalen Recht vorhanden sein muss, allerdings nicht, von welcher Qualität diese sein sollte. *Henke* ist aufgrund der oftmals gravierenderen Eingriffe im Sinne des Art. 9 Abs. 2 DSK der Auffassung, dass auch für Einschränkungen nach Art. 9 Abs. 2 ein formelles Gesetz erforderlich ist, um den Einzelnen vor einschränkenden Maßnahmen der Exekutive zu schützen.[513]

Des Weiteren verlangt Art. 9 Abs. 2 DSK, dass es sich bei der Maßnahme um eine „notwendige" handelt. Da die Notwendigkeit der Maßnahmen in den verschiedenen Ländern und zu verschiedenen Zeiten ganz unterschiedlich ausfallen kann, wurde hiermit eine allgemeingültige Formulierung gewählt. Der Maßstab ist dabei im Lichte der jeweiligen Landessituation auszulegen.[514]

---

[513] Henke, S. 149.

[514] CoE, Explanatory Report, ETS No. 108, Nr. 55; so auch Henke, S. 149 f.

Art. 9 Abs. 2 DSK listet die wichtigsten Interessen auf, für welche von den Bestimmungen der DSK Ausnahmen gemacht werden müssen. Um den Staaten allerdings keinen übermäßig großen Spielraum zu eröffnen, wurden die Ausnahmen genau bezeichnet.[515]

Der Begriff der „Staatlichen Sicherheit" in Art. 9 Abs. 2 lit. a) DSK ist zu verstehen als Schutz der nationalen Hoheitsgewalt gegen interne und externe Bedrohungen sowie Schutz der internationalen Beziehungen des Staates.[516] Unter „öffentlicher Sicherheit" ist die „Unverletzlichkeit der subjektiven Rechte und Rechtsgüter des Einzelnen sowie die Garantie der objektiven Rechtsordnung und der Einrichtungen des Staates"[517] zu verstehen. Die „Bekämpfung von Straftaten" erfasst die Ermittlung und Verfolgung von Straftaten, mithin also die repressive Tätigkeit der Exekutivbehörden.[518] Präventivmaßnahmen sind daher nicht von Art. 9 Abs. 2 DSK umfasst, wobei jedoch die genaue Abgrenzung im Einzelfall oftmals schwierig sein dürfte. Einleuchtend ist demnach, dass die Daten spätestens dann gelöscht werden sollten, wenn erkannt wird, dass die verfolgte Spur unzutreffend ist.[519]

Nach Art. 9 Abs. 2 lit. b) DSK sind zudem Ausnahmen von den Bestimmungen zum Schutz der Betroffenenrechte und zum Schutz eines Dritten möglich.

Die Empfehlungen Rec. R (87) 15 und (92) 1 schränken die Begrenzung durch die Ausnahmevorschriften des Art. 9 DSK stark ein (siehe oben).

Allerdings sieht auch Principle 6.4 der Rec. R (87) 15 Einschränkungen des Rechts auf Zugang, Berichtigung und

515 CoE, Explanatory Report, ETS No. 108, Nr. 56.
516 CoE, Explanatory Report, ETS No. 108, Nr. 56.
517 Henke, S. 151.
518 CoE, Explanatory Report, ETS No. 108, Nr. 56.
519 Henke, S. 153.

Löschung vor, sofern die Beschränkung unabdingbar für die Erfüllung der polizeilichen Aufgabe ist oder dies für den Schutz der Rechte des Betroffenen oder der Rechte und Freiheiten anderer notwendig ist. Principle 6.4 ähnelt damit Art. 9 Abs. 2 DSK. So ist eine Beschränkung z.B. erforderlich, um Zeugen oder Informanten zu schützen.

f) GRENZÜBERSCHREITENDER DATENSCHUTZ

Für personenbezogene Daten, welche automatisiert verarbeitet oder für eine solche Verarbeitung beschafft wurden, sind die Regelungen des Art. 12 DSK anzuwenden, sofern ein staatenübergreifender Datenverkehr stattfindet. Des Weiteren ist der Anwendungsbereich des Art. 12 DSK nur eröffnet, wenn es um den Datenaustausch zwischen Vertragsstaaten geht. Ziel des Art. 12 DSK ist es, die Erfordernisse eines effektiven Datenschutzes mit dem Prinzip des freien Datenflusses des Art. 10 EMRK abzugleichen.[520]

Art. 12 Abs. 1 DSK legt den Anwendungsbereich des grenzüberschreitenden Datenverkehrs fest. Es kommt nicht auf die Art des Datenträgers an, ebenso wenig auf die Art und Weise der Übermittlung.[521] Der Europarat hat einige Faktoren der Übermittlung in seinem Explanatory Report zur DSK besonders berücksichtigt, u.a. die Art der Darstellung der Daten (kodiert, Klartext), das Speichermedium (Dokument, Lochkarte, Magnetband etc.), die Transportart (Mail, der mit physischen Mitteln durchgeführte Transport, Telekommunikationsverbindung), die Verbindungsart (PC zu PC, PC zu Terminal, Verbindung manueller Datenbestände mit automatisierten Sammlungen), die Verbindung (vom Ursprungsland zum Zielort oder über Transitländer), die

[520] CoE, Explanatory Report, ETS No. 108, Nr. 62.
[521] Ellger, S. 471.

Beziehung zwischen Sender und Empfänger.[522] Zum Anwendungsbereich des Art. 12 Abs. 1 DSK gehört auch die Datenbeschaffung; damit soll verhindert werden, dass Daten in einem Land gesammelt und in einem anderen Land verarbeitet werden, um die Regelungen der DSK zu umgehen.[523] Aus Art. 12 Abs. 1 DSK ist weiter ersichtlich, dass die Bestimmungen nur für die Übermittlung von personenbezogenen Daten gelten. Es ist allerdings auch klar, dass die Bestimmungen des Art. 12 DSK zudem für andere Daten gelten, sofern die Vertragsstaaten die Anwendbarkeit gem. Art. 3 Abs. 2 lit. b) DSK auf diese ausgedehnt haben, d.h. diese Staaten können dann Übermittlungseinschränkungen vornehmen. Andererseits sind Staaten, welche bestimmte Daten gem. Art. 3 Abs. 2 lit. b) DSK von dem Anwendungsbereich der DSK ausgeschlossen haben, als Nicht-Vertragsstaaten zu behandeln, weswegen auch hier eine Übermittlungseinschränkung zu Lasten dieser Staaten vorgenommen werden kann.[524] Des Weiteren ist unter Datenweitergabe i.S.d. Art. 12 Abs. 1 DSK nur der Export zu verstehen. Die importierten Daten fallen hingegen nicht darunter, da diese von den Datenschutzregelungen des einführenden Staates erfasst werden[525], d.h. mit dem Eintritt der Daten in das Hoheitsgebiet des Empfängerlandes unterliegen diese den innerstaatlichen Datenschutzbestimmungen[526]. Der Europarat hat auch das Problem des Re-Imports von Daten erkannt, welche im Ausland unter Verletzung der Bestimmungen des Ursprungslands verarbeitet wurden. Allerdings hat der Europarat das Problem entschärft, indem er das Ursprungsland dazu verpflichtet,

[522] CoE, Explanatory Report, ETS No. 108, Nr. 63.
[523] CoE, Explanatory Report, ETS No. 108, Nr. 64.
[524] CoE, Explanatory Report, ETS No. 108, Nr. 65.
[525] CoE, Explanatory Report, ETS No. 108, Nr. 66.
[526] So Henke, S. 164.

Maßnahmen entsprechend Art. 12 DSK zu treffen, bevor die Daten exportiert werden.[527]

Nach Art. 12 Abs. 2 DSK darf der grenzüberschreitende Datenverkehr allein zum Zweck des Persönlichkeitsschutzes nicht verboten oder von einer besondere Genehmigung abhängig gemacht werden. Diese Regelung ist missverständlich. Der Europarat hat in seinem Explanatory Report zur DSK klargestellt, dass ein Vertragsstaat sich nicht auf die Konvention berufen darf, sofern Störungen beim grenzüberschreitenden Datenverkehr auftreten, es sei denn, die Gründe liegen gerade im Schutz des Persönlichkeitsrechts.[528] Vom Wortlaut des Art. 12 Abs. 2 DSK gedeckt ist die Möglichkeit, Regelungen zu treffen, um sich über den Datentransfer zwischen dem eigenen Hoheitsgebiet und dem eines anderen Vertragsstaates zu informieren. Demnach wären Regelungen, welche zur Anmeldung von grenzüberschreitenden Datenübermittlungen verpflichten, mit Art. 12 Abs. 2 DSK vereinbar; allerdings dürften diese nur zu Informationszwecken dienen und nicht zu versteckten Beschränkungen führen.[529] Ferner ist eine Vertragspartei trotz der Vorschrift des Art. 12 Abs. 2 DSK nicht gehindert, konkrete einschränkende Maßnahmen hinsichtlich bestimmter grenzüberschreitender Übermittlungen zu erlassen, sofern diese ungeachtet dessen Anwendung finden, ob solche Übermittlungen innerhalb des Staates erfolgen oder über die Grenzen hinweg[530], d.h. es darf keine Ungleichbehandlung zwischen innerstaatlichen und grenzüberschreitenden Datentransfers stattfinden.[531]

Abweichungen von Art. 12 Abs. 2 DSK sind möglich, sofern eine Vertragspartei bestimmte Arten von personenbezogenen Daten

[527] CoE, Explanatory Report, ETS No. 108, Nr. 66.
[528] CoE, Explanatory Report, ETS No. 108, Nr. 67; so auch Henke, S. 166.
[529] CoE, Explanatory Report, ETS No. 108, Nr. 67; s. auch Henke, S. 167; Ellger, S. 474.
[530] CoE, Explanatory Report, ETS No. 108, Nr. 67.
[531] S. auch Henke, S. 168.

oder Dateien wegen ihrer Beschaffenheit einem besonderen Schutz unterstellt, wobei hierbei auch dann kein Verbot möglich ist, wenn die andere Vertragspartei einen gleichwertigen Schutz vorsieht (Art. 12 Abs. 3 lit. a), oder „um zu verhindern, dass ihr [i. e. der Vertragspartei, Anm. d. Verf.] Recht dadurch umgangen wird, dass eine Weitergabe aus ihrem Hoheitsgebiet in das Hoheitsgebiet einer Nichtvertragspartei auf dem Weg über das Hoheitsgebiet einer anderen Vertragspartei erfolgt", sog. „Transitdatenverkehr" (Art. 12 Abs. 3 lit. b). Unter „bestimmten Arten von personenbezogenen Daten oder automatisierten Dateien/Datensammlungen" sind solche Daten zu verstehen, welche in Art. 6 DSK gemeint sind, sowie andere Datenkategorien. Ein Vertragsstaat kann diese Daten in Übereinstimmung mit Art. 11 DSK über das Minimum der datenschutzrechtlichen Regelungen des Kapitels 2 der DSK hinaus schützen. [532] Des Weiteren kann es sein, dass manche Staaten den Schutz der in Art. 6 DSK genannten Daten gem. Art. 9 Abs. 2 DSK eingeschränkt haben bzw. das Übereinkommen gem. Art. 3 Abs. 2 lit. a) DSK nicht auf die in Art. 6 DSK genannten Daten anwenden. Damit ist bei den Staaten, welche die Regelungen der DSK ohne Einschränkungen übernommen haben, automatisch ein höherer Schutz vorhanden, welcher zur Anwendung des Art. 12 Abs. 3 lit. a) DSK berechtigt, sofern sich die nationalen Schutzmaßnahmen von denen des Empfängerstaates „wesentlich" unterscheiden.[533] Dabei ist insbesondere zu beachten, dass manche Staaten psychologische Daten oder Daten über Alkoholmissbrauch explizit besonderen Schutzmaßnahmen unterwerfen, während andere Staaten diese entweder als „medizinische Daten" einem gleichwertigen Schutzniveau wie erstere unterwerfen oder aber diese Daten gar keinem Schutz unterwerfen; nur letzteres berechtigt zur

[532] CoE, Explanatory Report, ETS No. 108, Nr. 69.
[533] CoE, Explanatory Report, ETS No. 108, Nr. 69.

Anwendung des Art. 12 Abs. 3 lit. a) DSK, da nur hier ein „wesentlicher“ Unterschied vorhanden ist.[534] Diese Auslegung steht auch in Einklang mit HS. 2 des Art. 12 Abs. 3 lit. a) DSK, wonach eine Abweichung von Art. 12 Abs. 2 DSK nicht möglich ist, sofern die Vorschriften der anderen Vertragspartei einen gleichwertigen Schutz vorsehen. Was darunter jedoch genauer zu verstehen ist, lässt sich weder durch die Konvention noch durch den dazu verfassten Explanatory Report ersehen.[535]

Art. 12 Abs. 3 lit. b) DSK sieht Ausnahmen von Art. 12 DSK vor, sofern ein Datentransfer in einen Nichtvertragsstaat über einen Vertragsstaat vorgenommen werden soll. Die Behörden können dann den Datenexport in den Vertragsstaat untersagen, wenn zu befürchten ist, dass der datenschutzrechtliche Rahmen umgangen wird. Allerdings kann diese Beschränkung nur dann Anwendung finden, wenn eindeutig feststeht, dass der Vertragsstaat als Transitland benutzt wird; die bloße Wahrscheinlichkeit oder die Erwartung, dass dies so geschieht, reicht nicht aus, da sonst generelle Ausfuhrverbote zu befürchten sind. Auf der anderen Seite ist der Ursprungsstaat auch nicht verpflichtet, sich auf Art. 12 Abs. 3 lit. b) DSK zu berufen; vielmehr kann ein Staat sogar bewusst auf Genehmigungsvorbehalte verzichten, weil bspw. der Nichtvertragsstaat seinerseits befriedigende Datenschutzregelungen bereitstellt.[536]

Eine weitere Ausnahme ergibt sich aus dem Explanatory Report zur DSK, wonach Datenübermittlungen in mehrere Staaten, d.h. sowohl in Vertragsstaaten als auch in Nicht-Vertragsstaaten, möglich sind. In diesen Fällen hat jedoch der ausführende Staat sicherzustellen, dass solche Übermittlungen nicht Anlass für umfangreiche Untersuchungen und Genehmigungsverfahren

[534] Henke, S. 170 f.
[535] So auch Henke, S. 171; Ellger, S. 476.
[536] CoE, Explanatory Report, ETS No. 108, Nr. 70; so auch Henke, S. 172 ff.

bilden, sondern dass vielmehr eine Genehmigung ohne ausführliche Prüfung möglich ist.[537]

Grenzüberschreitende Übermittlungen in Nicht-Vertragsstaaten werden von dem Zusatzprotokoll zur DSK geregelt. Nach Art. 2 Abs. 1 DSK-ZP dürfen Daten in Staaten oder an Organisationen, welche nicht Vertragspartei sind, nur weitergegeben werden, wenn diese ein angemessenes Schutzniveau vorsehen. Die Adäquanz dieses Schutzniveaus bemisst sich anhand der Umstände des jeweiligen Transfers, d.h. der Datenarten, der Ziele und der Dauer der Verarbeitung, anhand des Ursprungs- und des Ziellands, der rechtlichen Regelungen, insbesondere anhand von berufsrechtlichen und sicherheitsrechtlichen Regelungen.[538] Allerdings ist die Weitergabe von Daten abweichend von Art. 2 Abs. 1 DSK-ZP erlaubt, a) „wenn dies im internen Recht vorgesehen ist wegen spezifischer Interessen des Betroffenen oder wegen berechtigter überwiegender Interessen (...) oder b) wenn Garantien, die sich insbesondere aus Vertragsklauseln ergeben können, von der für die Weitergabe verantwortlichen Stelle geboten werden und diese (...) für ausreichend befunden werden". Unter „berechtigten überwiegenden Interessen" sind solche des Art. 8 Abs. 2 EMRK sowie des Art. 9 Abs. 2 DSK zu verstehen. Des Weiteren ist eine Abweichung zu Gunsten der Interessen eines Betroffenen möglich, d.h. wenn eine Datenübermittlung zu Zwecken der Vertragserfüllung oder im Interesse des Betroffenen, ferner zum Schutz seiner lebenswichtigen Interessen und bei Vorliegen eines Einverständnisses des Betroffenen vorgenommen wird. Ein Einverständnis ist aber nur dann von Belang, wenn der Betroffene vorher angemessen über den bevorstehenden Transfer informiert wurde.[539] Eine weitere Einschränkung des

[537] CoE, Explanatory Report, ETS No. 108, Nr. 68; so auch Henke, S. 175.
[538] CoE, Explanatory Report, ETS No. 181, Nr. 26 f.
[539] CoE, Explanatory Report, ETS No. 181, Nr. 31.

Übermittlungsverbots ergibt sich, wenn Vertragsklauseln zwischen den Transferstellen vorhanden sind. In diesen müssen zum Schutz des Betroffenen die wesentlichen Elemente des Datenschutzes geregelt sein. Dies beinhaltet auch die Angabe einer Kontaktperson, welche für den Datenverkehr verantwortlich ist, sowie die Möglichkeit des Betroffenen, diese zu jeder Zeit ohne weitere Kosten anzurufen, damit sie u.a. seine Rechte ausübt.[540]

Art. 12 DSK sowie das Zusatzprotokoll sind augenscheinlich recht vage ausgedrückt.

Die Principles 5.4 und 5.5 ii. der Rec. R (87) 15 gehen hier etwas weiter und formulieren speziellere Voraussetzungen. Gem. Principle 5.4 soll die Datenübertragung der persönlichen Daten, welche vom Rec. R (87) 15 umfasst sind, auf Polizeibehörden beschränkt werden. Des Weiteren soll eine Übermittlung nur dann zulässig sein, a) wenn eine klare rechtliche Regelung im nationalen oder internationalen Recht besteht oder b) sofern keine solche Regelung existiert, dann nur, wenn die Übertragung für die Verhütung einer erheblichen und drohenden Gefahr oder die Bekämpfung eines schweren Verbrechens erforderlich ist. Beide Tatbestände stehen jedoch unter der Voraussetzung, dass innerstaatliche Bestimmungen zum Schutz des Betroffenen nicht beeinträchtigt werden. Diese Bestimmung spiegelt gewissermaßen Art. 12 DSK wider, welcher einen „adäquaten Schutz“ des Betroffenen verlangt. Verhängt also der übertragende Staat bestimmte Schutzbestimmungen, so sind diese vom Empfängerstaat zu befolgen. Nach Principle 5.5 ii. der Rec. R (87) 15 ist zudem vor einer Übertragung die Qualität der Daten zu überprüfen, da dies der letztmögliche Zeitpunkt ist, bevor die Daten aus der Hand gegeben werden. Es ist zudem zur Kenntnis zu nehmen, dass in den Ländern unterschiedliche Prüfungszeiträume

[540] CoE, Explanatory Report, ETS No. 181, Nr. 33.

bestehen, aus welchem Grund eine Überprüfung zumindest vor einer Übermittlung stattzufinden hat. Gerichtliche Entscheidungen bzw. Einstellungsverfügungen sind zu kennzeichnen und Daten, welche auf persönlichen Einschätzungen beruhen, sind nochmals zu überprüfen; deren Genauigkeit und Maß an Zuverlässigkeit sind anzugeben. Sollte entdeckt werden, dass die Daten nicht länger richtig bzw. nicht mehr aktuell sind, so sind die Daten nicht zu übermitteln. Sollte eine Übermittlung solcher Daten bereits stattgefunden haben, so sind die Empfänger der Daten darüber zu informieren, dass die Daten nicht richtig bzw. nicht aktuell sind.

Principle 12 der Rec. (92) 1 bestimmt generell nur, dass eine Übertragung der DNA-Analyse-Ergebnisse in ein anderes Land möglich ist, sofern die Bestimmungen der Rec. (92) 1, der DSK und weiterer internationaler Verträge bezüglich des Austauschs von Informationen in Strafsachen eingehalten werden. Ebenso sind die Bestimmungen, welche die Rec. (92) 1 an die untersuchenden Institutionen stellt, einzuhalten.

2. VERGLEICH DER MATERIELLEN DATENSCHUTZREGELUNGEN MIT DEM EPASS

a) ANWENDBARKEIT

Der ePass ist aufgrund seiner biometrischen Daten vom Anwendungsbereich der DSK erfasst. Denn sobald biometrische Daten gesammelt und automatisch verarbeitet werden, besteht die Möglichkeit, dass diese Daten einer bestimmten oder bestimmbaren Person zugeordnet werden können.[541] Durch die im ePass gespeicherten maschinenlesbaren Daten, welche ohne

[541] S. Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), Nr. 52.

großen Aufwand in Bezug zu den im Chip gespeicherten biometrischen Daten gesetzt werden können, ist eine Person zumindest bestimmbar; insbesondere weil statt Templates Bilddateien verwendet werden, ist ein Zusatzwissen vorhanden, welches den Personenbezug herstellt. Diese Bestimmbarkeit wird durch die automatisierte Verarbeitung erleichtert. Der Chip umfasst eine Gesamtheit von Informationen, welche er automatisiert verarbeitet, sobald ein Lesegerät in der Nähe ist; zudem wurden die Daten vor der Speicherung im Chip maschinell aufbereitet und somit einer automatischen Verarbeitung zugänglich gemacht.

Der Verantwortliche ist entsprechend Art. 2 lit. d) DSK derjenige, der für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist. Dies kann zum einen die ausstellende Behörde sein, da diese neben den Exekutivbehörden alleinigen Zugang zu den Daten hat und diese verändern kann; zum anderen können es aber auch der Gesetzgeber, da dieser die Zwecke, die Datenkategorien und deren Nutzung festlegt, oder das Innenministerium sein.[542] Gesetzlich wurde keine Verantwortlichkeit festgelegt. Allerdings wird man wohl eine gespaltene Zuständigkeit annehmen müssen. Es spricht nicht nur der Wortlaut dafür, dass der Hauptverantwortliche das jeweilige Innenministerium ist, da ansonsten zu viele verantwortliche Behörden existieren würden, was möglicherweise Zuständigkeitsstreitigkeiten in Bezug auf die Örtlichkeit hervorrufen könnte. Des Weiteren befolgen die unteren Behörden nur Weisungen. Die Verwaltungsvorschriften werden ebenfalls vom Innenministerium gemacht. Allerdings kann auch festgelegt werden, dass die sachnähere und damit die ausstellende Behörde dem Betroffenen bei der Durchsetzung seiner Rechte helfen soll.

[542] S. Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), Nr. 53.

Dies kann durch Weisung oder durch Gesetz geschehen. In der BRD sind die ausstellenden Behörden diejenigen, welche dem Betroffenen Auskunft gewähren, Berichtigungen und Löschungen vornehmen (vgl. Allgemeine Verwaltungsvorschrift zur Durchführung des Passgesetzes vom 17.12.2009).

b) RECHTMÄSSIGKEIT DER DATENBESCHAFFUNG UND -VERARBEITUNG

Nachdem also festgestellt wurde, dass der ePass vom Anwendungsbereich der DSK erfasst ist, hat er auch die Anforderungen an die Qualität der Daten zu erfüllen. Gemäß Art. 5 lit. a) DSK sind die Daten rechtmäßig zu beschaffen und zu verarbeiten. Der Bürger sollte zugestimmt oder zumindest Kenntnis von der Erhebung seiner Daten haben. Dies geschieht beim ePass durch die Beantragung desselben. Insbesondere basiert die Erhebung der Daten auf einer gesetzlichen Grundlage, nämlich der ePass-Verordnung i.V.m. den nationalen Gesetzen. Natürlich kann die Herausgabe der Daten auch freiwillig geschehen. Es stellt sich hier nur die Frage, ob die Herausgabe denn freiwillig erfolgt. Der Beantragende wird schließlich gesetzlich hierzu verpflichtet, einen ePass zu beantragen, sofern er in ein Drittland reist; andernfalls reicht bereits ein Personalausweis aus. Allerdings könnte er hierauf auch verzichten, indem er auf sein Recht auf Freizügigkeit verzichtet. Allerdings wird man dann die Beantragung eines ePasses nicht als freiwillig bezeichnen können, sondern als zwingende gesetzliche Voraussetzung für den Grenzübertritt, welche nicht auf der eigenen Entscheidung des Betroffenen beruht. Freiwilligkeit wird daher in aller Regel nicht gegeben sein. Des Weiteren sind die Daten auf rechtmäßige Art und Weise zu verarbeiten, d.h. auch hier sollte der Betroffene Kenntnis von der Verarbeitung haben. Der ePass ist

sicherheitstechnisch so konzipiert, dass der Passinhaber diesen der Behörde bzw. dem Beamten vorlegen muss. Erst dann können die maschinenlesbaren Daten abgerufen werden, aus welchen dann der Schlüssel zum Auslesen der biometrischen Daten erstellt wird. Der Betroffene hat es damit also in der Hand, wem und wann er den Pass vorlegt, d.h. er weiß in der Regel auch darüber Bescheid. Zwar gibt es bereits Bedenken, dass der Pass aus größeren Entfernungen ausgelesen werden kann. Dies ist jedoch ein missbräuchliches Auslesen und bereits aus diesem Grund rechtswidrig, d.h. den befugten Behörden nicht gestattet. Sicherheitstechnisch ist dies ein Problem, welches bei Art. 7 DSK zu verorten ist. Des Weiteren muss die Vorlage eines Dokuments gesetzlich vorgeschrieben sein, vgl. Art. 4 III Pass-Verordnung, d.h. die Vorlage erfolgt nicht im Ermessen des Beamten, sondern ist gesetzlich bestimmt und erfolgt damit auf rechtmäßige Art und Weise.

c) SPEICHERUNG ZU FESTGELEGTEN ZWECKEN UND ZWECKBINDUNG

Nach Art. 5 lit. b) DSK sind die Daten zu festgelegten und rechtmäßigen Zwecken zu speichern und dürfen nur zu diesen Zwecken verwendet werden. Die biometrischen Daten werden gem. Art. 4 III Pass-Verordnung nur verwendet, um die Authentizität des Passes und die Identität des Inhabers zu prüfen. Dies dient wiederum der Aufdeckung und Festnahme von Personen, die ein gefälschtes oder verfälschtes Dokument verwenden und in Folge dessen auch verdächtig sind, weitere Straftaten zu begehen. Allerdings ist es gem. Art. 4 III Pass-Verordnung UAbs. 2 auch erlaubt, zusätzliche Sicherheitsmerkmale nach Art. 7 II Schengener Grenzkodex zu überprüfen, d.h. die Gültigkeit des ePasses, ob Fälschungsmerkmale vorliegen und ob Einträge in der Datenbank für abhanden gekommene, gestohlene, für ungültig erklärte und

missbräuchlich verwendete Dokumente vorhanden sind. Ferner besteht auch die Möglichkeit eines Abgleichs der Seriennummer mit polizeilichen Datenbanken, sofern eine tatsächliche, erhebliche und gegenwärtige Gefahr angenommen wird. Dies wird gerade angenommen, wenn ein Ausweis gefälscht oder verfälscht ist, was Anlass zu weiteren Maßnahmen bietet, die jedoch noch vom Zweck des Art. 4 III Pass-Verordnung gedeckt sind. Es erfolgt in der Datenbank jedoch keine 1:n-Identifikation anhand biometrischer Merkmale, sondern es wird vielmehr ein Abgleich anhand der Seriennummer des Dokuments vorgenommen. Die letztgenannten Zwecke sind außerdem durch die Änderung der Pass-Verordnung gesetzlich festgelegt worden. Eine Änderung dieser Zwecke findet nicht statt. Da die Überprüfung zur Aufdeckung von Straftaten sowie zur Erhaltung der nationalen Sicherheit erfolgt, liegen auch rechtmäßige Zwecke für die Überprüfung vor. Außer Acht gelassen werden darf außerdem nicht, dass entsprechend den Zwecken der Identifizierung des Passinhabers sowie der Überprüfung der Echtheit des Ausweises nur eine Verifikation erforderlich ist. Genau diese wird beim ePass auch nur durchgeführt. Ein Passregister zur Identifikation wäre nicht gerechtfertigt.

d) INHALTLICHE QUALITÄT DER DATEN

Nach Art. 5 lit. c) DSK müssen die Daten dem Speicherzweck entsprechen, „dafür erheblich sein und dürfen nicht darüber hinausgehen“. Tatsächlich war bereits die alte Version des deutschen Reisepasses sehr fälschungssicher. Angesichts der technischen Entwicklungen ist es keine Frage, dass sich die Technologie dem Lauf der Zeit anpassen muss; ebenso wie sich das Verbrechertum neuer Technologien bedient, müssen auch die Behörden sich dem Fortschritt anpassen, um nicht hinterherzuhinken. Aus diesem Grund ist es auch sinnvoll gewesen, den ePass mit biometrischen Merkmalen auszustatten.

Theoretisch wäre zur Verbesserung der Fälschungssicherheit des ePasses aber nur ein biometrisches Merkmal erforderlich gewesen. Fraglich ist daher zunächst, ob überhaupt zwei biometrische Merkmale für den ePass erforderlich waren. Es kann durchaus sein, dass das biometrische Foto aufgrund von Nichtlesbarkeit, Defekt, falschem Lichteinfall oder sonstigen technischen Problemen keine Übereinstimmung mit dem Passinhaber anzeigt, weswegen es durchaus in dessen Interesse ist, ein zweites biometrisches Merkmal zur Verfügung zu haben, welches ihn verifiziert, anstatt einer Einzelkontrolle ausgesetzt zu sein. Ein zweites Merkmal ist daher durchaus auch im Interesse des Betroffenen und gerechtfertigt, zumal dadurch auch der Schutz vor Missbrauch eines fremden Ausweises erhöht wird. Für den Abgleich mit polizeilichen Fahndungsdatenbanken nach Art. 7 II Schengener Grenzkodex hingegen sind keine biometrischen Daten erforderlich, weswegen hier auch nur ein Abgleich über die Seriennummer des Passes erfolgt. Des Weiteren wurde in Art. 1 I Pass-Verordnung die Vorgabe „1 Person – 1 Pass“ eingeführt. Diese Einführung gilt für Familien mit Kindern, wonach bereits Kinder einen eigenen Reisepass vorweisen müssen. Früher wurden nur die Namen der Kinder ohne biometrisches Foto in den Pass der Eltern eingetragen, was zur Folge hatte, dass die Identität des Kindes nicht überprüft werden konnte. Die neue Vorgabe soll gleichzeitig den Kinderhandel bekämpfen und ist daher gerechtfertigt.[543]

Ferner stellt sich im Rahmen dieser Vorschrift die Frage, ob man sich anstatt einer Bilddatei, wie sie sowohl beim Gesichtsbild als auch beim Fingerabdruck derzeit verwendet wird[544], nicht eines Templates bedienen sollte. Templates haben nicht nur den Vorteil einer geringeren Speicherkapazität, sondern verraten auch keine

[543] Vgl. hierzu Vorschlag für eine Verordnung des Europäischen Parlaments zur Änderung der Verordnung (EG) Nr. 2252/2004, KOM (2007) 619 endgültig, S. 3.
[544] Vgl. Entscheidung der Kommission C (2006) 2909, Punkt 2.1.3 und 2.2.3.

überschüssigen Informationen wie bspw. medizinische Daten, wohingegen man einer Bilddatei durchaus verschiedene Informationen entnehmen kann. Ein weiterer Vorteil von Templates ist, dass das Originalbild des biometrischen Merkmals nicht mehr wiederhergestellt werden kann.[545] Durch die Verwendung der Bilddatei werden mehr Daten verarbeitet, als für die Zwecke des ePasses erforderlich. Leider gibt es jedoch noch keine interoperablen Standards für Templates, da die Biometrie sich erst in einem Anfangsstadium befindet. Aus diesem Grunde können derzeit in den Mitgliedstaaten und Drittstaaten nur Bilddateien verwendet werden. Es stellt sich daher die Frage, ob der Betroffene dies hinnehmen muss. Beim Gesichtsbild ist jedoch Folgendes zu beachten: Der ePass enthält aufgrund seines Ausweischarakters bereits ein Bild zur Identifizierung der Person, ohne dass es sich um ein biometrisches Bild handeln muss, d.h. Informationen sind bereits hieraus erkennbar. Hinsichtlich der Fingerabdruckdaten bleibt es jedoch dabei, dass eine Bilddatei zu viele überschüssige Informationen enthält, welche nicht erforderlich sind[546], insbesondere gibt es hierbei bereits Templateverfahren (s. Teil B Pkt. C. und Teil C Pkt. A. II. 2.), welche durchaus international angewandt werden könnten. Der ePass entspricht daher nicht Art. 5 lit. c) DSK.

Überdies sind die Voraussetzungen des Art. 5 lit. d) DSK zu erfüllen, wonach die Daten sachlich richtig und auf neuestem Stand sein müssen. Problematisch ist zum einen die lange Geltungsdauer der Pässe von zehn Jahren. Es ist anerkannt, dass sich Gesichtsbilder und Fingerabdrücke im Laufe der Zeit durch Abnutzung, Alterung, etc. verändern, weswegen eine solch lange Gültigkeitsdauer dazu führt, dass die Aktualität der Daten sinkt

[545] S. Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), Nr. 65.
[546] S. auch Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), Nr. 43.

und die Falschzurückweisungsrate ansteigt. Allerdings wird man gerade aufgrund der Kosten eines solchen ePasses keine kürzere Dauer in Betracht ziehen können. Zehn Jahre sind noch vertretbar, einerseits in Bezug auf die Kosten und andererseits in Bezug auf die Erkennungsleistung. Sollte sich dennoch ein Merkmal derart gravierend verändern, dass die Erkennungsleistung nicht mehr gewährleistet ist, gibt es noch ein zweites Merkmal (dies bestätigt wiederum die Zweckmäßigkeit der beiden Merkmale) und außerdem die Möglichkeit der Neuausstellung, deren Kosten dann aber die beantragende Person zu tragen hat.

Die Daten müssen zum anderen sachlich richtig sein. Der europäische Datenschutzbeauftragte hat hierbei in seiner Stellungnahme vom 26.03.08 bemängelt, dass es in den EU-Mitgliedstaaten erhebliche Unterschiede bei der Beantragung des Passes hinsichtlich der vorzulegenden Dokumente gibt und dass diese Dokumente, seien es Geburtsurkunde, Familienstammbuch etc., nicht nur gefälscht und verfälscht werden, sondern auch eine andere Person ausweisen könnten. Der europäische Datenschutzbeauftragte weist daher zu Recht darauf hin, dass der ePass nur so sicher sein kann, wie das schwächste Glied in der Kette der Dokumente.[547] Die Daten sind daher nicht unbedingt sachlich richtig. Es ist jedoch Sache der Mitgliedstaaten, dies durch geeignete Verfahren sicherzustellen.

„Sachlich richtig“ bedeutet im weitesten Sinne auch, dass die Daten sachlich richtig aufgezeichnet werden müssen. Für den Fingerabdruck muss daher eine vollständige Aufzeichnung der Fingerkuppe vorgenommen werden, damit genügend Minutien zum Abgleich zur Verfügung stehen. Nach Art. 1 II ePass-Verordnung i.V.m. Pkt. 2.2.2 der Kommissionsentscheidung C

[547] Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für eine Verordnung zur Änderung der ePass-Verordnung vom 26.03.2008, ABl. C 200 vom 06.08.2008, S. 1 ff., Nr. 24 ff.

(2006) 2909 sind die Finger des rechten und des linken Zeigefingers auf den Sensor flach aufzulegen. In Deutschland wird dies jeweils dreimal vorgenommen, wobei sich die Software dann das am besten geeignete Bild heraussucht.[548] Dies bedeutet erhebliche Sicherheit dafür, dass die Daten dann auch tatsächlich richtig gespeichert werden. Ist die Qualität des Fingerabdrucks ungenügend oder sind Verletzungen vorhanden, so sind gem. Pkt. 2.2.2 der Kommissionsentscheidung C (2006) 2909 andere Finger für den Abdruck heranzuziehen. Ist auch dies nicht möglich, ist entsprechend dem Befreiungstatbestand des Art. 1 II lit. b) der ePass-Verordnung ein provisorischer Pass auszustellen. So wird für alle Mitgliedstaaten sichergestellt, dass die gleiche Qualität hinsichtlich der Daten vorhanden ist. Dies wird dadurch bekräftigt, dass die Fingerabdrücke dem ISO-Standard für Fingerabdruckbilder genügen müssen. In Deutschland werden im Chip zudem noch die Qualitätswerte gespeichert sowie ggf., welcher Finger bzw. dass nur ein oder gar kein Finger aufgenommen wurde.[549]

Die Richtigkeit des Fingerabdrucks kann ferner durch Schweiß, Verbrennungen, Vernarbungen, schwach ausgeprägte Minutien etc. (s. Teil B Pkt. C.) beeinträchtigt werden. Dies wird jedoch gleich bei der erstmaligen Erfassung des Fingerabdrucks vom System erkannt, weswegen man diesem Problem sofort begegnen kann.

Das Lichtbild muss gem. Pkt. 2.1.2 der Kommissionsentscheidung C (2006) 2909 das Gesicht von vorne zeigen. Ferner sind gem. Pkt. 2.1.5 bei der Bildaufnahme die Leitlinien der ICAO zu beachten. Auch hier sind damit einheitliche Vorgaben für alle

[548] S. unter www.bmi.bund.de unter „Elektronischer Reisepass", „Besonderheiten bei der Aufnahme von Passfoto und Fingerabdrücken für den Reisepass".
[549] S. unter www.bmi.bund.de unter „Elektronischer Reisepass", „Besonderheiten bei der Aufnahme von Passfoto und Fingerabdrücken für den Reisepass".

Mitgliedstaaten vorhanden. Die Richtigkeit des Lichtbildes kann jedoch durch Veränderungen im Alter, Mimik, Brille, Lichteinfall etc. (s. Kapitel 1) beeinträchtigt werden. Gerade aus diesem Grund wurde die Gültigkeitsdauer des ePasses nur auf zehn Jahre angesetzt. Ferner haben die Lichtbilder besonders im Hinblick auf Lichteinfall, Brille und Mimik bestimmte Anforderungen zu erfüllen.

e) AUFBEWAHRUNG DER DATEN

Nach Art. 5 lit. e) DSK müssen die Daten „so aufbewahrt werden, dass der Betroffene nicht länger identifiziert werden kann, als es die Zwecke, für die sie gespeichert sind, erfordern". Dies wird beim ePass durch den RFID-Chip sichergestellt, durch den die Verifikation nur so lange möglich ist, wie der Chip Kontakt zum Lesegerät hat. Danach ist ein Auslesen nicht mehr möglich. Es wird seit langem bemängelt, dass ein Auslesen mittlerweile auch über mindestens 50 cm Entfernung möglich sei.[550] Zwar soll hiervor der Basic Access Control (BAC) schützen, jedoch ist es bereits gelungen, die auf dem Pass vorhandenen Daten auszulesen, wenn die in der maschinenlesbaren Zone gespeicherten Daten bekannt sind. Den Fingerabdrücken wird mehr Schutz durch den Extended Access Control (EAC) beigemessen, wonach zum Auslesen mathematische Verfahren verwendet werden, die nur den hierzu befugten Staaten bekannt sind. Damit wird zumindest ein Auslesen von Unbefugten verhindert. Letztlich sind jedoch kein ausreichender Schutz vor dem Auslesen des Lichtbildes und kein Schutz vor Missbrauch vorhanden. Diesem kann nur begegnet werden, wenn man einen sog. Faradayschen Käfig verwendet.[551]

---

[550] Meints, in: DuD 31/2007, 189 (192).

[551] s. Pressemitteilung des ULD Schleswig-Holstein vom 31.10.2007, „Ein Faradayscher Käfig für die Jacken- und Handtasche – Hansestadt Lübeck und Experten des Unabhängigen Landeszentrums für Datenschutz empfehlen Alu-Hüllen zum Schutz elektronischer Passdaten", einsehbar unter https://www.datenschutzzentrum.de/presse/20071031-epass-schutzhuelle.htm.

Dieser sollte eigentlich bereits vom Staat in den ePass eingebaut werden. Allerdings kann der Einzelne sich mit einer einfachen Alufolie, welche er um den ePass wickelt, behelfen. Ein weiteres Problem stellt sich hinsichtlich der Daten, die bei der Beantragung des ePasses den Behörden bekanntgegeben worden sind. In der ePass-Verordnung ist hierzu nichts geregelt. Dies ist vielmehr den Staaten überlassen. Deutschland hat dafür ein gesetzliches Verbot der Speicherung der Fingerabdruckdaten im Passregister eingeführt, d.h. die Fingerabdruckdaten müssen unmittelbar nach Ausgabe des ePasses gelöscht werden. Die anderen Daten werden im Passregister gespeichert. In anderen Staaten hingegen werden sämtliche Daten in Passregistern gespeichert. Es wurde bereits auch diskutiert, ein europäisches Passregister einzuführen, was ebenfalls die Speicherung der biometrischen Merkmale zur Folge hätte[552], bislang jedoch verworfen wurde. Fraglich ist allerdings, ob die Speicherung so vieler Daten erforderlich ist. Zur Erfüllung der in Art. 4 III der ePass-Verordnung genannten Zwecke reicht die Verifikation der Daten und damit eine dezentralisierte Speicherung der Daten im Chip aus. Alles andere verstößt gegen Art. 5 lit. e) DSK. Eine Ausnahme ist nur dann zulässig, wenn ein hinreichender Verdacht für einen Identitätsschwindel bestehen würde. Ein solcher liegt jedoch nicht bei jedem Passantragsteller vor. Überdies würde eine weitergehende Speicherung auch bedingen, dass die gespeicherten Daten verwendet werden. In Deutschland hat bspw. die Polizei Zugriff auf die bei den Meldebehörden gespeicherten Daten, also auch auf das Lichtbild. Der Zugriff auf das Lichtbild dient dann bspw. zur Identifizierung von Straftätern anhand der Gesichtserkennung. Dies ist aber ein anderer Zweck als diejenigen, welche von Art. 4 III ePass-Verordnung genannt werden, insbesondere dient eine solche

[552] vgl. Vorschlag der Kommission der Europäischen Gemeinschaften für eine Verordnung des Rates über Normen für Sicherheitsmerkmale und Biometrie in Pässen der EU-Bürger vom 18.02.2004, KOM (2004) 116 endg., S. 4.

Identifizierung u.a. der Aufklärung anderer Straftaten als der von Urkundendelikten oder Delikten gegen die nationale Sicherheit. Damit steht auch eine Verletzung des Art. 5 lit. b) DSK im Raum.

f) SENSIBLE DATEN

Art. 6 DSK sieht einen höheren Schutz für sensible Daten vor. Die biometrischen Daten enthalten nebenbei auch überschüssige Informationen wie bspw. medizinische Daten (s. Teil B Pkt. A. I., B. II. und C. II). Des Weiteren enthalten biometrische Lichtbilder Daten über die ethnische Herkunft und die Religionszugehörigkeit, indem man die Hautfarbe, das Haar bzw. ein Kopftuch erkennen kann. Für die Verifikation sind diese Daten irrelevant und werden nicht gebraucht. Im Übrigen sind sie nur Nebenprodukt des biometrischen Merkmals und werden nur dann im Besonderen registriert, wenn man es darauf abgesehen hat; die sensiblen Daten sind für die Zwecke der Überprüfung des Ausweises nicht relevant. Aus diesem Grund ist für diese Daten nur ein geringfügig besserer Schutz als für die restlichen Daten erforderlich. Zum einen wird dies bei den Fingerabdrücken durch den Extended Access Control gewahrt, indem Zugriffsrechte beschränkt werden, und zum anderen sind die Befugnisse der Behörden durch die festgelegten Zwecke stark eingeschränkt. Auch wenn man vielleicht anhand schwach ausgeprägter Minutien einen Asiaten oder hart arbeitenden Senioren erkennen könnte, so fällt diese Erkenntnis nicht erst mit der Überprüfung der Fingerabdrücke. Lediglich das Foto enthält zu viele Informationen, denen auch nicht durch die Verwendung eines Templates begegnet werden kann, da das Lichtbild immer auf dem Ausweis zu sehen sein wird. Allerdings begibt sich der Passinhaber mit seinem Gesicht auch in die Öffentlichkeit, d.h. bereits aufgrund seines öffentlichen Auftretens kann ein öffentlich zur Schau gestelltes biometrisches Merkmal wie das Gesicht mit allen seinen sensiblen Daten zur Kenntnis genommen werden. Ein solches Merkmal

bleibt auch im privaten Umgang mit anderen Menschen nicht verborgen und rechtfertigt daher nicht die besonders strengen Regelungen des Art. 6 DSK. Man könnte wiederum darüber diskutieren, dass ein Foto aufgrund der dauerhaften Aufzeichnung möglicherweise mehr Spielraum für eine genaue Profilanalyse lässt als ein sich bewegender Mensch; doch auch dies ist diskutabel. Zudem verbleibt der Ausweis nur kurz beim prüfenden Beamten, so dass dieser keinesfalls eine vollständige medizinische oder ethnische Analyse vornehmen kann.

g) DATENSICHERUNG

Nach Art. 7 DSK sind die Daten gegen Zerstörung, zufälligen Verlust, unbefugten Zugang, unbefugte Veränderungen und unbefugte Bekanntgabe zu schützen. Während der Grund für die letzteren drei selbsterklärend ist, so stellt sich hinsichtlich des Schutzes gegen Zerstörung und gegen zufälligen Verlust die Frage, inwiefern dies dem Betroffenen nützlich sein soll. Dabei ist zu bedenken, dass der Betroffene bei Zerstörung oder Verlust des ePasses bzw. der Daten einen neuen ePass beantragen muss und damit die Kosten zu tragen hat. Des Weiteren wird der Betroffene in einem solchen Fall mit zusätzlichen Überprüfungsmaßnahmen an der Grenze zu rechnen haben, die sich dann nach dem Recht des Einreiselandes richtet. Auch könnten dahingehende Bedenken aufkommen, dass jemand die Möglichkeit hatte, die Daten zu zerstören, indem er sich unbefugt Zugang zu den Daten verschafft hat. Dem Passinhaber wird also daran gelegen sein, dass die Daten nicht zerstört oder verlustig werden. Aufgrund des Charakters der biometrischen als personenbezogene Daten, welche der Mensch nur einmal besitzt, sind hinsichtlich des ePasses Schutzvorkehrungen zu treffen. Diese können physischer, organisatorischer oder technischer Natur sein. Der Hersteller hat hierfür Vorkehrungen zu treffen. Ein „zufälliger Verlust“ der Daten ist nicht möglich. Allerdings sind Schutzvorkehrungen gegen

„unbefugten Zugang“ zu treffen. Mit dem Basic Access Control, welcher das Abhören der Kommunikation zwischen dem Chip und dem Lesegerät verhindert, soll ein Zugriff durch Nichtberechtigte verhindert werden. Die gleiche Funktion hat der Extended Access Control, welcher vor einem Zugriff auf die Fingerabdrücke schützen soll. Letzterer ist durch mathematische Verfahren abgesichert, welche nur die Staaten erhalten sollen, die zum Auslesen befugt sind. Beim Basic Access Control hingegen reichen zum Auslesen die in der maschinenlesbaren Zone verfügbaren Daten aus, weswegen man auf das Gesichtsbild bereits zugreifen konnte. Ein besserer Schutz könnte dann gewährleistet werden, wenn der Einzelne über ein Passwort verfügen würde, welches er vor jedem Auslesen zuerst eingeben muss, bevor der Zugriff auf seine Daten gestattet würde. Auch bestehen aufgrund dessen, dass der RFID-Chip kontaktlos ausgelesen werden kann, erhebliche Bedenken. Ein Auslesen ist – wie bereits gesagt – bereits aus 50 cm (bei herkömmlichen RFID-Chips z.T. sogar noch größerer) Entfernung möglich. Diesem kann man bspw. durch einen Faradayschen Käfig oder – wie bereits angesprochen – durch ein Passwort begegnen (vgl. oben). Hierzu gehört aber auch, dass der Passinhaber über den ePass und die technischen Gegebenheiten informiert wird. Er sollte auch darüber informiert werden, was bei Verlust passieren kann. Der Passinhaber sollte in einem solchen Fall sofort Kontakt mit der Behörde aufnehmen, welche dann die Polizeibehörden informieren kann; diese werden die entsprechenden Informationen wie die Seriennummer des Passes etc. in ihren Datenbanken speichern, damit diese beim nächsten Abgleich gem. Art. 4 III ePass-Verordnung i.V.m. Art. 7 II Schengener Grenzkodex in der Sachfahndung gespeichert sind. Weiterer Schutz vor unberechtigtem Zugriff wird dadurch sichergestellt, dass nur die exekutiven Behörden, die ausstellenden Behörden sowie eine Druckerei (vgl. Art. 3 III ePass-Verordnung) Zugriff auf die Daten haben. Auch ist fraglich, ob der ePass

ausreichend gegen „unbefugte Veränderung“ geschützt ist. Es besteht zwar mit der Passive Authentification eine Sicherung, welche Veränderungen oder Verfälschungen der Daten erkennen könne. Allerdings hat man bereits erfolgreich einen Chip kopieren können (s. hierzu Teil C Pkt. A. III.). Hierbei schafft jedoch die freiwillige Active Authentification bzw. die vorgeschriebene Chip-Authentifizierung Abhilfe, welche erkennen kann, ob der originale Chip vorhanden ist. Weitere Angriffsmöglichkeiten bestehen zum einen durch Brute-Force-Attacken, d.h. indem mehrere Daten, bspw. zehn Finger, in das System eingespielt werden, um die Chance der Erkennung eines Fingers zu erhöhen. Zum anderen gibt es Relay-Attacken, bei denen das Sensorsignal abgegriffen und bei Bedarf wieder eingespielt wird. Ferner könnten künstliche oder tote Finger zur Erkennung verwendet werden, ebenso wie unter Zwang gesetzte oder bewusstlose Personen. Die letzten beiden eignen sich im Übrigen auch für die Gesichtserkennung, ebenso wie ein vorgehaltenes Foto. Diesen Problemen könnte man jedoch mit Lebenderkennung oder – einfacher – mit geschultem und anwesendem Personal begegnen. Auch sind regelmäßige Checks des Systems dringend erforderlich, um eventuelle Fehler auszubessern bzw. Angriffe auf das System zu erkennen. Eine „unbefugte Bekanntgabe“ der Daten kann nicht erfolgen, da der Passinhaber im Besitz des ePasses ist und daher die Verfügungsgewalt über die Daten hat. Art. 1 I der ePass-Verordnung i.V.m. dem Anhang zu den Mindestsicherheitsnormen legen weitere physische Maßnahmen fest, die bei der Herstellung des ePasses zu beachten sind. Im Großen und Ganzen sind einige Maßnahmen zur Datensicherheit getroffen worden, welche jedoch nicht ganz ausreichen, um einen angemessenen Schutz zu gewährleisten.

h) EINSCHRÄNKUNGEN UND AUSNAHMEN NACH ART. 9 I, II DSK

Art. 9 DSK lässt gewisse Ausnahmen von Art. 5, 6 und 8 DSK zu. Gerade in Bezug auf Art. 5 DSK bestehen erhebliche Bedenken (s. oben). Es ist daher fraglich, ob ein Passregister zulässig ist bzw. ob von den Voraussetzungen des Art. 5 DSK, bspw. hinsichtlich der Verwendung von Templates zur Vermeidung überschüssiger Informationen, abgewichen werden kann. Ein Passregister kann durchaus zur Bekämpfung von Straftaten erforderlich sein (s. oben in Bezug auf die Führung von Lichtbildern in den Melderegistern). Auch mag ein solches Passregister dem Schutz der nationalen Sicherheit dienen, indem die Daten abgeglichen werden können. Nicht gerechtfertigt ist allerdings die Verwendung überschüssiger Informationen. Auch die fehlende Überprüfung von Dokumenten vor der Ausstellung des ePasses ist nicht mit einem Verweis auf Art. 9 DSK zu rechtfertigen, da eine solche Überprüfung letztlich auch dem Schutz der öffentlichen Ordnung dient. Gleiches gilt für den Schutz der Daten vor unbefugtem Auslesen in Bezug auf Art. 5 lit. e) DSK, wenn es darum geht, dass Daten nicht länger aufbewahrt werden sollen, als es die Zwecke erfordern. Es dient nämlich letztlich dem Schutz des Betroffenen und damit einem der legitimen Zwecke des Art. 9 II DSK, wenn ein solcher Schutz gewährleistet wird.

i) GRENZÜBERSCHREITENDER DATENSCHUTZ

Art. 12 DSK ist nicht anwendbar, da kein staatenübergreifender Datenverkehr stattfindet. Der ePass wird zwar beim Grenzübertritt verwendet. Allerdings werden die Daten nicht von Behörden staatenübergreifend verarbeitet, d.h. es findet kein automatischer Datenaustausch statt, welcher die Regelungen des Art. 12 DSK zur Anwendung bringen könnte.

3. VERGLEICH DER MATERIELLEN DATENSCHUTZREGELUNGEN MIT DEM PRÜMER RATSBESCHLUSS

a) ANWENDBARKEIT

Der Anwendungsbereich der DSK ist eröffnet, da der Prümer Ratsbeschluss den automatisierten Austausch personenbezogener Daten regelt. Sobald biometrische Daten unter der Prämisse gesammelt werden, diese später automatisiert zu verarbeiten, besteht die Möglichkeit, dass diese Daten einer bestimmten oder bestimmbaren Person zugeordnet werden können.[553] Es handelt sich hierbei insbesondere um eine automatische Verarbeitung, da die biometrischen Daten maschinell aufbereitet bzw. die Daten in eine Datei eingegeben werden. So werden die daktyloskopischen Daten als Bilddatei gespeichert und anschließend durch eine Software aufbereitet, indem die Minutien hervorgehoben und deren Vektoren ebenfalls gespeichert werden; sowohl das Template als auch die Bilddatei stehen im Anschluss einem automatisierten Abgleich zur Verfügung. Ebenso werden die DNA-Identifizierungsmuster in die DNA-Datei eingegeben und stehen anschließend ebenfalls zum Abgleich bereit. Dass nach dem Prümer Ratsbeschluss eine automatische Verarbeitung stattfindet, zeigt letztlich auch Art. 24 I lit. b), worin der „automatisierte Abruf" definiert wird. Bei den Dateien handelt es sich um automatisierte Dateien. Die Informationen sind zwar nicht in einer Datei gespeichert, die Dateien werden jedoch zur Verarbeitung der Daten vernetzt.

Verantwortlicher der Dateien ist derjenige, der die Zwecke, die Datenkategorien sowie deren Nutzung festlegt. Dies ist eigentlich der Gesetzgeber. Allerdings hat dieser keinen Zugang zu den

[553] Progress Report on the application of the principles of Convention 108 to the collection and processing of biometric data (2005), Nr. 52.

Dateien. Aus diesem Grund wird man die nationalen Kontrollstellen gem. Art. 6 und 11 als die Verantwortlichen (aufgrund entsprechender Weisung) ansehen müssen. In Deutschland wäre dies das Bundeskriminalamt; dies ist in Deutschland für Verbunddateien in Art. 14 VII BKAG ausdrücklich niedergelegt. Für die Ordnungsmäßigkeit der Datenerhebung ist der Eingebende verantwortlich, wohingegen für die Zulässigkeit des Abrufs der Daten der Empfänger verantwortlich ist. Eine andere Regelung ist bei Datenabgleichen in automatisierten Datennetzen nicht zweckmäßig.

Des Weiteren handelt es sich bei den Daten, welche nach dem Prümer Ratsbeschluss ausgetauscht werden, um polizeiliche Daten gem. der Rec. (87) 15, welche zur Verfolgung und Verhütung von Straftaten verwendet werden.

b) RECHTMÄSSIGKEIT DER DATENBESCHAFFUNG UND -VERARBEITUNG

Nach Art. 5 lit. a) DSK müssen die Daten auf rechtmäßige Art und Weise beschafft und verarbeitet werden, d.h. der Betroffene soll Kenntnis von der Verarbeitung haben und es muss eine Rechtsgrundlage vorhanden sein. In Bezug auf die Errichtung einer DNA-Datei findet sich die Rechtsgrundlage in Art. 2 I Prümer Ratsbeschluss in Verbindung mit dem nationalen Recht und in Bezug auf die Errichtung einer Fingerabdruckdatei in Art. 8 Prümer Ratsbeschluss. Da das Bestehen allein noch keinen Eingriff bedeutet, ist hierfür auch keine Kenntnis des Betroffenen notwendig. Kenntnis ist erst ab dem Zeitpunkt notwendig, zu dem seine Daten erhoben werden. Der automatisierte Abruf der Daten stellt ebenfalls einen Eingriff dar. Rechtsgrundlage hierfür ist hinsichtlich des Abrufs von DNA-Profilen Art. 2 I, 3 I Prümer Ratsbeschluss i.V.m. nationalem Recht und für den Abgleich von Spuren-DNA Art. 2 I, 4 I Prümer Ratsbeschluss i.V.m. nationalem

Recht. Bei den Fingerabdruckspuren wird gem. Art. 8, 9 I Prümer Ratsbeschluss i.V.m. nationalem Recht Zugriff auf die Fundstellendatensätze zum Zwecke des Vergleichs gewährt. Wird aufgrund des automatisierten Abgleichs eine Übereinstimmung festgestellt, so richtet sich die Übermittlung der Fundstellendatensätze bei den DNA-Profilen nach Art. 2 I, 3 II Prümer Ratsbeschluss, bei der Spuren-DNA nach Art. 2 I, 4 II Prümer Ratsbeschluss. Da bei den daktyloskopischen Daten keine so eindeutige Zuordnung wie bei den DNA-Daten möglich ist, erfolgt die Übermittlung der Fundstellendatensätze hier gem. Art. 8, 9 II Prümer Ratsbeschluss, nach dem der empfangende Staat die endgültige Zuordnung vornehmen muss, bevor er weitere Daten erhält, d.h. der empfangende Staat muss seine gesuchten daktyloskopischen Daten mit den gefundenen daktyloskopischen Daten durch einen Sachbearbeiter abgleichen lassen. Bislang wurden also nur die Fundstellendatensätze bestehend aus Kennung und DNA-Identifizierungsmuster bzw. daktyloskopischen Daten übermittelt; die Übermittlung weiterer personenbezogener Daten richtet sich dann nach Art. 5 und 10 Prümer Ratsbeschluss i.V.m. dem nationalen Recht und den Vorschriften über die Rechtshilfe des ersuchten Staates. Da die Herausgabe der Daten zwingend mit einem Kontrollverlust verbunden ist, ist es angemessen, die Daten erst nach und nach und auch nur im Falle einer Übereinstimmung herauszugeben. Von dem Abgleich und der möglichen Übermittlung weiterer Daten erhält der Betroffene erst im Laufe seiner Beschuldigtenvernehmung Kenntnis. Zu diesem Zeitpunkt hat die Kenntnisnahme auch spätestens zu erfolgen, damit das Recht auf ein faires Verfahren des Betroffenen nicht verletzt wird und Waffengleichheit gewährleistet ist. Erfolgt ein automatisierter Abgleich, ohne dass eine Übereinstimmung festgestellt wird, insbesondere bei den daktyloskopischen Daten, bei welchen meistens mehrere Fundstellendatensätze zum Zwecke des direkten

Vergleichs an den empfangenden Staat übermittelt werden, so erhält der hiervon Betroffene keine Kenntnis. Kenntnis erhält er erst im Rahmen eines Auskunftsersuchens. Allerdings würden in diesem Fall Mitteilungen an die Betroffenen die Strafverfolgungsbehörden in ihrer Arbeit erheblich bremsen, weshalb eine solche Einschränkung gerechtfertigt ist. Der Betroffene erhält jedoch von der Gewinnung molekulargenetischen Materials und der Übermittlung der daraus gewonnenen Profile Kenntnis. Gem. Art. 7 Prümer Ratsbeschluss hat ein Mitgliedstaat, in welchem sich eine gesuchte Person aufhält, Rechtshilfe zu leisten, indem er der betroffenen Person DNA entnimmt und diese untersuchen lässt sowie anschließend übermittelt. Die Rechtsgrundlage hierfür ist Art. 7 Prümer Ratsbeschluss i.V.m. dem nationalen Recht des abrufenden Staates und des ersuchten Staates. Fraglich ist, ob die DSK auch Anforderungen an die Rechtsgrundlage stellt, welche die Maßnahme erst rechtmäßig machen. Denn dann würde aufgrund lückenhafter Regelung im Prümer Ratsbeschluss, welcher keine Voraussetzungen für den Abruf/Abgleich bereitstellt, ein Verstoß gegen Art. 5 lit. a) DSK vorliegen. Da der Explanatory Report hierzu keine Ausführungen bereithält und wenn man den Grundgedanken der DSK bedenkt, nämlich die abstrakte Bereitstellung internationaler Regelungen, so ist wohl davon auszugehen, dass in der DSK keine Anforderungen an die Rechtsgrundlage gestellt wurden; es hat nur eine vorhanden zu sein.

In Konkretisierung des Art. 5 lit. a) DSK verlangt Principle 5.1 der Rec. R (87) 15 hinsichtlich der Zulässigkeit der Übermittlung, dass legitime Interessen für eine solche Übermittlung vorliegen und diese innerhalb der rechtlichen Befugnisse liegen. Das legitime Interesse der Verfolgung (und Verhinderung) von Straftaten wird in allen Rechtsgrundlagen genannt, d.h. in den Art. 2 I, 3 I, 4 I, 7, 8 und 9 I Prümer Ratsbeschluss. Die Verhinderung und Verfolgung

von Straftaten ist zudem Aufgabe der Polizeibehörden und liegt damit innerhalb der rechtlichen Befugnisse. Die weitere Verwendung im innerstaatlichen Bereich, d.h. die Weiterleitung der Ergebnisse an die Staatsanwaltschaft oder an das Gericht, wird im Prümer Ratsbeschluss nicht geregelt, d.h. diese Übermittlung erfolgt nach innerstaatlichem Recht. Nach Principle 5.1 i. der Rec. R (87) 15 muss bei einer Anfrage auf Übermittlung die ersuchende Behörde, der Grund der Übermittlung und der Zweck der Anfrage mitgeteilt werden. In Art. 7 Prümer Ratsbeschluss ist der Zweck der Übermittlung, nämlich die Übermittlung im Zuge eines laufenden Ermittlungs- oder Strafverfahrens, bereits festgelegt. Ebenso soll nach lit. a) der Zweck mitgeteilt werden. Da der abrufende Staat eine nach seinem Recht erforderliche Untersuchungsanordnung vorzulegen hat (Art. 7 lit. b), ist davon auszugehen, dass in dieser auch die ersuchende Behörde bezeichnet ist. Hinsichtlich der Übermittlung der Fundstellendatensätze wird ebenfalls der Zweck, nämlich die Verfolgung von Straftaten, bereits in der Vorschrift bezeichnet, vgl. Art. 3, 4 und 9 Prümer Ratsbeschluss. Der Grund muss nach den Vorschriften ebensowenig angegeben werden wie die ersuchende Behörde. Allerdings ergibt sich der Grund bereits aus der Vorschrift selbst, nämlich der Abgleich der DNA-Daten bzw. der Spuren-DNA bzw. der daktyloskopischen Daten. Die ersuchende Behörde wird automatisiert festgestellt. Diese erhält bei einer Übereinstimmung automatisierten Zugang zu den Daten. Zwar lässt sich durch eine solche Übermittlung nicht der Zweck des Principle 5.5 i. erreichen, nämlich die Sicherstellung, dass die Übermittlung zu Recht erfolgt ist. Dies ist durch den Prümer Ratsbeschluss aber auch gar nicht möglich und wird daher durch umfangreiche Protokollierungsmaßnahmen zum Ausgleich gebracht. Die Übermittlung weiterer personenbezogener Daten richtet sich nicht nach dem Ratsbeschluss, sondern nach dem innerstaatlichen Recht sowie den Vorschriften über die

Rechtshilfe, weswegen die Voraussetzungen des Principle 5.5 i. im nationalen Recht gegeben sein müssen, welches hier jedoch nicht Untersuchungsgegenstand ist. Art. 8 I des Durchführungsbeschlusses regelt die Anforderungen an die Anfrage hinsichtlich eines Vergleichs der Daten gem. Art. 3 und 4 Prümer Ratsbeschluss. Danach ergibt sich der anfragende Staat aus dem Mitgliedstaatencode. Principle 2.3 der Rec. R (87) 15 normiert die Zulässigkeit von Datensammlung, welche aus technischen Überwachungsmaßnahmen bzw. anderen automatischen Mitteln stammen. Die daktyloskopischen Daten sowie die DNA werden zwar mit technischen Mitteln aufbereitet, allerdings stammt die Sammlung nicht aus automatischen Mitteln, da die Daten durch einfache Blutabnahme bzw. Abnahme der daktyloskopischen Daten bzw. durch Sicherung von Spuren-DNA gesammelt werden. Eine Sammlung liegt auch nicht in der Bereitstellung der DNA-Datenbank. Dies ist begrifflich keine Sammlung, da die Daten nur zur Verfügung gestellt, aber nicht dem Empfänger zur eigenen Speicherung weitergegeben werden. Die Voraussetzungen des Principle 2.3 müssen daher nicht vorliegen.

Die Entnahme von DNA muss den Voraussetzungen des Principle 4 der Rec. (92) 1 entsprechen, wonach die Umstände durch innerstaatliches Recht festgelegt sein müssen, d.h. es sollte z.B. eine richterliche Genehmigung erfolgt sein. Ohne Einwilligung ist eine solche Entnahme nur zulässig, sofern die Umstände die Maßnahme rechtfertigen. Grundsätzlich wird die DNA nach innerstaatlichem Recht entnommen, es sei denn, es liegen die Gründe des Art. 7 Prümer Ratsbeschluss vor, wonach um Rechtshilfe für die Gewinnung, Untersuchung und Übermittlung von DNA-Profilen ersucht wird. In diesem Fall enthält Art. 7 weitere spezielle Voraussetzungen. Natürlich müssen auch die Voraussetzungen des innerstaatlichen Rechts gegeben sein, vgl. Art. 7 lit. b) und c). Art. 7 lit. b) verlangt sogar eine

Untersuchungsanordnung bzw. -erklärung, welche von einem Richter ausgestellt sein könnte bzw. zumindest von einem ähnlichen Organ, welches die Voraussetzungen für die Gewinnung geprüft hat. Eine Einwilligung des Betroffenen ist nicht erforderlich. Allerdings rechtfertigen die Umstände die Entnahme der DNA, da diese zur Verfolgung von Straftaten notwendig ist, mithin also eines gewichtigen Ausnahmetatbestandes nach Art. 9 II DSK bzw. Art. 8 II EMRK.

c) SPEICHERUNG ZU FESTGELEGTEN ZWECKEN UND ZWECKBINDUNG

Nach Art. 5 lit. b) DSK müssen die Zwecke bei der Speicherung der Daten festgelegt sein; die Daten dürfen dann nur zu den festgelegten Zwecken verwendet werden. Ebenso verlangt Principle 2 der Rec. (92) 1, dass die Sammlung von Proben und die DNA-Analyse nur zum Zweck der Identifikation im Rahmen der Untersuchung und Verfolgung einer Straftat zulässig sind. Ebenso dürfen gem. Principle 3 Abs.1 der Rec. (92) 1 die daraus gewonnenen Informationen nur für Fälle der Untersuchung und Verfolgung von Straftaten genutzt werden. Die Errichtung der DNA-Dateien und der Abruf/Abgleich erfolgen zum Zwecke der Verfolgung von Straftaten, vgl. Art. 2 I, 3 I, 4 I und 7 Prümer Ratsbeschluss; der Abruf von daktyloskopischen Daten erfolgt zum Zwecke der Verfolgung und Verhinderung von Straftaten, vgl. Art. 8 und 9 I Prümer Ratsbeschluss. Der Zweck ist damit bereits in der Rechtsgrundlage bekanntgegeben worden. Spätestens mit der Abnahme der DNA bzw. der daktyloskopischen Daten wird dem Betroffenen in der Praxis kundgetan, dass diese der Verfolgung bzw. Verhinderung einer Straftat dienen; eine solche Mitteilung ist aufgrund des Grundsatzes der Waffengleichheit zu machen. Der Zweck ist damit bereits bei der Erhebung der Daten festgelegt. Problematisch ist ferner, dass im Prümer Ratsbeschluss keine spezifischen Delikte festgelegt wurden. Letztlich ist dies eine Frage

der Genauigkeit der Zweckfestlegung und sollte von der Kommission in einer Weiterentwicklung des Prümer Ratsbeschlusses erwogen werden.

Der Zweckbindungsgrundsatz wurde im Prümer Ratsbeschluss ausdrücklich in Art. 26 geregelt. Nach Art. 26 I Prümer Ratsbeschluss ist eine Verarbeitung der personenbezogenen Daten ausschließlich zu den Zwecken möglich, zu denen sie übermittelt wurden. Augenscheinlich sind hier die personenbezogenen Daten des Art. 5 und 10 Prümer Ratsbeschluss gemeint, da die Zweckbindung hinsichtlich der Personen-DNA, der Spuren-DNA und der Fingerabdrücke eigens in Art. 26 II Prümer Ratsbeschluss geregelt ist. Nach Art. 26 II Prümer Ratsbeschluss ist eine Zweckänderung nicht möglich. Allerdings erlaubt Art. 26 I Prümer Ratsbeschluss eine Zweckänderung, sofern die Zustimmung des dateiführenden Mitgliedstaates vorliegt und das innerstaatliche Recht des empfangenden Mitgliedstaates eine solche zulässt. Die Zustimmung darf ebenfalls nur dann erteilt werden, wenn das nationale Recht des dateiführenden Staates die Verarbeitung zu solchen anderen Zwecken zulässt. Damit ist der neue Zweck zumindest im Recht des dateiführenden Mitgliedstaates festgelegt. Des Weiteren basiert der Zweck dann auf einer nationalen Rechtsgrundlage. Leider wurde in Art. 26 I Prümer Ratsbeschluss nicht festgelegt, dass die spätere Zweckänderung entsprechend Art. 5 lit. b) DSK mit den bereits festgelegten Zwecken vereinbar sein muss, insbesondere stellt sich die Frage, was mit „anderen Zwecken“ gemeint ist.

Des Weiteren ist im Rahmen des Art. 5 lit. b) DSK Folgendes zu bedenken: Da der Betroffene nun auch in dem empfangenden Staat eine Straftat begangen hat, könnte der entsprechende Staat die Daten bei sich speichern und wiederum zum Abgleich bereitstellen. Dies ist im Hinblick auf die Vorschrift des Art. 35 VI Prümer Ratsbeschluss bedenklich, da die Daten aufgrund

bilateraler oder multilateraler Übereinkünfte möglicherweise Dritten zur Verfügung gestellt werden könnten. Damit würde ein Drittstaat Zugriff auf die Daten erhalten, obwohl die vom Prümer Ratsbeschluss geforderten Voraussetzungen möglicherweise nicht vorliegen. Aus diesem Grund sollten solche Übereinkünfte zum einen der Kommission mitgeteilt werden, wie dies auch im Falle weiterer Übereinkünfte zwischen den Mitgliedstaaten erforderlich ist, vgl. Art. 35 IV und V Prümer Ratsbeschluss. Die Kommission könnte dann gem. Art. 36 IV Prümer Ratsbeschluss eine Weiterentwicklung des Prümer Ratsbeschlusses anstreben. Zum anderen müssten diese Übereinkünfte mit Drittstaaten an bestimmte Voraussetzungen geknüpft sein, wie bspw., dass solche Übereinkünfte mit den Bestimmungen des Prümer Ratsbeschlusses in Einklang zu bringen sind. Dies fehlt jedoch gänzlich. Allerdings ist gem. Art. 26 II Prümer Ratsbeschluss eine Verarbeitung der Personen-DNA, der Spuren-DNA und der daktyloskopischen Daten nur zu der Feststellung erlaubt, ob die verglichenen DNA-Profile oder daktyloskopischen Daten übereinstimmen, sowie zu den in den lit. b) und c) genannten Fällen, d.h. eine Verarbeitung in der Weise, dass die Daten in eine neue Datei des empfangenden Staates eingestellt werden, ist nicht möglich. Nach der Feststellung gem. Art. 26 II UAbs. 1 Prümer Ratsbeschluss sind die Daten unverzüglich zu löschen, vgl. Art. 26 II UAbs. 2 S. 2 Prümer Ratsbeschluss. Auf der anderen Seite ist die Verwendung der personenbezogenen Daten (Art. 5 und 10 Prümer Ratsbeschluss) gem. Art. 26 I Prümer Ratsbeschluss unter bestimmten Bedingungen zulässig; fraglich ist allerdings, ob diese wirklich hilfreich sind, da es sich um einfache erkennungsdienstliche Daten bzw. Zusatzinformationen handelt, die keinen Abgleich zulassen. Jedoch ist es vorstellbar, diese für die Rasterfahndung zu nutzen. Zu beachten ist auch Art. 28 III UAbs. 1 Prümer Ratsbeschluss, welcher festlegt, dass Daten zu löschen sind, wenn sie nicht hätten übermittelt oder empfangen werden dürfen.

d) INHALTLICHE QUALITÄT DER DATEN

Nach Art. 5 lit. c) DSK müssen die Daten dem Speicherzweck entsprechen, dafür erheblich sein und dürfen nicht darüber hinausgehen. Der Abgleich von DNA und daktyloskopischen Daten ist ein besonders wichtiges Instrument im Rahmen der Verfolgung von Straftaten. Der Speicherumfang wird durch den Durchführungsbeschluss zum Prümer Ratsbeschluss beschränkt, vgl. zu den daktyloskopischen Daten Art. 2 lit. i). Die DNA wird auf den nicht-codierten Teil beschränkt und auch hier gemäß dem Durchführungsbeschluss auf den Europäischen Standardsatz (ESS), vgl. Anhang zum Durchführungsbeschluss, Kapitel 1.1. Aufgrund dessen, dass bei der DNA nur der nicht-codierte Teil untersucht und auch nur das entsprechende Identifizierungsmuster in das System eingestellt wird, können keine überschüssigen Informationen entnommen werden. Hinsichtlich der daktyloskopischen Daten ist dies anders. Dort werden auch Bilddateien gespeichert. Fraglich ist, ob diese erforderlich sind. Es ist jedoch leider so, dass die Templates für einen gesicherten Abgleich nicht ausreichen, weswegen zusätzlich zu den Templates Bildinformationen erforderlich sind, anhand derer man dann einen Direktabgleich durchführen kann. Diese Bilddatei wird im Übrigen erst nach Feststellung eines Treffers übermittelt. Es stellt sich dann aber die Frage, ob die Daten nicht auch von der ersuchten Partei untersucht werden könnten und eine eindeutige Zuordnung vorgenommen werden könnte. Allerdings wären damit Probleme im Rahmen einer Gerichtsverhandlung verbunden, da die Sprache des Sachverständigen nicht der Gerichtssprache des ersuchenden Staates entsprechen würde. Des Weiteren wäre damit nur eine Umkehrung der Speichermöglichkeit verbunden, denn die ersuchte Partei könnte ebenfalls die Daten der ersuchenden Partei, welche für einen Direktabgleich von Nöten sind, speichern. Es ist zum Schutz des Betroffenen erforderlich, hier Bilddateien zu

verarbeiten, da nur so eine eindeutige Zuordnung möglich ist. Des Weiteren wird im Prümer Ratsbeschluss nur eine Schritt-für-Schritt-Übermittlung vorgenommen, d.h. zunächst wird der Abgleich vorgenommen, anschließend wird im Trefferfall – und auch nur dann – die Übermittlung der Fundstellendatensätze vorgenommen. Sollten diese dann ebenfalls übereinstimmen, können weitere personenbezogene Daten übermittelt werden. Sowohl die Abfrage als auch die Übermittlung der Fundstellendatensätze enthalten keine personenbezogenen Daten, sondern sind vielmehr durch die Kennung anonymisiert. Des Weiteren wird eine Anfrage auf Gewinnung und Übermittlung von DNA-Profilen gem. Art. 7 Prümer Ratsbeschluss nur dann vorgenommen, wenn im Rahmen eines *laufenden* Strafverfahrens keine Daten hierzu vorliegen. In diesem Stadium ist von Erforderlichkeit auszugehen. Gemäß dem Erforderlichkeitsgrundsatz sind die Daten zu löschen, wenn „sie zu dem Zweck, zu dem sie übermittelt worden sind, nicht oder nicht mehr erforderlich sind“, vgl. Art. 28 III UAbs. 1 lit. a) Prümer Ratsbeschluss. Problematisch ist jedoch, dass im Rahmen der Erforderlichkeit nicht festgelegt wurde, für welche Delikte eine Speicherung nötig ist. Zwar verlangt Art. 5 lit. c) DSK nur, dass die Daten für den Speicherzweck erforderlich sind, d.h. Art. 5 lit. c) DSK wäre von dieser Frage nicht berührt, da der Speicherzweck die Erhebung von Daten im Rahmen aller Delikte offen lässt. Allerdings ist dies dennoch interessant und für die Frage der generellen Erforderlichkeit bedeutend. Es ist nicht einzusehen, warum bereits die Begehung von Bagatelldelikten wie bspw. Beleidigung den Abgleich von Daten zulassen soll. Es handelt sich hierbei um einen recht weitgehenden Eingriff. Es ist daher fraglich, inwiefern ein solcher Eingriff wirklich erforderlich ist, v.a. wenn man die zu erwartende Strafe sowie den Aufwand der Festnahme und Fahndung dazu in Verhältnis setzt. Dies ist jedoch v.a. eine

Frage der Verhältnismäßigkeitsprüfung im Rahmen des Art. 8 II EMRK und wurde bereits dort diskutiert.

Principle 2.1 der Rec. R (87) 15 konkretisiert Art. 5 lit. c) DSK und verlangt, dass die Sammlung der Daten nur für Zwecke erfolgt, die notwendig sind für die Verhütung einer tatsächlichen Gefahr oder die Aufklärung von besonderen Straftaten. Ausnahmen sind zulässig, sofern diese speziell vorgesehen sind. In diesem Zusammenhang ist wieder das eben angesprochene Problem relevant, wonach bereits Delikte gespeichert werden, die im Bagatellbereich anzusiedeln sind. Hier liegt z.T. weder eine tatsächliche Gefahr vor noch sind dies *besondere* Straftaten. Diese Delikte wurden auch nicht speziell vorgesehen. Vielmehr wurde der Prümer Ratsbeschluss – ohne dass auf einen Straftatenkataloge überhaupt eingegangen wird – allgemein gehalten. Principle 2.1 der Rec. (87) 15 wurde daher nicht eingehalten.

Principle 3.1 der Rec. R (87) 15 ist erfüllt, da die Speicherung der Daten zur Erfüllung der nationalen Aufgabe der Polizei, nämlich der Verfolgung und Verhütung von Straftaten, sowie zur Erfüllung ihrer internationalen Pflichten, nämlich Art. 2 I und 8 Prümer Ratsbeschluss, erforderlich ist.

Gem. Art. 5 lit. d) DSK müssen die Daten richtig (so auch Principle 3.1 HS. 1 der Rec. R (87) 15) und auf dem neuesten Stand sein; auch dürfen die Daten nicht unvollständig sein, da ansonsten die Richtigkeit in Zweifel steht. Die DNA-Profile müssen gemäß dem Anhang zum Durchführungsbeschluss, Pkt. 1.1, mindestens sechs vollständig bestimmte Loci enthalten; die DNA-Personenprofile müssen dessen ungeachtet mindestens sechs der sieben ESS-Loci enthalten. Dadurch wird ein gemeinsamer Standard gewährleistet. Nach Art. 12 II des Durchführungsbeschlusses ist außerdem sicherzustellen, dass die daktyloskopischen Daten von ausreichender Qualität sind. Des Weiteren bestimmt Art. 28 I S. 1

Prümer Ratsbeschluss, dass die Daten richtig und aktuell sein müssen. Sollten daktyloskopischen Daten dennoch einmal falsch verarbeitet worden sein (wenn z.B. die Templates nicht ordnungsgemäß sind), so kann dieser Fehler aufgrund der Bilddatei aufgefangen werden. Bei den DNA-Daten entsteht nur ein Near-Match, auf dessen Basis eine Fehlerbehebung nur schwer möglich ist; es verbleibt dann lediglich die Möglichkeit einer erneuten DNA-Analyse, wobei fraglich ist, ob eine solche bei einem Near-Match überhaupt angemessen ist. Sollten Daten entgegen Art. 28 I S. 1 Prümer Ratsbeschluss verarbeitet worden sein, so sind die Daten zu berichtigen oder zu löschen, vgl. Art. 28 I S. 2,3 Prümer Ratsbeschluss.

e) AUFBEWAHRUNG DER DATEN

Nach Art. 5 lit. e) DSK dürfen die Daten nicht länger aufbewahrt werden, als es die Zwecke, für die sie gespeichert werden, erfordern (vgl. auch Principle 7.1 der Rec. R (87) 15). Dies ist auch in Art. 28 III UAbs. 1 lit. a) Prümer Ratsbeschluss so festgelegt worden. Principle 7.2 der Rec. R (87) 15 verlangt die Festlegung von festen Aufbewahrungszeiten für die verschiedenen Kategorien von Daten sowie regelmäßige Qualitätskontrollen. Demgemäß sieht Art. 28 III UAbs. 1 lit. b) Prümer Ratsbeschluss vor, dass die Daten zu löschen sind, sobald die innerstaatlichen Höchstfristen abgelaufen sind und sofern die empfangende Stelle auf diese Fristen hingewiesen worden ist. Allerdings sehen viele Staaten keine Löschfristen, sondern nur Fristen zur Überprüfung der Erforderlichkeit vor; dies ist z.B. in Deutschland der Fall. Dementsprechend können die Höchstfristen ausgeweitet werden. Da Art. 5 lit. e) DSK jedoch die Aufbewahrung ebenfalls anhand der Erforderlichkeit bemisst, ergibt sich hieraus kein Problem. Die Mitgliedstaaten haben demnach zumindest konkrete Fristen festzulegen, nach deren Ablauf die Erforderlichkeit zu prüfen ist. In diesem Zusammenhang können dann auch Qualitätskontrollen

stattfinden. Allerdings fehlen feste Aufbewahrungszeiten gem. Principle 7.2 der Rec. R (87) 15. Außerdem sieht Art. 26 II UAbs. 2 S. 3 Prümer Ratsbeschluss vor, dass die übermittelten Daten nach Beendigung des Datenabgleichs bzw. nach der automatisierten Beantwortung unverzüglich zu löschen sind; damit können nur die Daten gemeint sein, die an die ersuchte Stelle zum Zwecke des Vergleichs übermittelt werden (vgl. Art. 8 I Durchführungsbeschluss).

Für die DNA-Proben legt Principle 8 Abs.1 der Rec. (92) 1 fest, dass Proben nicht länger als bis zur richterlichen Entscheidung aufbewahrt werden können, sofern die Zwecke nicht denen der neuen Verwendung entsprechen. Der Prümer Ratsbeschluss hat hierzu nichts geregelt, weshalb dies im nationalen Recht festzulegen ist. Die Ergebnisse der DNA-Analyse sollen gem. Principle 8 Abs. 2 hingegen dann gelöscht werden, wenn sie nicht länger notwendig sind, es sei denn, sie wurden im Rahmen der Verfolgung eines schweren Verbrechens gewonnen. Auch hier sind dann jedoch Aufbewahrungszeiten festzulegen. Bei Verbrechen gegen den Staat sind die Aufbewahrungszeiten von DNA-Analyseergebnissen länger, gleichwohl sind auch hier feste Aufbewahrungsfristen festzulegen, es sei denn, es handelt sich um Spuren-DNA oder der Betroffene erbittet die weitere Aufbewahrung. Der Prümer Ratsbeschluss legt auch hierzu nichts fest, weshalb dies wiederum den Mitgliedstaaten überlassen bleibt. Allerdings reicht hier keine einfache Frist, nach deren Ablauf die Erforderlichkeit zu prüfen ist; vielmehr sollten strenge Aufbewahrungszeiten festgelegt werden. Die Aufbewahrungszeiten können sich möglicherweise dadurch verlängern, dass der Betroffene ein neues Verbrechen begeht und dieses als Notiz in der Datenbank gespeichert wird (vgl. Art. 9 II und 11 II Durchführungsbeschluss).

f) SENSIBLE DATEN

Art. 6 DSK schützt sensible Daten im Besonderen. Fraglich ist daher, ob die DNA-Identifizierungsmuster bzw. die daktyloskopischen Daten Rückschlüsse auf die Gesundheit, die ethnische Herkunft oder die Religion, etc. zulassen. Die DNA-Identifizierungsmuster enthalten keine überschüssigen Informationen. Bei der Untersuchung des DNA-Materials lässt sich darüber streiten, ob der nicht-codierten DNA Informationen entnommen werden können (vgl. Teil B Pkt. D. IV.). Dies ist aber nicht relevant, da in der DNA-Datei nur DNA-Identifizierungsprofile gespeichert werden. Bei den daktyloskopischen Daten hingegen lassen sich anhand der Bilddateien Rückschlüsse auf die Gesundheit und die ethnische Herkunft ziehen. Hinsichtlich letzterer sind möglicherweise nur Asiaten aufgrund ihrer evtl. geringeren Minutienerkennbarkeit feststellbar. Die Fingerabdruckdaten enthalten jedoch unstreitig auch Informationen über die Gesundheit (vgl. Teil C Pkt. C. II.). Fraglich ist daher, ob ein besonderer Schutz erforderlich ist bzw. ob die Sammlung gem. Principle 2.4 der Rec. R (87) 15 ganz verboten werden kann. Jedoch werden die Daten nur Stück für Stück übermittelt und zudem wäre ein Vergleich der Fingerabdrücke ohne die Übermittlung der Bilddatei nicht fundiert, da erst die Bilddatei eine eindeutige Zuordnung ermöglicht. Des Weiteren wird bei jeder Übermittlung eine Einzelfallüberprüfung vorgenommen, vgl. Art. 9 I S. 2 Prümer Ratsbeschluss. Alles in allem lässt dies eine Ausnahme vom Verbot der Sammlung gem. Principle 2.4 der Rec. R (87) 15 zu.

g) DATENSICHERUNG

Die Daten sind gem. Art. 7 DSK bzw. Principle 8 der Rec. R (87) 15 zu sichern. Dementsprechend verlangt Art. 29 Prümer Ratsbeschluss, dass die Daten gegen zufällige oder unbefugte

Zerstörung, zufälligen Verlust, unbefugten Zugang, unbefugte oder zufällige Veränderung und unbefugte Bekanntgabe geschützt sind. Dabei sind gem. Art. 29 II Prümer Ratsbeschluss die Durchführungsbestimmungen zu beachten, welche technische (Art. 29 II lit. a) und b) Prümer Ratsbeschluss) und organisatorische Maßnahmen (lit. c) zu enthalten haben. So sehen Art. 7 II und 12 III der Durchführungsbestimmungen bspw. vor, dass das Übermittlungsverfahren im Wege einer dezentralen Struktur erfolgt, d.h. es gibt keine Datei, in der alle Daten eingegeben und mit der Daten abgeglichen werden können. Vielmehr gibt es viele Dateien, wobei die Verantwortlichkeit für diese weiterhin bei den Mitgliedstaaten verbleibt. Weiterer Vorteil einer dezentralen Datei ist die einfachere Klärung der Herkunft von Daten. Gem. Art. 7 III und 12 IV des Durchführungsbeschlusses sollen die Daten zudem verschlüsselt werden. Der Anhang zum Durchführungsbeschluss enthält viele weitere technische Bestimmungen zum Schutz der Daten, vgl. u.a. Anhang, Pkt. 5.3.2, 5.3.3 etc.

Zur Gewährleistung des Datenschutzes wurden insbesondere folgende organisatorische Maßnahmen getroffen: Art. 27 Prümer Ratsbeschluss sieht vor, dass die übermittelten personenbezogenen Daten ausschließlich durch die Behörden bearbeitet werden dürfen, welche für die Verfolgung (und die Verhinderung) von Straftaten zuständig sind. Eine Weitergabe an andere Behörden ist nur zulässig, sofern der übermittelnde Staat hierzu seine Zustimmung gegeben hat und sofern dies das innerstaatliche Recht des empfangenden Staats zulässt. Des Weiteren sind Protokolldaten zu erstellen, welche den Datenschutzbehörden auf Ersuchen mitzuteilen sind, Art. 30 Prümer Ratsbeschluss. Art. 30 II lit. a) Prümer Ratsbeschluss sieht zudem vor, dass der Abruf/Abgleich nur durch besonders ermächtigte Beamte der nationalen Kontaktstellen erfolgen darf. Zu erwähnen ist in diesem

Zusammenhang auch, dass die Daten pseudonymisiert abgeglichen werden.

Technische Maßnahmen sind in folgenden Vorschriften zu finden: Art. 30 I Prümer Ratsbeschluss bestimmt, dass jede nichtautomatisierte Übermittlung und jeder nichtautomatisierte Empfang sowohl durch die abrufende als auch die dateiführende Stelle dokumentiert werden müssen, deren Angaben ebenfalls von Art. 30 I geregelt werden. Gleiches gilt für den automatisierten Abruf/Abgleich gem. Art. 30 II lit. b) Prümer Ratsbeschluss. Die dadurch entstandenen Protokolldaten sind entsprechend Art. 30 IV Prümer Ratsbeschluss aufzubewahren.

Ferner soll gem. Principle 6 der Rec. (92) 1 die DNA-Analyse nur von Laboratorien ausgeführt werden, welche angemessene Erfahrungen und Einrichtungen haben sowie die Kriterien des Principle 6 der Rec. (92) 1 erfüllen. Es ist davon auszugehen, dass die Laboratorien der Mitgliedstaaten diese Voraussetzungen erfüllen. Zu beachten ist jedoch, dass eine Trennung des Labors von der Polizeibehörde angestrebt werden sollte. Das Labor muss nicht privatisiert, sondern kann durchaus staatlich sein. Allerdings sollten die Polizeibehörden niemals Zugriff auf die DNA erhalten, ebenso wenig wie die Laboratorien Zugriff auf die personenbezogenen Daten erhalten sollten.

h) AUSNAHMEN UND EINSCHRÄNKUNGEN NACH ART. 9 I, II DSK

Der Straftatenkatalog nach Art. 5 lit. b) DSK ist unabdingbar und auch nicht mit einer der Ausnahmen des Art. 9 DSK zu rechtfertigen. Eine Nichtfestlegung von Straftaten mag zwar dazu dienen, dass jeder Staat seine Austauschkriterien selbst festlegen kann und daher einen Austausch zur Verfolgung von Straftaten jeglicher Art vornehmen kann; dies legt jedoch nicht die genauen Zwecke fest und daher stellt sich die Frage der Notwendigkeit,

insbesondere im Zusammenhang mit dem weiteren Problempunkt, ob Bagatelldelikte einen Austausch rechtfertigen. Beleidigungen, Ladendiebstähle, etc. rechtfertigen m. E. ebenfalls keine Ausnahme von Art. 5 lit. b) DSK, da ein Austausch zum Zwecke der Aufklärung solcher Delikte nach dem Prümer Ratsbeschluss in einer demokratischen Gesellschaft nicht gerechtfertigt wäre (vgl. bereits Teil D. Pkt. I. 4. b).

Auch die Festsetzung von Aufbewahrungsfristen dient der Rechtssicherheit und kann zu keiner Ausnahme führen, welche notwendig ist für eine demokratische Gesellschaft. Schließlich reicht es, wenn ungefähre Fristen zur Prüfung der Erforderlichkeit festgelegt werden; dann kann sich der Beamte immer noch entschließen, die Daten weiter zu führen, sofern dies notwendig ist.

i) GRENZÜBERSCHREITENDER DATENSCHUTZ

Ferner sind die Regelungen des Art. 12 DSK zu beachten, da ein grenzüberschreitender Datenverkehr stattfindet. Der grenzüberschreitende Datenverkehr unter Mitgliedstaaten darf nicht verboten oder von einer besonderen Genehmigung abhängig gemacht werden. Der Prümer Ratsbeschluss bestimmt, dass sich der Abgleich/die Übermittlung von Daten sowohl nach dem Grundsatz der Verfügbarkeit als auch nach der Schwedischen Initiative zu richten hat, vgl. Erwägungsgründe 4 und 6 des Prümer Ratsbeschlusses. Diese Vorgabe wird z.B. in Art. 14 II des Durchführungsbeschlusses beachtet, wonach die Ersuchen in Bezug auf daktyloskopische Daten innerhalb von 24 Stunden, auf Anfrage sogar unverzüglich, beantwortet werden müssen. Die Anfragen nach Art. 3 des Prümer Ratsbeschlusses sollten sogar innerhalb von 15 Minuten beantwortet werden, vgl. Anhang zum Durchführungsbeschluss, Pkt. 3.1. Unter Beachtung der

Schwedischen Initiative und des Grundsatzes der Verfügbarkeit ist eine Einschränkung des Datenverkehrs nicht ersichtlich.

Gem. Principle 5.4 der Rec. R (87) 15 soll die Übermittlung personenbezogener Daten auf Polizeibehörden beschränkt bleiben. Die gleiche Regelung findet sich in Art. 27 Prümer Ratsbeschluss.

Ferner ist eine Übermittlung nur zulässig, wenn eine klare rechtliche Regelung vorhanden ist bzw. es um die Verhütung einer erheblichen und drohenden Gefahr oder die Bekämpfung eines schweren Verbrechens geht und sofern die nationalen Bestimmungen zum Schutz des Betroffenen nicht beeinträchtigt werden. Klare rechtliche Regelungen existieren in Art. 3 I, II, 4 I, II, 9 I, II und 7 Prümer Ratsbeschluss i.V.m. den nationalen Vorschriften. Die zweite Variante hingegen würde zum Teil nicht zutreffen, da es teilweise weder um ein schweres Verbrechen noch um eine erhebliche oder drohende Gefahr geht. Bestimmungen zum Schutz des Betroffenen finden sich in Art. 25 II Prümer Ratsbeschluss, wonach eine Übermittlung erst zulässig ist, wenn Datenschutzbestimmungen des Prümer Ratsbeschluss umgesetzt worden sind. Dies muss auch erst durch den Rat festgestellt werden. Hinsichtlich der Mitgliedstaaten, welche bereits Übermittlungen nach dem Vertrag von Prüm durchgeführt haben, gilt Art. 25 II Prümer Ratsbeschluss nicht. Allerdings regelt auch Art. 34 II des Vertrags von Prüm, dass eine Übermittlung erst beginnen darf, wenn die Datenschutzbestimmungen des Vertrags von Prüm erfüllt sind, was der Ministerrat festzustellen hat.

Außerdem hat eine Anfrage nur im Einzelfall zu erfolgen, d.h. es sollte eine vorherige Prüfung, ob der Abgleich der Daten wirklich erforderlich ist, stattfinden, vgl. Art. 3 I, 9 I Prümer Ratsbeschluss. Gem. Principle 5.5 ii. der Rec. R (87) 15 ist außerdem vor einer Übermittlung die Qualität der Daten zu überprüfen. In Art. 14 I des Durchführungsbeschlusses ist dies jedoch genau gegenteilig

geregelt, d.h. der Empfänger überprüft die Daten. Des Weiteren erfolgt gem. Art. 14 I der Durchführungsbestimmungen nur eine Überprüfung dahingehend, ob die Daten für einen Abgleich geeignet sind und nicht ob die Daten richtig, aktuell und vollständig sind. Dies ist nicht ausreichend. Würde nämlich von der übermittelnden Stelle festgestellt werden, dass die Daten nicht mehr richtig bzw. nicht mehr aktuell sind, sind die Daten gar nicht erst zu übermitteln. Nachträglich können die Empfänger nur informiert werden. Allerdings bestimmt Art. 28 I S. 3 Prümer Ratsbeschluss, dass die Mitgliedstaaten dann verpflichtet sind, die Daten zu berichtigen. Problematisch ist hierbei jedoch, dass gar keine Überprüfung der Richtigkeit und Aktualität durchgeführt wird, bevor die Daten aus der Hand gegeben werden. Es stellt sich daher die Frage, wann dann eine Überprüfung der Qualität stattfinden soll. Dies muss eigentlich vor der Übermittlung geschehen.

4. FAZIT

Die Bestimmungen der DSK sind sowohl hinsichtlich des ePasses als auch des Prümer Ratsbeschlusses anwendbar.

Der Verantwortliche wurde jedoch weder in der ePass-Verordnung noch im Prümer Ratsbeschluss festgelegt, weswegen die Ermittlung des Verantwortlichen sich nach den innerstaatlichen Regelungen richtet. In beiden Fällen sind nicht diejenigen Behörden zuständig, welche die Merkmale des Art. 2 lit. d) DSK erfüllen; vielmehr wurde die Zuständigkeit an andere Behörden verwiesen: im Fall des ePasses an die ausstellenden Behörden und im Fall des Austausches von Daten an das BKA als sachnähere Behörde.

Sowohl beim ePass als auch nach dem Prümer Ratsbeschluss werden die Daten auf rechtmäßige Art und Weise beschafft und verarbeitet. Beim ePass erfolgen die Erfassung und die

Verarbeitung in Kenntnis des Passinhabers, da dieser bei der Beantragung persönlich erscheinen muss und danach die Verfügungsgewalt über seinen Ausweis hat. Ferner sind die Erfassung und Verarbeitung seiner Daten, insbesondere seiner biometrischen Daten, durch die ePass-Verordnung festgelegt worden. Der Prümer Ratsbeschluss regelt die Einrichtung einer DNA-Datei, den Abgleich und Abruf von DNA-Profilen sowie den Abruf von daktyloskopischen Daten. Der Betroffene erhält zwar von Abgleichen/Abrufen keine Kenntnis; dennoch hat er hiervon aufgrund des Grundsatzes der Waffengleichheit spätestens bei der Beschuldigtenvernehmung zu erfahren. Zu beachten ist allerdings auch, dass mit der Erfassung der Daten im System, wovon der Betroffene Kenntnis erhält, indem er seine daktyloskopischen Daten bzw. DNA-Daten zur Verfügung stellt, für den Betroffenen zumindest klar sein muss, dass diese Daten weiterhin für die Verfolgung (und Verhinderung) von Straftaten genutzt würden und dass ein Abgleich mit anderen Datenbanken wahrscheinlich ist; insbesondere ist die weitere Verwendung der Daten in innerstaatlichen Regelungen vorgeschrieben und der Abgleich ebenfalls durch innerstaatliches Gesetz umgesetzt worden. Bei einer Untersuchung und Übermittlung nach Art. 7 Prümer Ratsbeschluss erhält der Betroffene sogar bereits bei der Erhebung der Daten Kenntnis. Des Weiteren sind auch die Voraussetzungen der Principles 5.1 (Vorliegen eines legitimen Interesses) und 5.1 i. (Anfragevoraussetzungen) der Rec. R (87) 15 ebenso wie die Voraussetzungen von Principle 4 der Rec. (92) 1 (Gesetzesvorbehalt hinsichtlich der Umstände der DNA-Entnahme) erfüllt.

Hinsichtlich Art. 5 lit. b) DSK wurde festgestellt, dass der ePass den Anforderungen entspricht, da er in Art. 4 III Pass-Verordnung die Zwecke festlegt und eine Zweckänderung nicht erfolgt, insbesondere werden die biometrischen Merkmale nicht für einen Abgleich verwendet. Der Prümer Ratsbeschluss hingegen erfüllt

nicht ganz die Anforderungen. Zwar wurden die Zwecke eines Abgleichs/Abrufs eindeutig festgelegt, allerdings fehlt eine Angabe eines Straftatenkatalogs, was jedoch im Endeffekt eine Frage der Genauigkeit der Zweckfestlegung sein dürfte. Ein weiteres Problem war im Zweckbindungsgrundsatz zu sehen, da in Art. 26 I Prümer Ratsbeschluss (Übermittlung weiterer personenbezogener Daten) nicht festgelegt wurde, dass eine spätere Zweckänderung mit den bereits festgelegten Zwecken vereinbar sein muss, und nicht bestimmt worden ist, was unter „anderen Zwecken" zu verstehen ist. Außerdem wäre gem. Art. 26 I Prümer Ratsbeschluss eine Weiterverwendung der personenbezogenen Daten unter bestimmten Voraussetzungen zulässig. Wie man daran erkennen kann, erfüllt der Prümer Ratsbeschluss die Anforderungen des Art. 5 lit. b) DSK nicht vollständig. Eine weiteres Problem stellte sich bei der möglichen Speicherung der übermittelten Daten im Empfängerstaat, sofern eine solche Regelung im dortigen Recht vorgesehen ist; hier gilt allerdings zu beachten, dass sich der Betroffene dort bereits strafbar gemacht hat, d.h. der Betroffene wird dann nach nationalem Recht sowieso verpflichtet sein, seine Daten herauszugeben, ebenso wie dies im deutschen Recht nach § 81 e ff. StPO geschieht.

Die Voraussetzungen des Art. 5 lit. c) werden hingegen weder durch den ePass noch durch den Prümer Ratsbeschluss erfüllt. Es ist im Rahmen des ePasses durchaus erforderlich – auch zwei – biometrische Merkmale zu verwenden. Auch die Vorgabe „1 Person – 1 Pass" ist angemessen. Allerdings ist nicht verständlich, warum hinsichtlich der Fingerabdrücke keine Templates verwendet werden, da durch die Bilddateien zu viele überschüssige Informationen bekannt werden. Bilddateien sind an sich nicht erforderlich. Im Gegensatz hierzu sind Bilddateien der daktyloskopischen Daten beim Austausch nach dem Prümer Ratsbeschluss durchaus notwendig, um einen zuverlässigen

Vergleich durchzuführen. Hervorzuheben ist außerdem die Schritt-für-Schritt-Übermittlung und die anonyme Verarbeitung. Doch auch hier ist wiederum zu kritisieren, dass kein Straftatenkatalog festgelegt wurde; gleichwohl ist dies im Rahmen des Art. 5 lit. c) DSK auch nicht erforderlich, da der Speicherzweck des Prümer Ratsbeschlusses die Verfolgung aller Delikte ist und die Erhebung der Daten damit im Rahmen des Art. 5 lit. c) DSK liegt. Auswirkungen hat der fehlende Straftatenkatalog zumindest auf Principle 2.1 der Rec. R (87) 15, wonach die Sammlung für Daten nur für Zwecke zu erfolgen hat, welche notwendig für die Verhütung einer tatsächlichen Gefahr oder die Aufklärung von besonderen Straftaten sind; Principle 2.1 der Rec. R (87) 15 wurde daher nicht erfüllt.

Immerhin wurden aber die Voraussetzungen des Art. 5 lit. d) DSK erfüllt. Sowohl der Prümer Ratsbeschluss als auch die ePass-Verordnung verlangen, dass die Daten sachlich richtig und aktuell sein müssen. Da besonders beim Prümer Ratsbeschluss auch Vorschriften zur Vollständigkeit gemacht wurden, kann auch diese nicht bemängelt werden. Der einzige problematische Punkt, welchen die Mitgliedstaaten jedoch selbst regeln müssen, ist die Vorlage ordnungsgemäßer Dokumente bei der Ausstellung eines ePasses.

Allerdings ergaben sich wiederum bei Art. 5 lit. e) DSK Schwachpunkte. Der Prümer Ratsbeschluss erfüllt zwar die Anforderungen des Art. 5 lit. e) DSK, hingegen nicht die der ähnlichen Principles 7.1 bzw. 7.2 der Rec. R (87) 15, wonach feste Aufbewahrungszeiten festzulegen sind. Es ist fraglich, ob es ausreicht, wenn nach Ablauf gewisser Fristen die Erforderlichkeit geprüft wird; dies wird aber freilich nicht den Anforderungen an *feste* Aufbewahrungen gerecht. Auch Principle 8 der Rec. (92) 1 fordert feste Aufbewahrungszeiten für die Ergebnisse der DNA-Analyse, welche jedoch nicht existieren. Beim ePass ist zu

erwähnen, dass nicht festgelegt wurde, ob eine Speicherung der Fingerabdruck- und Gesichtsbild-Daten in einem Register zulässig ist. Während in Deutschland die Fingerabdruckdaten nach Ausgabe des ePasses gelöscht werden müssen, muss dies in anderen Staaten nicht so sein. Eine Speicherung des Gesichtsbildes erfolgt sogar in Deutschland, weswegen man sich fragen muss, ob dies wirklich erforderlich ist und nicht eine zu lange Aufbewahrungsdauer bedingt. Immerhin können diese Daten von den Polizeibehörden – zumindest nach deutschem Recht – abgerufen werden. Mit der langen Aufbewahrung hängt auch eine Verletzung von Art. 5 lit. b) DSK zusammen.

Ferner wurde festgestellt, dass sowohl der Austausch nach dem Prümer Ratsbeschluss als auch der ePass nicht die strengen Vorschriften des Art. 6 DSK einhalten. Das Gesichtsbild bleibt der Öffentlichkeit generell nicht verborgen; die Überprüfung des Fingerabdrucks auf medizinische Daten hin wird bei der Verifikation aufgrund des Zeitmangels gar nicht möglich sein. Im Übrigen gewährt der EAC hinsichtlich der Fingerabdruck-Daten im ePass bereits einen besseren Schutz. Beim Austausch nach dem Prümer Ratsbeschluss sind die Bilddateien sogar erforderlich, um einen Vergleich vorzunehmen. Auch wird der übermäßigen Verbreitung biometrischer Daten dadurch vorgesorgt, dass erst ein Hit-/No Hit-Verfahren durchgeführt wird, bevor weitere Daten übermittelt werden. Aus dem DNA-Identifizierungsmuster lassen sich im Übrigen auch keine medizinischen Daten ablesen.

Die Datensicherung des Austauschs nach dem Prümer Ratsbeschluss erfolgt auf vielerlei Ebenen. So sieht Art. 29 Prümer Ratsbeschluss i.V.m. den Durchführungsbestimmungen technische und organisatorische Maßnahmen vor. Es findet nur eine dezentrale Vernetzung statt. Die datenverarbeitenden Behörden und Beamten werden nach dem Prümer Ratsbeschluss ebenfalls eingeschränkt. Es werden Protokolldaten erhoben und

Übermittlungen dokumentiert. Die Übermittlung der Daten erfolgt anonymisiert. Einzig Principle 6 der Rec. (92) 1 hat keinen Eingang in den Prümer Ratsbeschluss gefunden. Vielmehr bleibt es den Mitgliedstaaten überlassen, die Anforderungen an die Laboratorien umzusetzen. Beim ePass hingegen sind einige Mängel sichtbar geworden. So ist eine Zerstörung des Chips durch Mikrowellen möglich. Des Weiteren können die Daten auf dem Chip unbemerkt ausgelesen werden; dazu gehört insbesondere auch das Gesichtsbild. Einem solchen Angriff kann mittels eines Passworts bzw. eines Faradayschen Käfigs vorgebeugt werden. Zudem wurde festgestellt, dass nach der Kommissions-Entscheidung kein Schutz vor unbefugter Veränderung besteht, da der Chip kopiert werden könnte. Mit der Änderung der Kommissionsentscheidung wurde jedoch die Chip-Authentifizierung eingeführt, durch welche man einen Original-Chip von einem kopierten Chip unterscheiden kann. Weiteren Angriffen auf die Daten kann man dadurch begegnen, dass man geschultes Personal einstellt, welches bei der Passkontrolle anwesend ist. Auch sollte der Passinhaber hinsichtlich des Umgangs mit dem Pass informiert werden.

Aufgrund der Anwendung der Schwedischen Initiative und des Grundsatzes der Verfügbarkeit auf den Austausch nach dem Prümer Ratsbeschluss wurde festgestellt, dass auch Art. 12 DSK eingehalten worden ist. Im Übrigen wurde auch Principle 5.4 der Rec. R (87) 15 eingehalten, wonach die Übermittlung personenbezogener Daten auf Polizeibehörden beschränkt bleiben muss und wonach für die Übermittlung eine klare rechtliche Regelung vorhanden sein muss. Principle 5.5 ii. der Rec. R (87) 15 wurde hingegen nicht eingehalten. Die Qualität der Daten wird erst nach Übermittlung der Daten überprüft. Allerdings ist beim Abgleich nach dem Prümer Ratsbeschluss ein vorheriger Abgleich aufgrund des automatisierten Verfahrens gar nicht möglich, weshalb die erste Gelegenheit zur Prüfung auch erst beim

Empfänger gegeben ist. Dennoch wurde festgestellt, dass dies den Anforderungen des Principle 5.5. ii. der Rec. R (87) 15 nicht genügt, da bei dieser Qualitätsprüfung nicht geprüft wird, ob die Daten richtig und aktuell sind. Mangels staatenübergreifender Übermittlung von Daten war Art. 12 DSK für den ePass nicht relevant.

III. ZWISCHENERGEBNIS

Zusammenfassend lässt sich also Folgendes feststellen: Sowohl der ePass als auch der Austausch nach dem Prümer Ratsbeschluss unterfallen dem Schutzbereich des Art. 8 I EMRK. Das Recht auf Achtung des Privatlebens wird durch vielfache Maßnahmen beeinträchtigt. Hierfür existiert eine Gesetzesgrundlage. Beim ePass erfüllt diese die Anforderungen der Rechtsprechung. Der Prümer Ratsbeschluss hingegen weist Mängel in der Vorhersehbarkeit der Maßnahmen aufgrund unbestimmter Rechtsgrundlage auf. So ist insbesondere im Rahmen des Ermessens das Fehlen eines Straftatenkataloges zu kritisieren. Ungeachtet dessen verfolgen sowohl der ePass als auch der Prümer Ratsbeschluss legitime Ziele. Im Rahmen der Verhältnismäßigkeitsprüfung wurde aber wiederum festgestellt, dass ein Mangel an Sicherheitsvorkehrungen besteht, insbesondere aufgrund des Fehlens von Vorschriften zur strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit. Auch könnte die Sicherheit des ePasses durch ein Passwort verbessert werden. Der Grundsatz der Subsidiarität ändert letztlich nichts an dieser Bewertung, da zumindest im Rahmen der Verantwortlichkeit festgelegt werden sollte, dass von den Mitgliedstaaten solche Maßnahmen zu treffen sind; auch ein Straftatenkatalog ist unentbehrlich, um den Beurteilungsspielraum einzugrenzen.

Beim Vergleich mit der DSK bzw. mit der Rec. R (87) 15 und Rec. (92) 1 sind mehrere Mängel aufgefallen. Um einen Überblick zu bekommen, erfolgt nun eine getrennte Darstellung von ePass und Prümer Ratsbeschluss.

Der ePass weist Mängel gerade in Bezug auf Art. 5 lit. c) DSK auf, da hinsichtlich der Fingerabdrücke keine Templates, sondern Bilddateien verwendet werden, welche überschüssige Informationen enthalten, obwohl die Verwendung von Templates durchaus möglich wäre. Des Weiteren sollten die Mitgliedstaaten darauf achten, dass bei der Ausstellung der Pässe ordnungsgemäße Dokumente vorgelegt werden. Weiterer Kritikpunkt ist, dass nicht geregelt wurde, dass eine Speicherung von Fingerabdruck- und Gesichtsbild-Daten in einem Register nicht zulässig ist. Dies verstößt gegen Art. 5 lit. e) DSK. Ferner wurden die Vorgaben des Art. 7 DSK nicht vollständig eingehalten, d.h. der Chip kann durch Mikrowellen zerstört werden und es ist ein unbemerktes Auslesen möglich. Dagegen sind noch Maßnahmen zu ergreifen. Auch sollte der Inhaber für den Fall des Verlusts informiert und geschultes Personal zur Verhinderung von Computer-Angriffen eingesetzt werden.

Der Prümer Ratsbeschluss weist ebenfalls zahlreiche Mängel auf. So wurde entgegen Art. 5 lit. b) DSK der Zweckbindungsgrundsatz nicht eingehalten. Gem. Art. 26 I Prümer Ratsbeschluss können personenbezogene Daten übermittelt und zu „anderen Zwecken“ verwendet werden. Es wurde nicht festgelegt, dass dies mit den bereits festgelegten Zwecken vereinbar sein muss und zudem sind die „anderen Zwecke“ nicht bestimmt worden. Des Weiteren wurde festgestellt, dass aufgrund des fehlenden Straftatenkatalogs Principle 2.1 der Rec. R (87) 15 nicht beachtet wurde, welche vorschreibt, dass eine Sammlung nur für Zwecke der Aufklärung einer besonderen Straftat zu erfolgen hat. Auch die Principles 7.1 und 7.2 der Rec. R (87) 15 sowie Principle 8 der Rec. (92) 1 wurden

mangels Festlegung einer festen Aufbewahrungszeit nicht beachtet. Des Weiteren konnte wegen des Fehlens einer entsprechenden Vorschrift im Prümer Ratsbeschluss nicht sicher ausgesagt werden, ob die DNA-untersuchenden Laboratorien die Anforderungen des Principle 6 der Rec. (92) 1 erfüllen. Im Übrigen wurden auch die Anforderungen von Principle 5.5 ii. der Rec. R (87) 15 nicht erfüllt. Auch wenn aufgrund des automatisierten Austauschs eine Überprüfung der Qualität erst nach der Übermittlung möglich ist, so hat sich die Prüfung nicht nur auf die Geeignetheit der Merkmale, sondern auch auf deren Richtigkeit und Aktualität zu beziehen. Dies wird wohl bei der dateiführenden Stelle verbleiben müssen, und zwar nachdem ein Treffer festgestellt wurde, aber bevor eine Übermittlung der Fundstellendatensätze vorgenommen wird.

C. ÜBERPRÜFUNG DES EPASSES UND DER PRÜM-REGELUNGEN IM HINBLICK AUF DIE VERFAHRENSRECHTLICHEN VORGABEN DES DATENSCHUTZES

In diesem Kapitel sollen die verfahrensrechtlichen Möglichkeiten eines Betroffenen erörtert werden. Hierzu gehören die datenschutzrechtlich gewährten Verfahrensrechte wie z.B. das Recht auf Auskunft, Löschung, Berichtigung, Sperrung und Kontrolle durch eine unabhängige Datenschutzinstanz. Daneben gibt es auch gewisse Rechtsschutzgewährleistungen, wie etwa den Zugang zu einer unabhängigen Instanz, die Waffengleichheit, die Garantie gerichtlichen Rechtsschutzes etc.

Die eben erwähnten Rechte und Garantien ergeben sich u.a. aus Art. 8 I EMRK selbst sowie aus den Art. 6 und 13 EMRK. Hinzu kommen die DSK sowie die Empfehlung R (87) 15, wobei letztere nur speziell datenschutzrechtliche Verfahrensgarantien gewähren.

Bei der Prüfung der nachfolgenden Rechtsschutzmöglichkeiten geht es darum, ob durch den ePass und die Prümer Rechtsakte verfahrensrechtliche Sicherungen im Sinne des Datenschutzrechts vorhanden sind, also Löschungs- und Auskunftsrechte etc. sowie um die Möglichkeit der Anrufung einer nationalen gerichtlichen Kontrollinstanz, welche den Anforderungen der EMRK gerecht wird.

Zunächst wird daher mangels gesetzlicher Konkretisierung in der EMRK die Rechtsprechung zu den allgemeinen Verfahrensgarantien beleuchtet und anschließend auf die konkreten datenschutzrechtlichen Garantien der DSK und der Empfehlung R (87) 15 eingegangen.

I. VÖLKERRECHTLICHE RECHTSPRECHUNG

Sowohl zu Art. 8 I EMRK als auch zu den Art. 6 und 13 EMRK gab es bislang Rechtsprechung im Zusammenhang mit dem Recht auf Zugang zu Informationen bzw. mit dem Recht auf Zugang zu einer unabhängigen Instanz.

1. VERFAHRENSRECHTLICHE GARANTIEN IN ART. 8 I EMRK

Die Rechtsprechungsorgane haben in Art. 8 I EMKR aus dem Recht auf Achtung des Privatlebens entsprechende Garantien zur Sicherung dieser Ansprüche abgeleitet.

Nach der Rechtsprechung des Gerichtshofs ist der Staat verpflichtet, ein Zugangsrecht zu gewähren. Im Fall *McMichael* hat sich der Gerichtshof mit dem Verhältnis von Art. 6 I zu Art. 8 I EMRK auseinandergesetzt und festgestellt, dass in beiden Artikeln Verfahrensgarantien enthalten sind.[554] In der Sache *Leander* hat der EGMR entschieden:

> *„Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Art. 8 § 1."*[555]

Betrachtet man den Wortlaut „which were coupled", so wird ersichtlich, dass die Verweigerung des Rechts auf Einsichtnahme den Eingriff wesentlich erschwert und aufgrund der erhöhten Eingriffsqualität erhöhte Verhältnismäßigkeitserwägungen nach sich zieht.[556] Im Fall *Gaskin*[557] hat sich der Beschwerdeführer gegen die Weigerung, ihm Zugang zu seinen Akten zu gewähren,

---

[554] EGMR, Urteil vom 24.02.95 – *McMichael./.Vereinigtes Königreich,* § 91; Siemen, S. 191 f.
[555] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 48.
[556] Siemen, S. 181 f.
[557] EGMR, Urteil vom 07.07.89 – *Gaskin./.Frankreich*.

gewendet. Die britischen Behörden hatten dem in einer Pflegefamilie aufgewachsenen Beschwerdeführer die Einsicht in die Akten verweigert, obwohl die Akten für den Beschwerdeführer die einzige Quelle seine Herkunft und seine Kindheit betreffend war. Der Gerichtshof ging davon aus, dass es sich bei der bloßen Verweigerung des Zugangs zu Informationen um ein Unterlassen handle, weswegen eine positive Verpflichtung des Staates vorhanden sein müsste.[558] Fraglich war daher eine Handlungspflicht des Staates. Der Gerichtshof sah im Sammeln der Daten zusammen mit der Verweigerung der Einsichtnahme einen Eingriff in Art. 8 I EMRK.[559] Daraus ist zu folgern, dass ein Eingriff nur dann – aber nicht stets – angenommen werden kann, wenn der Staat bereits zuvor tätig war und Daten über eine Person gesammelt hat. Auch in der Sache *M.G./.Vereinigtes Königreich* hat der EGMR eine Verletzung des Art. 8 I EMRK wegen Verweigerung des Zugangs anerkannt. Der Beschwerdeführer verlangte Einsicht in die Akten des Sozialamtes, das in seiner Kindheit mindestens fünfmal die Fürsorge übernommen hatte. Statt der vollen Einsicht wurden ihm nur ausgewählte Informationen mitgeteilt. In dieser Zeit war auch ein neues Gesetz – der Data Protection Act 1998 – erlassen worden, welches ungehinderten Zugang zu Informationen gewährte und im Fall der Zugangsverweigerung eine Beschwerdemöglichkeit zu einem Gericht oder Datenschutzbeauftragten eröffnete. Für die Beurteilung des Eingriffs war letztlich entscheidend, dass im nationalen Recht bis zum Inkrafttreten des Data Protection Act 1998 keine Möglichkeit einer Beschwerde vorgesehen war, weswegen der EGMR vom ersten Auskunftsersuchen bis zum Inkrafttreten des Data

[558] EGMR, Urteil vom 07.07.89 – *Gaskin./.Frankreich*, § 41.
[559] EGMR, Urteil vom 07.07.89 – *Gaskin./.Frankreich*, § 49; Siemen, S. 182 ff.; Sule, S. 76.

Protection Act 1998 eine Verletzung des Art. 8 I EMRK feststellte.[560]

Auch die Kommission hat ein Einsichtsrecht anerkannt. So waren dem Beschwerdeführer in der Sache *Martin./.Schweiz* auf seinen Auskunftsantrag hin nur geschwärzte Textpassagen ausgehändigt worden. Der Beschwerdeführer forderte daraufhin vollständige Einsichtnahme und Vernichtung. Allerdings wurde daraufhin nur der Zugang zu den Informationen für 50 Jahre gesperrt. Hinsichtlich der Sperre ging die Kommission von einem verhältnismäßigen Eingriff aus, da die Sperre von 50 Jahren einen ausreichenden Schutz der Privatsphäre bieten würde. In Bezug auf die lückenhafte Einsichtnahme geht die Kommission ebenfalls von einem gerechtfertigten Eingriff aus. Zur Eingriffsqualität selbst lässt sich jedoch aus der Entscheidung nichts entnehmen.[561] Wie die Kommission eine solche Verweigerung der Einsichtnahme beurteilt, lässt sich jedoch aus der Entscheidung *Martin./.Vereinigtes Königreich* erkennen. Der Beschwerdeführer hatte Einsicht in seine medizinischen Daten verlangt, welche im Verlauf seiner vierjährigen psychologischen Behandlung angefertigt worden waren. Die Herausgabe der Informationen machte man jedoch von einem vom Betroffenen zu bestimmenden medizinischen Berater abhängig, der die Einsicht letztlich ablehnte. Im Unterschied zum Fall *Martin./.Schweiz* verlangte die Kommission nun eine positive Verpflichtung zur Einsichtsgewährung. Diese Verpflichtung wurde mit Hinweis darauf abgelehnt, dass die Geheimhaltung dem Wohl der Gesundheit des Betroffenen diene. Dies sei auch gerechtfertigt, da die Daten im Vergleich zur Sache Gaskin, welcher um Einsicht in Daten über sein gesamtes Leben ersuchte, nur einen Zeitraum von

[560] EGMR, Urteil vom 24.09.02 – *M.G./.Vereinigtes Königreich*, § 32; Siemen, S. 189 f.
[561] EKMR, Entscheidung vom 05.04.96 – *Martin./.Schweiz,* DR 81-B, 136 (139 f.); Siemen, S. 186 f.

vier Jahren beträfen und für die weitere Behandlung des Betroffenen nicht erforderlich seien. Zudem habe der Betroffene den Berater schließlich selbst aussuchen können.[562] Dagegen gewährte die Kommission den Beschwerdeführern in der Sache *V. et alia./.Niederlande* Einsicht in die gespeicherten Informationen, da durch die Speicherung und die Verweigerung der Auskunft ein Eingriff nicht auszuschließen sei, der zudem noch auf keiner gesetzlichen Grundlage basierte. Die Beschwerdeführer waren Mitglieder der niederländischen Friedensbewegung, weshalb sie beim militärischen Spionageabwehrdienst gespeichert wurden. Nachdem eine solche Speicherung bekannt wurde, verlangten die Beschwerdeführer Einsicht in die Akten.[563]

Des Weiteren hat die Kommission im Zusammenhang mit dem Fall *Chave née Julien./.Frankreich*[564] auch Löschungsansprüche anerkannt. Die Beschwerdeführerin war in eine psychiatrische Klinik eingewiesen worden. Jahre später stellte sich die Unrechtmäßigkeit dieser Maßnahme heraus, weswegen die Beschwerdeführerin die Löschung sämtlicher vorhandenen Unterlagen verlangte. Die Behörde bestritt die Existenz solcher Unterlagen. Die Kommission hat einen Eingriff für möglich gehalten, da in der behandelnden Klinik solche Unterlagen vorhanden gewesen sein mussten. Jedenfalls sei der Eingriff gerechtfertigt, da die Daten nicht allgemein zugänglich seien und aufgrund des medizinischen Inhalts dem Wohl der Beschwerdeführerin dienten. Zwar wurden Löschungsansprüche hier abgelehnt; dass die Kommission jedoch die Möglichkeit eines

[562] EKMR, Entscheidung vom 28.02.96 – *Martin./.Vereinigtes Königreich*, § 1; Siemen, S. 188 f.
[563] Sule, S. 76.
[564] EKMR, Entscheidung vom 09.07.91 – *Chave née Julien./.Frankreich*.

solchen Anspruchs in Betracht zog, zeigt, dass sie von der Existenz eines Löschungsanspruchs ausgeht.[565]

Jedoch stellt sich auch bei Vorliegen einer positiven Verpflichtung die Frage der Rechtfertigung.[566] Hierbei ist eine Abwägung zwischen den Interessen des Betroffenen und anderen Interessen vorzunehmen.[567] Sofern Interessen Dritter betroffen sind, kollidieren diese mit den Interessen des Betroffenen. So war den an der Pflege von Herrn Gaskin beteiligten Personen Vertraulichkeit zugesichert worden. Letztlich hat der Gerichtshof die Verhältnismäßigkeit der Verweigerung verneint, da keine unabhängige Institution über die Akteneinsicht entschieden habe.[568] Der Staat ist insgesamt in der Wahl seiner Mittel relativ frei und hat einen großen Beurteilungsspielraum. Dieser reduziert sich jedoch in dem Maße, in dem Mitgliedstaaten einen gemeinsamen europäischen Standard angenommen haben.[569]

Zusammenfassend lässt sich daher sagen, dass der Gerichtshof den Auskunftsanspruch im Rahmen des Art. 8 I EMRK nur im Einzelfall gewährt und grundsätzlich von der Qualität der Daten abhängig macht. Allerdings sind die Anforderungen hinsichtlich des Bestehens einer positiven Verpflichtung wesentlich höher als bei einem Abwehranspruch.[570] Falls jedoch eine positive Verpflichtung festgestellt wird, belässt der Gerichtshof den Behörden zusätzlich einen weiten Beurteilungsspielraum,[571] weswegen bislang noch von einem relativen niedrigen Schutzgehalt der Verfahrensrechte auszugehen ist.

---

565 Vgl. zu diesem Absatz Siemen, S. 192 f.
566 EGMR, Urteil vom 17.10.86 – *Rees./.Vereinigtes Königreich*, § 37; EGMR, Urteil vom 21.02.90 – *Powell & Rayner./.Vereinigtes Königreich*, § 41.
567 EGMR, Urteil vom 17.10.86 – *Rees./.Vereinigtes Königreich*, § 37.
568 EGMR, Urteil vom 07.07.89 – *Gaskin./.Frankreich*, § 49.
569 siehe zu diesem Absatz Siemen, S. 197 ff.
570 So Siemen, S. 196.
571 Siemen, S. 197 f.

Nach *Esser* enthält Art. 8 EMRK auch die Möglichkeit der Überprüfung des Eingriffs durch eine unabhängige nationale Instanz.[572] Wie man daran und an der Rechtsprechung des EGMR erkennen kann, ist mittlerweile eine Tendenz ersichtlich, dem Art. 8 EMRK Garantien des Art. 6 EMRK zuzusprechen. So hat der EGMR in der Sache *Elsholz* ein unzulängliches Verfahren als Verstoß gegen Art. 8 EMRK betrachtet und deswegen zugleich einen Verstoß gegen Art. 6 I EMRK festgestellt,[573] wohingegen der Gerichtshof in der Sache *Haase* bereits den Art. 6 I EMRK gar nicht mehr geprüft hat.[574] Dies ein sinnvoller Ansatzpunkt. [575] Art. 6 EMRK würde damit nicht völlig überflüssig, sondern wirkt nur als allgemeines Justizgrundrecht, welches natürlich auch im Rahmen des Art. 8 EMRK zu beachten ist. Um jedoch eine saubere Zuordnung vornehmen zu können, wäre es sinnvoller, sämtliche verfahrensrechtlichen Garantien, welche im Zusammenhang mit dem Recht auf Privatleben, im Besonderen mit dem Recht auf Datenschutz, stehen, mit Art. 8 EMRK zu begründen. Art. 8 EMRK würde damit zu einem ganzheitlichen Abwehr- und Schutzrecht. Der Datenschutz als eigenständiges Element des Rechts auf Privatleben kann auch nur in Verbindung mit zu gewährenden Verfahrensregelungen Bestand haben, denn wenn einem ein Recht auf Privatleben gewährt wird, muss man dieses mithilfe von verfahrensrechtlichen Sicherungen auch durchsetzen können. Natürlich existiert hierzu die Möglichkeit gerichtlicher Verfahren etc. Aber diese sind nur möglich, wenn man erstens Kenntnis von der Speicherung usw. erhält und zweitens bestimmte Rechte wie bspw. Löschung oder Berichtigung hat. Zudem ist die gerichtliche Überprüfung zu unterscheiden von einer kontrollierenden Instanz wie bspw. dem Datenschutzbeauftragten. Es ist jedoch

572 Esser, in: Wolter/Schenke/Hilger/Ruthig/Zöller, Art. 8 S. 307.
573 EGMR, Urteil vom 13.07.00 – *Elsholz./.BRD*, § 53, 67.
574 EGMR, Urteil vom 08.04.04 – *Haase./.BRD*, § 108.
575 Uerpmann, in: Ehlers, § 3 Rn. 29.

anzunehmen, dass die Rechtsprechung gerade letztere von Art. 8 EMRK umfasst gesehen hat, wohingegen die gerichtliche Überprüfung von Art. 6 EMRK umfasst ist. Während die Kontrollinstanz bereits bei der Erhebung, Verarbeitung etc. die Kontrolle vornehmen und zur Durchsetzung der Löschungs- und Berichtigungsrechte des Art. 8 EMRK verhelfen kann, soll eine gerichtliche Überprüfung dazu dienen, gegen eine Auskunfts- oder Löschungsverweigerung oder dergleichen vorgehen zu können. In diesem Verfahrensstadium sind dann die Gewährleistungen des Art. 6 EMRK von Bedeutung.

Sämtliche verfahrensrechtlichen Garantien nur auf Art. 6 EMRK zu stützen, würde auch Art. 8 II EMRK nicht gerecht werden. Die Rechtsprechungsorgane haben im Rahmen der Rechtfertigungsprüfung mehrfach verfahrensrechtliche Garantien verlangt, um einen Eingriff zu rechtfertigen und um den Schutz des Einzelnen gegen Missbrauch zu stärken. Würde man diese Garantien – u.a. das Recht auf Unabhängigkeit der Kontrollinstanz – in Art. 6 EMRK verorten, so rechtfertigt sich zwangsläufig in höherem Maße ein Eingriff in Art. 8 I EMRK, wohingegen Art. 6 EMRK verletzt wäre, obwohl der Eingriff selbst mit Art. 6 EMRK nur im Allgemeinen zu tun hat, da es sich eigentlich um ein Problem des Privatrechtsschutzes handelt. Dennoch sollten gewisse Gewährleistungen des Art. 6 EMRK – wie etwa die Unabhängigkeit der Instanz – auch im Rahmen des Art. 8 II EMRK gewahrt werden, da nur so eine wirkungsvolle Sicherung des Rechts auf Privatleben möglich ist und der Eingriff nur dann auch wirklich gerechtfertigt ist. Würden die allgemeinen Garantien des Art. 6 EMRK bei Art. 8 II EMRK missachtet, so wäre die Prüfung der Verhältnismäßigkeit im Rahmen des Art. 8 II EMRK bedeutungslos.

2. VERFAHRENSRECHTLICHE GARANTIEN IN ANDEREN VORSCHRIFTEN DER EMRK

a) ART. 5 EMRK

Der Gerichtshof stellte in Art. 5 IV EMRK ein Recht auf Zugang zu Informationen im Zusammenhang mit Strafverfahren fest. Dem Beschwerdeführer war die Einsicht in seine strafrechtlichen Akten verwehrt worden, so dass er die Rechtmäßigkeit seiner Freiheitsentziehung nicht überprüfen lassen konnte. Der Gerichtshof sah darin eine Verletzung der Rechte aus Art. 5 IV EMRK, da eine solche Einsichtnahme unbedingt erforderlich gewesen sei.[576] Allerdings ist Art. 5 EMRK nur im Falle einer Freiheitsentziehung anwendbar, weswegen er im Folgenden keine Beachtung mehr findet.

b) ART. 6 EMRK

Neben den Vorgaben des Art. 8 I EMRK enthalten auch die Art. 6 und 13 EMRK verfahrensrechtliche Garantien, welche auch vom EGMR bereits mehrfach im Zusammenhang mit Art. 8 I EMRK geprüft wurden.[577] Aus diesem Grund sind die Garantien dieser Vorschriften ebenfalls näher zu erläutern.

Art. 6 EMRK garantiert ein Recht auf ein faires Verfahren. Nach Art. 6 I EMRK hat *„jede Person ein Recht darauf, dass über Streitigkeiten in Bezug auf ihre zivilrechtlichen Ansprüche und Verpflichtungen oder über eine gegen sie erhobene strafrechtliche Anklage von einem unabhängigen und unparteiischen, auf Gesetz beruhenden Gericht in einem fairen Verfahren, öffentlich und innerhalb angemessener Frist verhandelt wird“*. Des Weiteren hat

[576] EGMR, Urteil vom 30.03.89 – *Lamy./.Belgien*, § 29 Siemen, S. 205.
[577] Vgl. u.a. EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*, § 55; EGMR, Urteil vom 25.09.01 – *P.G. und J.H./.Vereinigtes Königreich*, § 88; EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, § 77.

jede Person nach Art. 6 III lit a), b) und d) EMRK das Recht, *„a) innerhalb möglichst kurzer Frist in einer ihr verständlichen Sprache in allen Einzelheiten über Art und Grund der gegen sie erhobenen Beschuldigung unterrichtet zu werden; (...) b) ausreichende Zeit und Gelegenheit zur Vorbereitung ihrer Verteidigung zu haben; d) Fragen an Belastungszeugen zu stellen oder stellen zu lassen und die Ladung und Vernehmung von Entlastungszeugen unter denselben Bedingungen zu erwirken, wie sie für Belastungszeugen gelten."* Natürlich verfügt Art. 6 EMRK über weitere Rechte wie bspw. das Recht auf eine angemessene Verfahrensdauer oder auf Prozesskostenhilfe, welche jedoch für die vorliegende Arbeit nicht von Bedeutung sind.

Die Rechte des Art. 6 EMRK sind gerade für den Datenschutz und die damit verbundenen Verfahrensgarantien von Belang. Art. 6 EMRK erfasst entgegen seinem Wortlaut nicht nur zivil- und strafrechtliche Streitigkeiten im engeren Sinne, so dass viele Streitigkeiten, welche nach deutschem Recht eigentlich als öffentlich-rechtlich zu qualifizieren sind, vom Gerichtshof als zivilgerichtliche Angelegenheit angesehen werden.[578] Der Gerichtshof stellt für die Prüfung, ob ein zivilgerichtlicher Anspruch vorliegt, darauf ab, ob „der Ausgang des Verfahrens zivilrechtliche Ansprüche oder Verpflichtungen begründet, ändert oder aufhebt"[579]. Aus diesem Grund fallen darunter Streitigkeiten über die Aufhebung strafrechtlicher Verurteilung, Disziplinarverfahren gegen Beamte, Streitigkeiten über Persönlichkeitsrechte sowie Streitigkeiten über Schadensersatzansprüche gegen den Staat.[580]

[578] Meyer-Ladewig (2011), Art. 6 EMRK, Rn. 4.
[579] Meyer-Ladewig (2011), Art. 6 EMRK, Rn. 14.
[580] Meyer-Ladewig (2011), Art. 6 EMRK, Rn. 17.

(1) Recht auf Zugang zu einem Gericht

Des Weiteren muss das Gericht unabhängig und unparteiisch sein. Ersteres bedeutet, dass dessen Mitglieder unabsetzbar und unversetzbar sowie weisungsfrei[581] sind. Unabsetzbarkeit bedeutet dabei nicht, dass ein Richteramt auf Lebenszeit erforderlich ist, sondern vielmehr für eine gewisse Dauer, welche eine Instabilität vermeidet.[582]

Außerdem muss das Gericht eine effektive Kontrolle ausüben können, d. h. es muss ausreichende Entscheidungsbefugnisse haben, um über Rechts- und Tatsachenfragen verfügen zu dürfen und die Aufhebung von Maßnahmen anordnen zu können.[583] Natürlich kann das Recht auf Zugang auch Beschränkungen unterworfen werden, solange ein legitimes Ziel verfolgt wird und die Maßnahmen hierzu verhältnismäßig sind.[584] Dementsprechend sind Beschränkungen zum Schutz vor missbräuchlichen und wiederholten Klagen sowie Bedingungen an die Zulässigkeit eines Rechtsmittels möglich.[585]

Regelungen, welche an Gerichte eines anderen Staats verweisen, stellen im Vergleich zum nationalen Rechtsschutz Beschränkungen dar. So wird sich womöglich ein Betroffener durch die andere Gerichtssprache, die räumliche Entfernung, das ungewohnte Verfahrensrecht, die Unkenntnis möglicher Rechtsbehelfe sowie

---

581 EGMR, Urteil vom 28.06.84 – *Campbell & Fell./.Vereinigtes Königreich*, § 80; Heselhaus/Nowak, § 53 Rn.2.
582 EGMR, Urteil vom 28.06.84 – *Campbell & Fell./.Vereinigtes Königreich*, § 80; Heselhaus/Nowak, § 53 Rn.2.
583 EGMR, Urteil vom 21.09.93 – *Zumtobel*, § 29; EGMR, Urteil vom 23.09.82 – *Sporrong&Lönnroth./.Schweden*, §§ 84 ff.
584 EGMR, Urteil vom 28.05.85 – *Ashingdane./.Vereinigtes Königreich,* § 57.
585 Grabenwarter, in: Ehlers, § 6 Rn. 39 f.

erhöhte Schwierigkeiten bei der Anwaltssuche abschrecken lassen.[586]

(2) Recht auf ein faires Verfahren

Zum Recht auf ein faires Verfahren zählen viele Teilgewährleistungen, wobei hier nur einige ausgesuchte aufgezeigt werden.

Danach ist bspw. der Grundsatz der Waffengleichheit ein Aspekt des „fair trial". Demnach muss jede Partei die Möglichkeit haben, ihren Sachverhalt mit den entsprechenden Beweisen vortragen zu können, ohne gegenüber der anderen Partei benachteiligt zu sein, es gilt mithin also verfahrensrechtliche Gleichstellung.[587] Jeder muss somit die gleiche Chance haben, die Entscheidung des Gerichts zu beeinflussen. Dies setzt natürlich auch den Zugang zu den entsprechenden Informationen voraus.[588]

Zum Recht auf ein faires Verfahren gehört auch der Anspruch auf rechtliches Gehör. Dazu zählt die Möglichkeit der gleichberechtigten Kenntnisnahme vom Akteninhalt, d.h. in Bezug auf Stellungnahmen oder Beweismittel, so dass der Betroffene über den Verfahrensstoff umfassend informiert ist.[589] In Verbindung mit der Waffengleichheit ist auch zu überprüfen, ob eine Partei über bessere Möglichkeiten der Stellungnahme zu einem Sachverhalt verfügt, weil sie möglicherweise einen Wissensvorsprung hat.[590] Dies könnte gerade bei der Durchsetzung eines Auskunftsrechts eines Betroffenen relevant werden, da dieser gerade mangels

[586] Baldus, S. 349; Hofmann, S. 239, Harings, S. 340 f.
[587] Grabenwarter, in: Ehlers, § 6 Rn. 43.
[588] Satzger, § 11 Rn. 70.
[589] EGMR, Urteil vom 23.06.93 – *Ruiz-Mateos./.Spanien*, § 63; EGMR, Urteil vom 22.07.03 – *Edwards & Lewis./.Vereinigtes Königreich*, §§ 50 ff.
[590] EGMR, Urteil vom 23.06.93 – *Ruiz Mateos./.Spanien*, § 67.

Akteneinsicht niemals die Möglichkeit hat, etwaige Verletzungen, unrichtige Informationen etc. vorzubringen. Dies bringt letztlich auch Art. 6 III lit. a) EMRK zum Ausdruck. Bei Verweigerung der Akteneinsicht müssen entsprechende verfahrensrechtliche Garantien dennoch den Anspruch auf ein faires Verfahren sicherstellen.[591] Denn ohne diese Möglichkeit kann der Betroffene bspw. einen Zeugen gar nicht befragen (vgl. Art. 6 III lit. d) EMRK). Ausreichende Zeit zur Vorbereitung ist nur notwendig, wenn auch die erforderlichen Unterlagen vorhanden sind, d.h. es ist die Gelegenheit zur Vorbereitung zu geben (vgl. Art. 6 III lit. b) EMRK).

Des Weiteren kann aus dem Recht auf ein faires Verfahren auch ein Recht auf Begründung von Entscheidungen abgeleitet werden, wobei das Ausmaß der Begründungen vom konkreten Verfahren abhängt. Allerdings dürfte klar sein, dass bei Ermessensentscheidungen eine erhöhte Begründungsobliegenheit besteht.[592]

c) ART. 10 EMRK

Art. 10 EMRK gewährleistet u.a. die „Freiheit, Informationen und Ideen ohne behördliche Eingriffe und ohne Rücksicht auf Staatsgrenzen zu empfangen und weiterzugeben". Dementsprechend könnte sich hieraus auch die Möglichkeit ergeben, aus Art. 10 EMRK Zugang zu Informationen über vorhandene Daten betreffend die eigene Person zu erlangen. Allerdings verneint die Rechtsprechung ein solches Recht aus Art. 10 EMRK. Art. 10 EMRK gewähre dem Einzelnen in diesem Zusammenhang „weder ein Recht auf Zugang zu einem Register,

[591] EGMR, Urteil vom 19.06.01 – *Atlan./.Vereinigtes Königreich*;, §§ 40 f.; EGMR, Urteil vom 16.02.00 – *Rowe und Davis./.Vereinigtes Königreich*, § 61.
[592] Grabenwarter, in: Ehlers, § 6 Rn. 44.

das Daten über seine Person enthält, noch verpflichtet er die Regierung, dem Einzelnen solche Daten zur Verfügung zu stellen".[593]

d) ART. 13 EMRK

Im Gegensatz zu Art. 6 EMRK ist Art. 13 EMRK nur akzessorisch zur Verletzung eines Konventionsrechts anwendbar, d.h. es muss die Verletzung eines anderen Konventionsrechts behauptet werden, wobei aber nicht erforderlich ist, dass eine Verletzung des anderen Rechts auch tatsächlich vorliegt.[594]

Art. 13 EMRK statuiert das Recht auf eine wirksame Beschwerde, d.h. *„jede Person, die in ihren in dieser Konvention anerkannten Rechten oder Freiheiten verletzt worden ist, hat das Recht, bei einer innerstaatlichen Instanz eine wirksame Beschwerde zu erheben (...)"*.

Art. 13 gewährt keinen gerichtlichen Rechtsschutz, gefordert wird nur, dass es einen Anspruch auf Zugang und Entscheidung gibt und dass die Entscheidung eine wirksame Abhilfemöglichkeit bietet, sei es die Aufhebung einer Maßnahme oder eine Entschädigung.[595] Für die Effektivität der Beschwerdestelle sind die im Verfahren vorgesehenen Garantien, der Zugang der Beschwerdestelle zu allen Daten, Unparteilichkeit und Unabhängigkeit maßgeblich.[596] Es reicht auch, wenn „die Gesamtheit der im innerstaatlichen Recht zur Verfügung

[593] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 74.
[594] EGMR, Urteil vom 27.04.88 – *Boyle & Rice./.Vereinigtes Königreich,* § 52*;* EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 77; EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, § 64.
[595] EGMR, Urteil vom 25.03.83 – *Silver./.Vereinigtes Königreich*, § 113; EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 77.
[596] EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, §§ 67 ff.; EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 83; EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, § 67.

stehenden Beschwerdemöglichkeiten (…) den Anforderungen des Art. 13 [genügt], auch wenn eine einzelne Beschwerdemöglichkeit für sich genommen nicht ausreichend sein“[597] mag. Die Beschwerdestelle kann auch eine Verwaltungsbehörde oder ein anderes Kontrollgremium[598] sein, d.h. es muss sich nicht notwendigerweise um ein Gericht handeln.

Die Zugänglichkeit darf nicht durch übermäßig hohe Kosten oder unüberwindbare Verfahrenshindernisse eingeschränkt sein.[599]

Die Beschwerde muss nicht bereits während einer Maßnahme gegeben sein. Vielmehr reicht hier schon eine objektive Kontrolle durch eine Beschwerdeinstanz aus; nach Abschluss der Ermittlungen muss aber eine Beschwerdemöglichkeit vorhanden sein, damit der Betroffene die Maßnahme überprüfen lassen kann, gerade bei geheimen Maßnahmen.[600] Insbesondere bei der Weitergabe von Daten reicht die nachträgliche Kontrolle aus, sofern diese die Maßnahme nachträglich beseitigen kann.[601] Da gerade bei strafprozessualen Maßnahmen eine Überprüfung erst später stattfindet, hat der EGMR hierzu entschieden, dass auch danach noch ein Rechtsschutzbedürfnis gegeben ist.[602] Der Betroffene hat dann – z. B. im deutschen Recht – beim Zivilgericht Schadensersatz geltend zu machen bzw. die Vernichtung von Unterlagen zu verlangen. Letzten Endes kann dann auch das Verfassungsgericht eingeschaltet werden.[603]

---

597 EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, §§ 77, 84.
598 Heselhaus/Nowak, § 51 Rn. 16.
599 EGMR, Urteil vom 19.06.01 – *Kreuz./.Polen*, § 66.
600 EGMR, Urteil vom 04.05.00 – *Rotaru./.Rumänien*, § 69; EGMR, Urteil vom 06.09.78 – *Klass u.a./.BRD*, § 71; Eser, in: Wolter/Schenke/Hilger/Ruthig/Zöller, Art. 8 EMRK S. 308.
601 EGMR, Urteil vom 27.08.97 – *M.S./.Schweden*, § 55.
602 EGMR, Urteil vom 16.12.97 – *Camenzind./.Schweiz*, §§ 54 ff.
603 So auch EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, § 71.

Des Weiteren kann das Fehlen einer Benachrichtigung auch nicht zu einer Verletzung des Art. 13 EMRK führen, wenn schon gar keine Verletzung nach Art. 8 EMRK vorliegt. Die Konvention ist in ihrer Gesamtheit und damit als Einheit zu betrachten, weswegen zu Art. 13 EMRK keine andere Entscheidung ergehen kann als im Rahmen von Art. 8 EMRK.[604]

3. ZUSAMMENFASSUNG DER VERFAHRENSRECHTLICHEN GARANTIEN DER EMRK IM RAHMEN DES DATENSCHUTZES

Um auch hier einen Überblick über die relevante Rechtsprechung zu erlangen, werden die Vorgaben der EMRK in Bezug auf die verfahrensrechtlichen Garantien zunächst zusammengefasst.

Art. 8 EMRK gewährt ein Recht auf Zugang zu Informationen. Wird das Recht auf Zugang in Verbindung mit der Feststellung, dass in der Speicherung ein Eingriff liegt, geltend gemacht, ist eine normale Verhältnismäßigkeitsprüfung durchzuführen.[605] Wird das Recht auf Zugang zu Informationen isoliert geltend gemacht, so liegt ein Unterlassen vor, weswegen eine positive Verpflichtung des Staates vorhanden sein müsste. Eine Handlungspflicht des Staates ergibt sich jedoch nur dann, wenn der Staat durch die Sammlung oder Speicherung der Daten bereits vorweg tätig gewesen ist.[606] Die Anforderungen an das Bestehen einer positiven Verpflichtung sind damit höher als bei Geltendmachung eines Abwehranspruchs in Verbindung mit dem Begehren, Auskunft zu erteilen. Sollte dennoch eine positive Verpflichtung angenommen werden, so besteht ein großer Beurteilungsspielraum des Staates. Der Zugang zu Informationen kann aber auch beschränkt werden, bspw. zum

---

[604] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 78; EGMR, Urteil vom 06.09.78 – *Klass u.a./BRD*, § 68.
[605] EGMR, Urteil vom 26.03.87 – *Leander./.Schweden*, § 58 ff.
[606] EGMR, Urteil vom 07.07.89 – *Gaskin./.Frankreich,* § 49.

Wohl des Betroffenen[607]. Lückenhafte Auskünfte wurden von der Kommission teilweise ebenfalls für gerechtfertigt erachtet[608] ebenso wie eine Verweigerung der Auskunft, wenn es sich bei den gewollten Daten nur um solche einer kurzen Lebensspanne handelte[609]. Des Weiteren ist eine unabhängige Beschwerdemöglichkeit vorzusehen.[610] Die Kommission hat ferner die Möglichkeit eines Löschungsanspruchs bedacht, diesen im Endeffekt in dem Fall *Chave née Julien./.Frankreich* jedoch verneint, da die Daten nicht allgemein zugänglich gewesen seien und allein dem Wohl der Beschwerdeführerin dienten. Z. T. hat die Kommission einen Anspruch auf Löschung auch deshalb verneint, weil eine Sperrung von Daten ausreichenden Schutz biete.[611] Im Rahmen der Verhältnismäßigkeit ist eine Abwägung der Interessen des Betroffenen und Interessen anderer, insbesondere auch Dritter, vorzunehmen.

Art. 6 EMRK gewährt zunächst in Bezug auf gerichtliche Verfahren des ordentlichen Rechtswegs ein Recht auf Zugang zu einem Gericht. Dies bedeutet, dass die Zuständigkeit, die Organisation und die Zusammensetzung des Gerichts gesetzlich geregelt sein müssen. Verweisungen an Gerichte anderer Staaten stellen eine Beschränkung von Art. 6 EMRK dar. Die Gerichte müssen außerdem eine effektive Kontrollbefugnis haben sowie unabhängig und unparteiisch sein. Unabhängigkeit bedeutet Unabsetzbarkeit, Unversetzbarkeit für eine gewisse Dauer und Weisungsfreiheit; Unparteilichkeit muss sowohl in subjektiver als auch in objektiver Hinsicht (z.B. durch Verfahrensvorschriften, Organisation etc.) gegeben sein. Des Weiteren besteht gem. Art. 6 EMRK ein Recht

607 EKMR, Entscheidung vom 28.02.96 – *Martin./.Vereinigtes Königreich*, § 1.
608 EKMR, Entscheidung vom 05.04.95 – *Martin./.Schweiz,* DR 81-B, 136 (139 f.).
609 EKMR, Entscheidung vom 28.02.96 –*Martin./.Vereinigtes Königreich*, § 1; im Gegensatz dazu *Gaskin./.Frankreich*.
610 EGMR, Urteil vom 24.09.02 – *M.G./.Vereinigtes Königreich,* § 32.
611 EKMR, Entscheidung vom 05.04.95 – *Martin./.Schweiz*, DR 81-B, 136 (139).

auf ein faires Verfahren. Dies beinhaltet den Grundsatz der Waffengleichheit, d.h. jede Partei muss ihren Fall ohne Benachteiligung gegenüber der anderen vortragen können, was auch den Zugang zu entsprechenden Informationen voraussetzt. Des Weiteren beinhaltet das Recht auf ein faires Verfahren den Anspruch auf rechtliches Gehör. Eine Einschränkung des Art. 6 EMRK ist diesbezüglich nur möglich, sofern ein legitimes Ziel verfolgt wird und die Maßnahmen hierzu verhältnismäßig sind.

Art. 13 EMRK gibt dem Betroffenen die Möglichkeit, im Fall einer Verletzung eines Konventionsrechts eine Beschwerdeinstanz anzurufen, welche nicht notwendigerweise ein Gericht sein muss. Diese Instanz muss eine wirksame Abhilfemöglichkeit bieten können. Für die Effektivität der Instanz sind die verfahrensrechtlichen Garantien, der Zugang der Beschwerdestelle zu allen Informationen, Unabhängigkeit und Unparteilichkeit ausschlaggebend. Dem Gerichtshof reicht es dabei aus, wenn alle möglichen Beschwerdestellen in ihrer Gesamtheit die Anforderungen erfüllen. Die Zugänglichkeit zur Beschwerdestelle darf dabei nicht eingeschränkt sein (z.B. durch hohe Kosten oder unüberwindbare Verfahrenshindernisse). Ferner reicht es aus, wenn erst nach Abschluss der Ermittlungen eine Beschwerdemöglichkeit vorhanden ist, was gerade bei geheimen Maßnahmen nicht anders möglich ist.

4. PRÜFUNG AM MASSSTAB DER GARANTIEN DER EMRK MIT DEN EPASS-REGELUNGEN UND DEM PRÜMER RATSBESCHLUSS

a) UMSETZUNG DER VERFAHRENSRECHTLICHEN GARANTIEN DER EMRK BEIM EPASS

Art. 8 EMRK gewährt ein Recht auf Zugang zu den Informationen, insbesondere wenn der Staat durch die Speicherung der Daten bereits vorweg tätig gewesen ist.[612] In der Verordnung 2252/2004 steht hierzu nichts geschrieben. Aus diesem Grund sind hierfür die Mitgliedstaaten selbst zuständig. Diese haben durch die Umsetzung der Datenschutzrichtlinie 95/46/EG (s. auch nachfolgendes Kapitel) dem Betroffenen gem. Art. 12 ein Auskunftsrecht zu gewähren. Wie dies geschieht, ist Sache der Mitgliedstaaten. In Deutschland wird dies durch entsprechende Lesegeräte, welche in den Meldeämtern zur Verfügung stehen, gewährleistet. Der Einzelne kann dort unter Mitwirkung des Personals seine Daten einsehen. Die Mitwirkung des Personals ist eine zulässige Beschränkung bzw. Ausgestaltung zur Gewährleistung der ordnungsgemäßen Anwendung der Geräte und garantiert auch dem Einzelnen, dass kein anderer als der Inhaber des Ausweises seine Daten überprüfen und einsehen kann.

Des Weiteren sind die Garantien des Art. 6 EMRK einzuhalten. Art. 6 EMRK ist anwendbar, sofern vom Betroffenen Schadensersatzansprüche gegen den Staat geltend gemacht werden. Da in der ePass-Verordnung keine Regelungen zum Rechtsschutz getroffen wurden, gilt das nationale Recht, wobei davon auszugehen ist, dass dieses die Voraussetzungen des Art. 6 EMRK erfüllt.

[612] EGMR, Urteil vom 07.07.89 – Gaskin./.Frankreich, § 49.

Art. 13 EMRK gibt im Falle einer Konventionsrechtsverletzung das Recht auf eine wirksame Beschwerde. Das Vorliegen einer Beschwerdeinstanz ergibt sich wiederum nicht aus den Vorschriften der Verordnung 2252/2004, sondern aus der Datenschutzrichtlinie 95/46/EG, welche von den Mitgliedstaaten umzusetzen war. Nach Art. 28 IV der Richtlinie kann sich jede Person an die Kontrollstelle wenden. Gemäß der Richtlinie 95/46/EG sind verfahrensrechtliche Garantien der Kontrollstelle vorgesehen, wie Zugang zu Daten und Recht auf Einholung aller erforderlichen Informationen sowie Einwirkungsbefugnisse in Form von Anordnungsmöglichkeiten hinsichtlich der Sperrung, Löschung oder Vernichtung von Daten. Des Weiteren hat die Kontrollstelle ein Klagerecht, vgl. hierzu Art. 28 III der Richtlinie. Gemäß Art. 28 II der Richtlinie walten die Kontrollstellen in völliger Unabhängigkeit. Ferner steht gegen Entscheidungen der Beschwerdestelle der Rechtsweg offen, vgl. Art. 28 III a.E. der Richtlinie. Die Richtlinie wurde in allen Mitgliedstaaten umgesetzt. In Deutschland existiert daher ein unabhängiger Datenschutzbeauftragter sowohl auf Landes- als auch auf Bundesebene. Ferner gibt es behördliche Datenschutzbeauftragte, um z.B. die datenschutzrechtlichen Garantien in den Meldebehörden durchzusetzen.

b) UMSETZUNG DER VERFAHRENSRECHTLICHEN GARANTIEN DER EMRK BEIM PRÜMER RATSBESCHLUSS

Art. 8 EMRK gewährt dem Einzelnen zur Wahrung seines Rechts auf Privatleben ein Recht auf Zugang zu seinen Daten. Das Recht auf Zugang kann theoretisch isoliert geltend gemacht werden, da den Staat aufgrund seiner vorherigen Sammlung und Speicherung der DNA- und daktyloskopischen Daten eine positive Handlungspflicht trifft. Dennoch besteht nach der Rechtsprechung ein großer Beurteilungsspielraum des Staates, ob er einen solchen

Zugang gewährt, insbesondere kann der Zugang beschränkt werden. Art. 31 I S. 1 Prümer Ratsbeschluss gewährt einen solches Recht auf Zugang zu Informationen, behält sich aber gem. Art. 31 I S. 4 Prümer Ratsbeschluss vor, das Auskunftsrecht einzuschränken. Des Weiteren sieht Art. 31 I S. 3 Prümer Ratsbeschluss entsprechend der Rechtsprechung eine unabhängige Beschwerdemöglichkeit vor. Darüber hinaus sehen Art. 30 I S. 2 sowie Art. 28 I S. 3, III UAbs. 1 Prümer Ratsbeschluss Löschungsvorschriften und Art. 28 II und III UAbs. 2 Prümer Ratsbeschluss Kennzeichnungs- und Sperrungsvorschriften vor. Eine Einschränkung dieser Rechte ist im Prümer Ratsbeschluss nicht vorgesehen, wäre aber dennoch zur Verfolgung der in Art. 8 II EMRK genannten legitimen Ziele gerechtfertigt.

Art. 6 EMRK ist anwendbar im Rahmen von Streitigkeiten über Schadensersatzansprüche gegen den Staat, d.h. auch im Rahmen des Amtshaftungsanspruchs nach Art. 34 GG, § 839 BGB, sowie über die zur Beschuldigung führenden Maßnahmen, d.h. auch DNA- und Fingerabdruck-Abgleiche. Art. 6 EMRK gewährt einem Betroffenen Zugang zu einem unabhängigen und unparteiischen Gericht, was in der Regel durch die nationalen Rechtsordnungen sichergestellt wird. Der Betroffene hat die Wahl bzgl. seines Gerichtsstandes, wobei er sich in der Regel an das Gericht seines Heimatstaates wenden wird. Des Weiteren ist dem Betroffenen der Zugang zu den Informationen zu gewähren, da er sich nur so verteidigen kann. Bei Verweigerung des Akteneinsichtsrechts ist dies nicht möglich. Dann muss es aber möglich sein, dass eine unabhängige Kontrollinstanz eingeschaltet wird, welche eine Überprüfung vornimmt und im Rahmen des Gerichtsverfahrens die fehlende Kenntnis des Betroffenen ersetzt, ohne den Betroffenen zu informieren. Auch sind Ablehnungsentscheidungen zu begründen, um dem Betroffenen die Möglichkeit zur Stellungnahme zu geben.

Art. 13 EMRK gewährt dem Betroffenen die Möglichkeit, eine Beschwerdeinstanz anzurufen, welche eine wirksame Abhilfemöglichkeit bietet, unabhängig und unparteilich ist sowie Zugang zu allen relevanten Informationen besitzt. Art. 31 I S. 3 Prümer Ratsbeschluss gewährt einem Betroffenen ebenfalls eine Beschwerdemöglichkeit. Sofern ein Gericht angerufen wird, hat dieses nach dem Prümer Ratsbeschluss unparteilich und unabhängig i.S.d. Art. 6 I EMRK zu sein. Aufgrund des Standorts dieser Vorschrift im Kapitel über Datenschutzvorschriften ist davon auszugehen, dass alle Staaten, welche eine Übermittlung vornehmen, diese Voraussetzung erfüllen. Ferner besteht die Möglichkeit, eine unabhängige Kontrollinstanz anzurufen. Diese unabhängige Kontrollinstanz gemäß der Datenschutzrichtlinie besitzt ausreichende Zugangsmöglichkeiten zu Informationen. Fraglich ist, ob aufgrund der mangelnden Einwirkungsbefugnis auf Behörden anderer Mitgliedstaaten eine Verletzung des Art. 13 EMRK gegeben ist. Zudem besteht die Möglichkeit, seine Rechte auch in einem anderen Mitgliedstaat geltend zu machen. Der Betroffene wird jedoch mangels Kenntnis der Sprache und des Verfahrens seine Rechte nur schwerlich durchsetzen können. Grundsätzlich ist die Kombination beider Beschwerdemöglichkeiten nach dem Gerichtshof ausreichend, welcher entschieden hat, dass die Beschwerdemöglichkeiten in ihrer Gesamtheit den Anforderungen entsprechen müssen, wenn es sich um innerstaatliche Einwirkungsbefugnisse handelt. Dann ist Art. 13 EMRK eingehalten worden. Geht es hingegen um staatenübergreifende Einwirkungsbefugnisse, muss der Betroffene Hindernisse zur Geltendmachung seiner Rechte hinnehmen, welche jedoch nicht mit Art. 13 EMRK vereinbar sind, insbesondere da das Vorliegen von Einwirkungsbefugnissen fraglich ist.

5. FAZIT

Es wurde festgestellt, dass Art. 8 EMRK auch Recht auf Zugang zu Informationen gewährt. Da der Staat sowohl beim ePass als auch nach dem Prümer Ratsbeschluss bereits durch die Speicherung der Daten tätig gewesen ist, trifft ihn eine positive Handlungspflicht. Nach der ePass-Verordnung sowie nach dem Prümer Ratsbeschluss wird dem Betroffenen ein Recht auf Auskunft über seine Daten gewährt. Aufgrund des bestehenden Beurteilungsspielraums darf dieses Auskunftsrecht eingeschränkt werden. Ferner sieht der Prümer Ratsbeschluss Löschungs- und auch Kennzeichnungsvorschriften vor und wird damit dem Art. 8 EMRK gerecht. Die ePass-Verordnung enthält ebenfalls ein Recht auf Löschung und Berichtigung.

Art. 6 EMRK ist sowohl beim ePass als auch beim Austausch nach dem Prümer Ratsbeschluss anwendbar. Beim ePass werden die Rechte des Art. 6 EMRK im Rahmen eines Schadensersatzverfahrens durch das nationale Recht sichergestellt. Beim Prümer Ratsbeschluss sind die Rechte des Art. 6 EMRK ebenfalls im Schadensersatzverfahren relevant und außerdem bei der Überprüfung der Rechtmäßigkeit der Verarbeitung von DNA- und Fingerabdruck-Daten. Problematisch ist letztlich nur die Möglichkeit, dass dem Betroffenen aufgrund gesetzlicher Ausnahmen keine Auskunft gewährt wird. Damit würde dem Betroffenen das Recht auf Waffengleichheit genommen. Letztlich wird die Auskunftsverweigerung im Rahmen dieser gesetzlichen Ausnahmetatbestände jedoch gerechtfertigt sein, da in der Regel das Ziel, bspw. um strafrechtliche Ermittlungen nicht zu gefährden, dieser Verweigerung übergeordnet ist. In diesem Fall könnte jedoch eine Kontrollinstanz eingesetzt werden.

Auch die Anforderungen des Art. 13 EMRK wurden gewahrt. Sowohl beim ePass als auch beim Austausch nach dem Prümer

Ratsbeschluss liegt eine Verletzung des Art. 8 I EMRK nahe (siehe auch oben Teil B. Pkt. B. I.), weswegen der Anwendungsbereich des Art. 13 EMRK eröffnet ist. Da die Mitgliedstaaten der EU die Datenschutzrichtlinie umgesetzt haben, ist davon auszugehen, dass eine unabhängige und unparteiliche Beschwerdeinstanz zur Verfügung steht, welche zudem ausreichende innerstaatliche Einwirkungsbefugnisse besitzt. Geht es hingegen um staatenübergreifende Einwirkungsbefugnisse, so wird der Rechtsschutz nicht dem des Art. 13 EMRK entsprechen, insbesondere da solche Befugnisse nach dem Prümer Ratsbeschluss nicht vorhanden sind. Beim Prümer Ratsbeschluss ergibt sich zudem die Möglichkeit der Inanspruchnahme eines Gerichts entsprechend den Vorgaben des Art. 6 I EMRK, vgl. Art. 31 I S. 3 Prümer Ratsbeschluss.

II. DIE VERFAHRENSRECHTLICHEN VORGABEN DER DSK UND DER EMPFEHLUNG R (87) 15

Die DSK und die Empfehlung R (87) 15 stellen konkrete verfahrensrechtliche Regelungen im Bereich des Datenschutzes auf. Diesen Vorgaben müssen sowohl der ePass als auch die Prümer Regelungen gerecht werden. Aus diesem Grund werden im Folgenden zunächst die Regelungen zusammenfassend – wie bereits in Punkt B. – dargestellt und anhand dieser Ausführungen ein Vergleich mit den Regelungen des ePasses und dem Prümer Ratsbeschluss daraufhin wird vorgenommen. Aus den bereits in Punkt B. II. genannten Gründen erfolgt auch hier wieder eine ausführliche Darstellung aller Regelungen.

1. DIE REGELUNGEN DER DSK UND DER EMPFEHLUNG R (87) 15

Art. 8 DSK gewährt dem Betroffenen zusätzlichen Schutz, welcher jedoch – im Einklang mit dem Charakter der DSK als non self-executing Abkommen – von den Vertragsstaaten auszugestalten ist. V.a. Art. 8 lit. a) und b) DSK normieren den Grundsatz der Transparenz, wodurch es dem Betroffenen ermöglicht werden soll, zu erkennen, welche Daten wann, von wem, wie und wo gespeichert werden. Gem. Art. 9 Abs. 2 DSK sind jedoch die Ausnahmen und Einschränkungen des Art. 9 DSK auch auf Art. 8 DSK anzuwenden. Ferner sieht Art. 11 DSK vor, dass Sanktionen und Rechtsmittel für die entgegen den Vorschriften verarbeitenden Stellen festzulegen sind. Art. 13 ff. DSK regeln ferner die gegenseitige Hilfeleistung, insbesondere zum Zweck der Sicherstellung eines Betroffenen-Rechtsschutzes. Ferner sind nach dem Zusatzprotokoll zur DSK Kontrollstellen einzurichten.

a) RECHT AUF KENNTNIS DER DATEI, DER ZWECKE DER DATEI SOWIE DES VERANTWORTLICHEN

Nach Art. 8 lit. a) DSK muss jeder die Möglichkeit haben, von einer vorhandenen Datei Kenntnis zu nehmen sowie ihre Zwecke und die Bezeichnung festzustellen. Des Weiteren muss der Sitz des Verantwortlichen feststellbar sein. Die Bekanntgabe kann innerstaatlich durch Veröffentlichung des Verantwortlichen in öffentlichen Registern oder durch Mitteilung auf Anfrage geschehen.[613] Möglich ist natürlich auch die Bekanntgabe durch den Datenverarbeiter selbst, wobei dies allerdings aufgrund des

[613] CoE, Explanatory Report, ETS No. 108, Nr. 51.

enormen Aufwands nur in Ausnahmefällen gerechtfertigt sein wird.[614]

Ebenso bestimmt Principle 1.4 der Rec. R (87) 15, dass dauerhafte Dateien der Aufsichtsbehörde bekanntgegeben werden müssen. Die Benachrichtigung umfasst die Art der einzelnen Datei, den Verantwortlichen, die Zwecke der Datei, die Arten der zu verarbeitenden Daten sowie die Empfänger. Die Aufsichtsbehörde wiederum hat gem. Principle 6.1 Maßnahmen zu ergreifen, um sicherzustellen, dass die Öffentlichkeit über die Existenz von Dateien sowie über ihre diesbezüglichen Rechte informiert wird.

b) RECHT AUF AUSKUNFT

Die Konvention gewährt in Art. 8 lit. b) jedem das Recht, eine Mitteilung darüber zu erhalten, ob Daten über ihn gespeichert sind, und sofern dies der Fall ist, dass ihm diese Daten auch in verständlicher Art und Weise mitgeteilt werden. Diese Mitteilung ist Voraussetzung für die Geltendmachung der weiteren Ansprüche und dient zusammen mit Art. 8 lit. a) DSK der Transparenz. Von Art. 8 lit. b) DSK wurde jedoch nicht festgelegt, welche Angaben der Antrag enthalten muss. Denklogisch ergibt sich das jedoch aus der Notwendigkeit einzelner Angaben, ohne welche eine Auskunft aufgrund Verwechslungsgefahr ansonsten nicht möglich wäre. Dies sind im Einzelnen der Vor- und Zuname, das Geburtsdatum und die Anschrift. Zum Teil können auch spezifische Angaben, z.B. Versicherungsnummer, Personalnummer etc., gefordert werden, um die Suche zu vereinfachen. Weitere Angaben sind hierfür nach *Henke* jedoch nicht erforderlich, insbesondere nicht, welche Informationen der Antragsteller zu erhalten wünscht. Der Antragsteller habe nämlich oftmals gar

[614] S. auch Henke, S. 128 f.

keine Kenntnis davon, in welchen konkreten Einzeldateien (gerade bei Verbunddateien) seine Daten gespeichert sind oder in welchem Umfang Daten über ihn verarbeitet werden. Daher kann auch bspw. die Erklärung der Bundesrepublik Deutschland vom 29.09.1985[615], die zum Inhalt hat, dass einem nicht ausreichend spezifizierten Auskunftsverlangen gem. Art. 8 lit. b) DSK nicht entsprochen werden kann, nicht mehr verlangen als die eben angesprochenen Angaben.[616] Allerdings übersieht *Henke* dabei Art. 14 Abs. 3 DSK, welcher zwar nur eine Regelung im Rahmen der gegenseitigen Hilfeleistung trifft, wobei allerdings nicht davon auszugehen ist, dass der Europarat für inländische Personen andere Vorgaben trifft als für die in einem anderen Vertragsstaat der DSK lebenden Personen. Zum einen würde dies der vom Europarat angestrebten Vereinheitlichung entgegenstehen. Zum anderen ergibt sich dies schon aus dem Umkehrschluss (arg. e contrario). Es stellt sich dabei nämlich folgende Frage, deren Beantwortung sich bereits aus der Frage selbst ergibt: Der Betroffene soll trotz innerstaatlicher Bekanntmachung der nationalen Dateisammlungen weniger Angaben machen als derjenige, der Auskunft über Daten aus einem anderen Staat verlangt und dabei noch nicht einmal Kenntnisse über etwaige Dateisammlungen besitzt? Des Weiteren bestimmt Principle 2.2 der Rec. R (87) 15, dass ein Betroffener über die Datenerhebung zu informieren ist, wenn Daten ohne sein Wissen gesammelt und gespeichert wurden und sofern diese nicht gelöscht werden. Diese Benachrichtigung hat zu erfolgen, sobald die polizeiliche Aufgabenerfüllung dadurch voraussichtlich nicht mehr beeinträchtigt ist.

[615] BGBl. 1985 II Nr. 34, S. 1134 f.; so im Übrigen auch Malta.
[616] Henke, S. 137.

Eine solche Auskunft hat nach der DSK in angemessenen Zeitabständen und ohne übermäßige Kosten zu erfolgen. Der Explanatory Report zur DSK hat hierzu mehrere nationale Regelungen als denkbar erachtet. Demnach ist eine Mitteilung sowohl auf Anfrage des Betroffenen als auch auf Initiative des Verantwortlichen möglich. Des Weiteren steht es dem nationalen Gesetzgeber nach dem Report des Expertenkomitees auch offen, die Auskunft gebührenfrei, jedoch nur in festgelegten Zeitabständen zu erteilen oder andernfalls eine jederzeitige Mitteilung, dann allerdings nur gegen angemessenes Entgelt zu ermöglichen.[617] Etwas anders sieht dies *Henke*, der annimmt, dass die Auskunft generell nur in bestimmten Zeitabständen erfolgen kann und dass es dem Datenverarbeiter generell freistehe, Gebühren für die Auskunft zu erheben.[618] Beide Ansichten verfolgen jedoch wohl letztlich den Zweck, missbräuchliche sowie Massen-Anfragen zu verhindern.

Ebenso verlangt Principle 6.2 der Rec. R (87) 15, dass der Betroffene in Übereinstimmung mit den Regelungen des nationalen Rechts in angemessenen Intervallen und ohne übermäßige Verzögerung Zugang zur polizeilichen Datei, d.h. Auskunft, verlangen kann.

Art. 8 lit. a) DSK dient letztlich auch der Verteidigung des Einzelnen. So ist eine Auskunft bspw. Voraussetzungen dafür, dass auf die DNA-Analyse auch zu Zwecken der Verteidigung zurückgegriffen werden darf (vgl. auch Principle 5 der Rec. (92) 1)). So ist von den Ländern sicherzustellen, dass die DNA-Analyse als besonderes Beweismittel der Verteidigung gleichermaßen zugänglich ist; dies kann entweder durch richterliche Entscheidungen oder durch einen unabhängigen Sachverständigen erfolgen (vgl. Principle 9).

---

617 CoE, Explanatory Report, ETS No. 108, Nr. 53.
618 Henke, S. 138.

c) RECHT AUF BERICHTIGUNG UND LÖSCHUNG

Nach Art. 8 lit. c) DSK soll der Betroffene einen Anspruch auf Berichtigung bzw. Löschung haben, wenn die Daten entgegen den innerstaatlichen Vorschriften, welche die in Art. 5 und 6 DSK niedergelegten Grundsätze verwirklichen, verarbeitet wurden. Sowohl hinsichtlich des Auskunftsrechts als auch der in lit. c) genannten Rechte wurde nicht geregelt, bei wem der Betroffene die Rechte geltend machen kann. Allerdings ergibt sich aus dem Zweck der vorhergehenden Vorschrift des Art. 8 lit. a) DSK, dass eine mögliche Anlaufstelle der Dateiverantwortliche sein kann, da dieser ansonsten nicht feststellbar sein müsste. Der Explanatory Report zur DSK nennt ferner noch die Kontrollstelle als mögliche Auskunftsstelle.[619] Allerdings kann der DSK keine Pflicht dergestalt entnommen werden, dass der Verantwortliche sämtliche Datenempfänger über die Löschung oder Berichtigung informieren muss oder diese Maßnahmen gar veranlassen muss. Das Expertenkomitee hat in seinem Report lediglich festgestellt, dass dementsprechendes nationales Recht bereits existiere.[620] Da jedoch ein Berichtigungs- bzw. Löschungsanspruch allein in der Datei des Verantwortlichen dem Zweck des Art. 8 lit. c) DSK nicht genügt, wäre der Verantwortliche eigentlich zu verpflichten, solche Löschungen und Berichtigungen weiterzugeben. Nebenbei sei erwähnt, dass dies prinzipiell auch für die Mitteilung von Informationen gilt, welche über einen Dateiverbund verschiedenen Empfängern zur Verfügung stehen und von diesen weiterverarbeitet werden können. Entsprechend dem Gesamtkonzept der DSK wird auch im Rahmen des Art. 8 lit. c) DSK eine Verpflichtung erst angenommen, wenn Daten

[619] CoE, Explanatory Report, ETS No. 108, Nr. 52.
[620] CoE, Explanatory Report, ETS No. 108, Nr. 54; so auch Henke, S. 141.

gespeichert werden. Damit sind auch von der Rechtsschutzseite her manuelle Daten sowie Erfassungsvorgänge nicht erfasst.[621]

Auch gem. Principle 6.3 der Rec. R (87) 15 muss der Betroffene die Möglichkeit erhalten, eine Richtigstellung zu erlangen. Entsprechend den Bestimmungen der Empfehlung sind persönliche Daten zu löschen, zu korrigieren oder es ist ein richtigstellender Zusatz an das Datum anzufügen, sofern sich aufgrund der Ausübung des Auskunftsrechts herausstellt, dass Daten überschüssig, ungenau oder unwichtig sind. Die Löschung bzw. korrigierenden Maßnahmen haben sich auf alle Dokumente zu erstrecken und sofern dies nicht sofort möglich ist, hat die Löschung bzw. Korrektur spätestens bei der anschließenden Verarbeitung der Daten oder bei der nächsten Übermittlung zu erfolgen. Auch hier ist jedoch nichts dergestalt ersichtlich, dass der Datenverarbeiter eventuelle Datenempfänger über die Löschung und Berichtigung informieren muss. Allerdings ergibt sich in Verbindung mit Principle 5.5 ii., dass zumindest die Empfänger über unrichtige oder veraltete Daten informiert werden müssen. Die Löschung bzw. Berichtigung ist damit vom jeweiligen Empfänger vorzunehmen entsprechend Principle 6.3.

d) RECHT AUF EIN RECHTSMITTEL BEI UNZULÄSSIGER VERWEIGERUNG DER IN PKT. b) UND c) GENANNTEN RECHTE

Ferner soll der Betroffene nach Art. 8 lit. d) DSK ein Rechtsmittel zur Verfügung haben, wenn seinen Anliegen nach Auskunft oder Berichtigung und Löschung i.S.d. Art. 8 lit. b) und c) DSK nicht entsprochen wird. Dies kann sowohl eine unabhängige Beschwerdeinstanz sein als auch ein Rechtsmittel im Rahmen des

[621] S. Henke, S. 142.

normalen Instanzenzuges.[622] Allerdings enthält die DSK keine Regelung, wodurch der Verantwortliche verpflichtet würde, die Gründe für die Ablehnung mitzuteilen. Der Europarat hat dies jedoch als selbstverständlich erachtet und daher auf eine ausdrückliche Normierung verzichtet.[623]

Anders als in der DSK wurde in Principle 6.5 der Rec. R (87) 15 geregelt, dass die Ablehnung oder Beschränkung des Auskunftsrechts schriftlich begründet werden muss. Eine Mitteilung kann gem. Principle 6.5 nur dann unterbleiben, wenn dies für die Durchführung der polizeilichen Aufgabe unerlässlich oder zum Schutz der Rechte und Freiheiten anderer notwendig ist. Wenn das Auskunftsersuchen abgelehnt wurde, so soll der Betroffene gem. Principle 6.6 die Möglichkeit haben, sich bei der Aufsichtsbehörde oder einer anderen unabhängigen Institution zu beschweren; diese Behörde soll dann die Rechtmäßigkeit der Ablehnung überprüfen. Statt einer Aufsichtsbehörde kann dies auch durch ein Gericht geschehen.[624] Nach der Überprüfung muss dem Betroffenen nicht mitgeteilt werden, warum die Ablehnung rechtmäßig war; es reicht vielmehr, wenn ihm mitgeteilt wird, dass eine Überprüfung erfolgt ist und dass die Daten in Ordnung sind.[625]

e) WEITERE SANKTIONEN UND RECHTSMITTEL

Art. 10 DSK sieht vor, dass jede Vertragspartei zur Bereitstellung von geeigneten Sanktionen und Rechtsmitteln verpflichtet ist, um die „Verletzungen der Vorschriften des nationalen Rechts, welche die in [Kapitel II der DSK] (…) aufgestellten Grundsätze für den

622 S. Henke, S. 143.
623 Henke, S. 143; Unger, S. 55.
624 Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 94.
625 Committee of Ministers, Explanatory Memorandum zu Rec. R (87) 15, Nr. 95.

Datenschutz verwirklichen“ zu sanktionieren. Aufgrund des non self-executing-Charakters der DSK wird damit den Mitgliedstaaten die Wahl der Sanktionen und Rechtsmittel überlassen, wobei der Explanatory Report auch hierzu Anregungen beisteuert, indem er vorschlägt, solche Sanktionen auf zivil-, verwaltungs- und strafrechtlicher Ebene vorzusehen.[626]

f) GEGENSEITIGE HILFELEISTUNG

Nach Art. 13 DSK verpflichten sich die Staaten zur gegenseitigen Hilfeleistung. Damit soll die Durchsetzung subjektiver Rechte auch dann möglich sein, wenn die Daten in einem anderen Vertragsstaat verarbeitet werden.[627] Hierzu hat jede Vertragspartei eine zuständige Behörde zu bezeichnen sowie im Fall der Bezeichnung mehrerer Behörden die Zuständigkeiten festzulegen und bekanntzumachen. Die bezeichnete Behörde muss keine Datenschutzbehörde sein.[628] Vielmehr dient die Vorschrift des Art. 13 Abs. 2 DSK lediglich dazu, dem Betroffenen die Stelle, an die er sich wenden kann, erkennbar zu machen, ohne dass er sich lange mit den Zuständigkeitsregelungen des betreffenden Staates vertraut machen muss.[629] Diese Behörde soll dann Auskünfte über das Recht und die Verwaltungspraxis ihres Staates sowie Sachauskünfte über bestimmte Datenverarbeitungen erteilen, soweit dies nach dem innerstaatlichen Recht zulässig ist.

Nach Art. 14 DSK haben die gem. Art. 13 Abs. 2 DSK bezeichneten Behörden „Personen, die im Ausland wohnen, bei der Ausübung ihrer Rechte“ entsprechend den in Art. 8 DSK gemachten Vorgaben zu unterstützen. Damit sind sowohl Betroffene, welche

626 CoE, Explanatory Report, ETS No. 108, Nr. 60.
627 S. Henke, S. 177.
628 CoE, Explanatory Report, ETS No. 108, Nr. 73.
629 Henke S. 180.

in einem anderen Vertragsstaat wohnen, als auch Betroffene, welche in einem Drittstaat wohnen, angesprochen.[630] Betroffene können dementsprechend ihre Anträge direkt an den Vertragsstaat richten, in welchem die Daten verarbeitet werden, oder sich aber gem. Art. 14 Abs. 2 DSK indirekt durch Vermittlung des eigenen Staates an die bezeichnete Behörde des verarbeitenden Staates wenden.[631] Art. 14 Abs. 3 DSK legt ferner fest, welche Anforderungen an den Antrag des Betroffenen zu stellen sind. So hat er den Namen, die Anschrift und den verfolgten Zweck zu bezeichnen. Ferner sind „alle anderen für die Identifizierung des Antragstellers erheblichen Einzelheiten" anzugeben. Aufgrund dieser ungenauen Bezeichnung ist es natürlich möglich, dass der Antragsteller zu wenig oder unzweckmäßige Daten angibt und dadurch Gefahr läuft, dass der Antrag gem. Art. 16 lit. b) DSK abgewiesen wird, weil er nicht den Anforderungen der DSK entspricht. Allerdings wird man zu Gunsten der Rechtsschutzgarantie die Anzahl der erforderlichen Daten einschränken müssen, d.h. erheblich sind Name, Geburtsdatum, Nationalität, Anschrift und evtl. eine dem System immanente Nummer, die der Betroffene auch kennt (bspw. Personalnummer, Versicherungsnummer etc.).[632] Der gleiche Gedanke ist Art. 14 Abs. 3 lit. b) DSK zugrunde zu legen. Der Betroffene wird das System meistens nicht genau bezeichnen können, weshalb den bezeichneten Behörden in bestimmtem Maße zuzumuten ist, die Datei und den Verantwortlichen zu ermitteln.[633]

Art. 15 DSK soll dem Missbrauch durch die verarbeitenden und ersuchenden Behörden vorbeugen. Art. 15 DSK normiert daher in Abs. 1 den Grundsatz der Zweckbindung. Danach hat eine Behörde, welche Auskünfte erhalten hat, diese entsprechend den Zwecken

630 CoE, Explanatory Report, ETS No. 108, Nr. 77.
631 CoE, Explanatory Report, ETS No. 108, Nr. 78.
632 S. auch Henke, S. 187 f.
633 S. Henke, S. 188.

zu verwenden, welche der Auskunft zugrunde lagen. Die Vertragsparteien haben außerdem dafür zu sorgen, dass die Behörden bzw. deren handelnde Personen die Daten vertraulich behandeln. Dies kann durch Geheim-haltungserklärungen oder ähnliche Maßnahmen geschehen.[634] Ferner darf ein Antrag nach Art. 14 Abs. 2 DSK nicht ohne die Zustimmung des Betroffenen erfolgen.

Eine Behörde ist grundsätzlich verpflichtet, dem Antrag bzw. Ersuchen nachzukommen.[635] Um jedoch missbräuchliche Anfragen einzudämmen, kann gem. Art. 16 DSK ein Antrag nach Art. 14 DSK oder ein Ersuchen nach Art. 13 DSK abgelehnt werden, wenn die Beantwortung die Befugnisse der Behörde überschreiten würde oder wenn diese nicht den Bestimmungen der DSK entsprechen oder wenn die Beantwortung „mit der Souveränität, der Sicherheit oder der öffentlichen Ordnung der Vertragspartei [...] oder mit den Rechten und Grundfreiheiten der Personen, die der Gerichtsbarkeit dieser Vertragspartei unterstehen, nicht vereinbar wäre". Die Aufzählung der Ausnahmen ist erschöpfend.[636] Unter die Ausnahmeregelung des Art. 16 lit. b) DSK fallen neben der zu Art. 14 DSK angesprochenen Ausnahme u.a. Rechtshilfeersuchen anderer als der in Art. 13 Abs. 2 DSK bezeichneten Behörden sowie die Verweigerung von Auskünften hinsichtlich Dateien, welche entsprechend Art. 3 Abs. 2 lit. a) DSK vom Anwendungsbereich der Konvention ausgenommen werden.[637]

Art. 17 DSK regelt, dass für die Hilfe nach Art. 13 DSK bzw. für die Unterstützung nach Art. 14 DSK keine Kosten erhoben werden dürfen, mit Ausnahme von Sachverständigen- und Dolmetscherkosten. Letztere dürfen jedoch nicht höher sein als für

[634] Henke, S. 190.
[635] Henke, S. 191.
[636] CoE, Explanatory Report, ETS No. 108, Nr. 80.
[637] S. Henke, S. 191 f.

Personen, die im Hoheitsgebiet der ersuchten Vertragspartei wohnen. Die sonstigen Auslagen und Kosten sind dann von der Vertragspartei zu tragen, zu welcher die ersuchende Behörde gehört. Weitere Einzelheiten, d.h. Form und Verfahren, sind unmittelbar zwischen den Vertragsparteien festzulegen.

g) EINRICHTUNG VON KONTROLLSTELLEN

Das Zusatzprotokoll zur DSK sieht in Art. 1 die Einrichtung von Kontrollstellen vor. Nach dessen Abs. 1 sind die Kontrollstellen für die Einhaltung der Maßnahmen zuständig, damit die in den Kapiteln II und III der DSK und im Zusatzprotokoll zur DSK genannten Grundsätze verwirklicht werden. Abs. 1 verfolgt damit zwei Ziele. Zum einen soll dadurch ein effektiver Schutz des Einzelnen sichergestellt werden. Dies erfordert die Bereitstellung notwendiger technischer und personeller Mittel. Zum anderen soll damit auch eine bessere Harmonisierung der Regelungen erreicht werden, womit nicht nur eine Verbesserung der Datenschutzstandards, sondern auch eine engere Kooperation zwischen den Vertragsstaaten bewirkt werden soll.[638] Ebenso sieht Principle 1.1 der Rec. R (87) 15 die Einrichtung von Kontrollstellen außerhalb der Polizeibehörden vor, welche die Einhaltung der Bestimmungen der Empfehlung sicherstellen soll.

Nach Art. 1 Abs. 2 DSK-ZP haben die Kontrollstellen Untersuchungs- und Einwirkungsbefugnisse, ein Klagerecht und eine Anzeigebefugnis bei Verstößen sowie die Kompetenz, von Betroffenen mit der Wahrnehmung ihrer Rechte beauftragt zu werden. Im Rahmen der Einwirkungsbefugnisse hat die Kontrollstelle zahlreiche Möglichkeiten, u.a. kann sie entweder eigenständig oder auf Gesuch des Betroffenen den

[638] CoE, Explanatory Report, ETS No. 181, Nr. 8 ff.

Datenverantwortlichen zwingen, unrichtige oder rechtswidrig erlangte Daten zu korrigieren, zu löschen oder zu zerstören. Die Kontrollstelle kann ferner verfügen, dass die angeforderten Informationen innerhalb angemessener Zeit erteilt werden. Des Weiteren kann sie u.a. Stellungnahmen zur Anwendung von Datenverarbeitungsvorgängen abgeben. So ist sie gem. Principle 1.3 der Rec. R (87) 15 auch zu befragen, wenn die Einführung von automatisierten Dateien Fragen zur Anwendung der Empfehlung R (87) 15 aufwirft. Die Kontrollstelle muss außerdem die Befugnis haben, die Öffentlichkeit durch regelmäßige Berichte, Veröffentlichung oder Stellungnahmen, etc. zu informieren.[639] Darüber hinaus hat sie als Vermittler zwischen dem Betroffenen und dem Datenverarbeiter zu fungieren.[640] Die in Art. 1 Abs. 2 DSK-ZP aufgeführten Kompetenzen der Kontrollstelle sind jedoch nicht abschließend.[641]

Nach Art. 1 Abs. 3 DSK-ZP nehmen die Kontrollstellen „ihre Aufgaben in völliger Unabhängigkeit wahr". Diese Unabhängigkeit kann durch zahlreiche Elemente sichergestellt werden, u.a. durch den Aufbau der Kontrollstelle, das Verfahren der Ernennung, die Dauer der Ausübung und die Bedingungen der Beendigung ihrer Funktion, die Bereitstellung hinreichender Mittel sowie die Verabschiedung von Verfügungen.[642] Letztere sind jedoch nicht als Gegenstand einer externen Anordnung oder gar Vorschrift zu sehen, sondern sollen vielmehr einen Rahmen für die Arbeit der Kontrollstelle bieten.

Nach Art. 1 Abs. 4 DSK-ZP steht „gegen beschwerende Entscheidungen der Kontrollstellen (...) der Rechtsweg offen". Diese Vorschrift soll die Rechtsstaatlichkeit des Verfahrens vor der

[639] CoE, Explanatory Report, ETS No. 181, Nr. 13.
[640] CoE, Explanatory Report, ETS No. 181, Nr. 14.
[641] CoE, Explanatory Report, ETS No. 181, Nr. 16.
[642] CoE, Explanatory Report, ETS No. 181, Nr. 17.

Kontrollstelle gewährleisten, insbesondere wenn die Kontrollstelle keine eigenen richterlichen Befugnisse hat.[643]

Nach Art. 1 Abs. 5 DSK-ZP haben die Kontrollstellen in Übereinstimmung mit den Vorschriften zur „Gegenseitigen Hilfeleistung" in der DSK „für die zur Erfüllung ihrer Kontrollaufgaben notwendige gegenseitige Zusammenarbeit, insbesondere durch den Austausch sachdienlicher Informationen" zu sorgen. Diese verstärkte Zusammenarbeit soll es den Betroffenen erleichtern, ihre Rechte nicht nur national, sondern auch international durchzusetzen, was insbesondere aufgrund des verstärkten grenzüberschreitenden Datenaustausches erforderlich ist.[644]

2. BEWERTUNG DES EPASSES ANHAND DER DSK

a) RECHTE DES BETROFFENEN

Art 8 lit. a) DSK wird gewahrt. Der Betroffene erhält durch die Verordnung und die entsprechenden Gesetze Kenntnis von den Zwecken des ePasses, vgl. Art. 4 III der Verordnung 2252/2004, wonach die biometrischen Daten nur verwendet werden dürfen, um die Authentizität des Passes zu prüfen und die „Identität des Inhabers [...] zu überprüfen" sowie entsprechend den Zwecken des Art. 7 II Schengener Grenzkodex zu überprüfen, ob der Pass gestohlen, missbräuchlich verwendet, abhanden gekommen oder für ungültig erklärt wurde und ob durch den Betroffenen eine „tatsächliche, gegenwärtige und erhebliche Gefahr für die innere Sicherheit, die öffentliche Ordnung, die internationalen Beziehungen zu den Mitgliedstaaten oder die öffentliche Ordnung"

643 CoE, Explanatory Report, ETS No. 181, Nr. 18 f.
644 CoE, Explanatory Report, ETS No. 181, Nr. 20.

gegeben ist. Kenntnis von den Überprüfungsmöglichkeiten erhält der Betroffene ebenfalls durch die Verordnung. Der Sitz des Verantwortlichen ist in der Verordnung nicht geregelt. Dieser ergibt sich vielmehr aus den Zuständigkeitsverteilungen der Mitgliedstaaten. Für den Fall der Gewährung des Auskunftsrechts und des Rechts auf Berichtigung und Löschung sind wohl aufgrund der Sachnähe die ausstellenden Behörden die Verantwortlichen (Arg. siehe oben in Teil D Pkt. B. II. 2. a).

Des Weiteren haben die Passinhaber gem. Art. 8 lit. b) DSK einen Anspruch auf Auskunft darüber, ob Daten gespeichert sind und auf Mitteilung dieser Daten. Gemäß Art. 4 I der Pass-Verordnung hat jeder das Recht darauf, die Daten im Pass zu überprüfen. Genaueres wird nicht geregelt. Dies wird vielmehr durch die Mitgliedstaaten in eigener Verantwortung vorgenommen. In Deutschland steht den Passinhabern hierfür ein Lesegerät in den Meldeämtern zur Verfügung, mit dem man unter Aufsicht des Personals die Daten auslesen kann.

Ebenso steht dem Passinhaber gem. Art. 4 I Pass-Verordnung ein Recht auf Berichtigung und Löschung zu, so dass Art. 8 lit. c) DSK ebenfalls Genüge getan wurde. Dieses Recht steht insbesondere dann zu, wenn die Daten unrichtig sind, z.B. bei Veränderungen der persönlichen Daten wie Name, Wohnort etc. Diese können einfach im Chip geändert werden. Problematisch ist es, wenn das Lichtbild nicht mehr zutrifft. Einfache Veränderungen wie Bartwuchs etc. sind nicht änderungsbedürftig. Sollte sich jedoch aufgrund von Schönheits- oder Unfallchirurgie eine Veränderung ergeben, so müsste dies auch im Pass aufgenommen werden. Fraglich ist derzeit immer noch, wer hierfür dann die Kosten trägt. Dies müsste im Einzelfall geklärt werden. Selbst die deutsche „Allgemeine Verwaltungsvorschrift zur Durchführung des

Passgesetzes“[645] enthält hierzu keine Angaben. Die Kosten wird aber wohl der Passinhaber tragen müssen, da dem Staat keine Kosten auferlegt werden können, die er nicht vorhersehen kann und die insbesondere nicht in seinen Verantwortungsbereich fallen. Selbst wenn den Passinhaber kein Verschulden trifft (wie bspw. bei unfallchirurgisch behandelten Gesichtern), so liegt es in seinem Verantwortungsbereich, den Pass zu erneuern, um den Ausreisebestimmungen gerecht zu werden. Berichtigungen können aber auch aufgrund altersbedingter Veränderungen erforderlich werden. Statt einer Berichtigung könnte man in solchen Fällen jedoch die Falschakzeptanzrate erhöhen und zwar jeweils im Verhältnis zum Alter des ePasses. Dies könnte vom System automatisch durchgeführt werden.

Dem Betroffenen soll ferner ein Rechtsmittel zustehen, wenn seinem Recht auf Auskunft, Berichtigung oder Löschung nicht entsprochen wird. Hierzu muss gem. Art. 8 lit. d) DSK eine unabhängige Beschwerdeinstanz oder ein Rechtsmittel im Rahmen des normalen Instanzenzuges vorhanden sein. Die Mitgliedstaaten erfüllen sämtlichst die Voraussetzungen der Datenschutzrichtlinien 95/46/EG, wonach in solchen Fällen ein Datenschutzbeauftragter angerufen werden kann, vgl. Art. 28 IV der Richtlinie, bzw. wonach bei Gericht ein Rechtsbehelf eingelegt werden kann, vgl. Art. 22 der Richtlinie. Sofern es sich um Maßnahmen im Rahmen der Strafverfolgung handelt, ist der ordentliche Rechtsweg gegeben.[646] Außerdem ist dem Betroffenen der Hinweis zu erteilen, dass er sich an eine unabhängige Instanz, in Deutschland wäre dies der Datenschutzbeauftragte, wenden kann.

[645] Gemeinsames Ministerialblatt vom 23.12.2009, Nr. 81, S. 1685 ff.
[646] Vollkommer, S. 70.

b) WEITERE SANKTIONEN UND RECHTSMITTEL

Gem. Art. 10 DSK sind zudem Sanktionen und Rechtsmittel vorzusehen. Hierzu gehört auch ein Schadensersatzanspruch, in Deutschland existiert bspw. ein Amts-haftungsanspruch nach Art. 34 GG, § 839 BGB. Wenn infolge unrichtiger Daten beim Enrolement die Verifikation fehlschlägt und infolgedessen die Aus- bzw. Einreise verweigert oder verzögert wird, entsteht dem Passinhaber ein Schaden, der zu ersetzen ist, egal ob der Fehler von der verifizierenden oder von der ausstellenden Behörde verursacht wurde. Der Betroffene sollte dann ein Wahlrecht haben, wen er in Anspruch nimmt, da ihm nicht aufgelastet werden kann, die Ursache des Fehlers zu finden. [647] Leider ist ein solcher Anspruch der ePass-Verordnung nicht zu entnehmen und daher Sache der Mitgliedstaaten, weswegen es zu divergierenden Regelungen kommen kann. In Deutschland ist ein Schadensersatzanspruch aufgrund falscher Datenverarbeitung auch in §§ 7, 8 BDSG geregelt.

c) EINRICHTUNG VON KONTROLLSTELLEN

Gem. Art. 1 des Zusatzprotokolls zur DSK sind Kontrollstellen einzurichten. Dies entspricht wiederum Art. 28 I der Datenschutzrichtlinie, welche von allen Mitgliedstaaten umgesetzt wurde. Den Kontrollen stehen entsprechend Art. 1 II DSK-ZP Zugangsbefugnisse und Untersuchungsbefugnisse in Form eines Rechts auf Einholung entsprechender Informationen sowie die in Art. 28 III der Richtlinie genannten Einwirkungsbefugnisse zu, namentlich u.a. Befugnis zur Anordnung der Löschung, Sperrung oder Vernichtung und die Befugnis zur Abgabe von Stellungnahmen. Die Kontrollstellen sind gem. Art. 1 III DSK-ZP als

[647] Meuth, S. 58.

unabhängige Stellen einzurichten, was auch von der Datenschutzrichtlinie verlangt wird, vgl. Art. 28 I. Ebenso hat gem. Art. 1 IV der Rechtsweg offen zu stehen, was auch in Art. 28 III der Richtlinie niedergelegt ist. Die Mitgliedstaaten erfüllen in Umsetzung der Datenschutzrichtlinie automatisch auch die Vorgaben des Art. 1 DSK-ZP.

3. BEWERTUNG DES PRÜMER RATSBESCHLUSSES ANHAND DER DSK UND DER EMPFEHLUNG R (87) 15

a) RECHTE DES BETROFFENEN

Art. 8 lit. a) DSK verlangt, dass der Betroffene von der Datei, den Zwecken der Datei und dem Verantwortlichen Kenntnis erlangen kann. Da die Datei aufgrund ihrer dezentralen Struktur eine nationale Datei bleibt, gelten auch die dementsprechenden nationalen Bestimmungen, d.h. sowohl der Verantwortliche als auch die Datei als auch die Zwecke der Datei sind im innerstaatlichen Recht festzulegen. Dies ist auch so in Art. 31 I S.1 Prümer Ratsbeschluss festgelegt worden. Nach Principle 1.4 der Rec. R (87) 15 sind dauerhafte Dateien der Aufsichtsbehörde bekanntzugeben, welche wiederum gem. Principle 6.1 die Öffentlichkeit über die Existenz der Dateien informieren muss. Grundsätzlich wird hier keine neue dauerhafte Datei errichtet; vielmehr wird eine vorhandene Datei mit anderen vorhandenen Dateien vernetzt. Eine Ausnahme ist dann gegeben, wenn die Mitgliedstaaten bislang noch keine solche DNA-Datei erstellt hatten, was nach dem Wortlaut der Art. 2 I Prümer Ratsbeschluss durchaus möglich ist. Hinsichtlich der daktyloskopischen Daten geht der Prümer Ratsbeschluss davon aus, dass solche Dateien in jedem Mitgliedstaat bereits existieren, vgl. Wortlaut des Art. 8 Prümer Ratsbeschluss. Trotz der Tatsache, dass nur ein Zusammenschluss der Dateien erfolgt, ist das Generalsekretariat über die nationalen DNA-Analyse-Dateien zu informieren, vgl. Art.

2 III Prümer Ratsbeschluss. Über diese Erklärungen wird die Öffentlichkeit jedoch nicht informiert. Aus diesem Grund ist davon auszugehen, dass das Generalsekretariat nicht die Aufgaben der Aufsichtsbehörde wahrnimmt. In diesem Fall entspricht der Prümer Ratsbeschluss nicht den Bestimmungen der Principle 1.4 und 6.1 der Rec. R (87) 15.

Art. 8 lit. b) DSK sowie Principle 6.2 der Rec. R (87) 15 gewähren dem Einzelnen ein Recht, Auskunft über die zu seiner Person gespeicherten Daten zu erhalten. Diese Auskunft muss in verständlicher Form und ohne dass übermäßige Kosten erhoben werden, mitgeteilt werden. Art. 31 I S.1 Prümer Ratsbeschluss gewährt dem Betroffenen ein solches Recht auf Auskunft über die zu seiner Person gespeicherten Daten, deren Herkunft und den Empfänger. Da der empfangende Mitgliedstaat den übermittelnden Mitgliedstaat über die Verarbeitung der übermittelten Daten und deren Ergebnisse unterrichtet (vgl. Art. 32 Prümer Ratsbeschluss), ist der Betroffene auch hierüber zu informieren. Des Weiteren kann der Betroffene gem. Art. 30 V S. 2 Prümer Ratsbeschluss verlangen, dass die Rechtmäßigkeit der Verarbeitung von Daten zu seiner Person geprüft wird. Dass die Auskunft ohne übermäßige Kosten sowie in allgemein verständlicher Form und ohne zumutbare Verzögerung zu erfolgen hat, wurde ebenfalls in Art. 31 I S. 1 Prümer Ratsbeschluss festgehalten. Art. 8 lit. b) DSK ist letztlich auch unter dem Licht der Waffengleichheit zu betrachten, d.h. der Betroffene muss von seinen Daten Kenntnis erlangen, damit er sich angemessen verteidigen kann, vgl. ebenso Principle 5 und 9 der Rec. (92) 1. Aus diesem Grund ist es gerechtfertigt, die Informationen des Art. 32 Prümer Ratsbeschluss in die Auskunft miteinzubeziehen. Dieses Auskunftsrecht kann nach Art. 9 II DSK zum Zwecke der Verfolgung von Straftaten eingeschränkt werden. Eine solche Ausnahme sieht auch Art. 31 I S. 2 Prümer Ratsbeschluss vor,

wonach sich die Gründe für die Einschränkung nach innerstaatlichem Recht richten. Eine Entscheidung hierüber ist gerichtlich nachprüfbar. Hierbei ist insbesondere zu beachten, dass keine Auskunft gewährt werden kann, wenn der Verantwortliche nicht ausreichend Daten zur Verfügung hat. So kann er durchaus zum Nachweis der Identität des Betroffenen eine beglaubigte oder polizeilich bestätigte Kopie eines Ausweises verlangen. Dies dient dem Schutz des Betroffenen und wird bspw. in Deutschland beim BKA so gehandhabt.[648]

Der Betroffene hat daneben gem. Art. 8 lit. c) DSK ein Recht auf Berichtigung bzw. Löschung seiner Daten, wenn die Daten entgegen den innerstaatlichen Vorschriften verarbeitet werden. Nach seiner Umsetzung zählt der Prümer Ratsbeschluss ebenfalls zu den innerstaatlichen Vorschriften, weshalb auch dessen Regelungen zu beachten sind. Art. 31 I S. 2 Prümer Ratsbeschluss gewährt dem Betroffenen ebenfalls ein solches Recht auf Berichtigung unrichtiger und Löschung unzulässig verarbeiteter Daten. Gerade Fingerabdruckdaten können sich im Laufe der Zeit durch Abnutzung, Alter, Unfall etc. verändern. Gem. Art. 28 I S. 2 Prümer Ratsbeschluss ist einem empfangenden Mitgliedstaat eine Mitteilung darüber zu machen, wenn ihm unrichtige oder solche Daten, welche nicht hätten übermittelt werden dürfen, übermittelt worden sind. Der empfangende Staat ist dann zur Berichtigung bzw. Löschung verpflichtet (s. auch Art. 28 III UAbs. 1 S. 1 Prümer Ratsbeschluss). Damit wurde mit Art. 28 I S. 2 und 3 Prümer Ratsbeschluss die Lücke geschlossen, welche in der DSK vorhanden war. Aber auch die empfangende Behörde hat die Pflicht zur Information der dateiführenden Stelle, wenn sich

[648] S. „Antwort der Bundesregierung auf die Kleine Anfrage BT-Drs. 16/14120 – Bilanz des Datenaustausches mit den Unterzeichnerstaaten des Prüm-Vertrages und Stand der Umsetzung des EU-Ratsbeschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Polizeizusammenarbeit“, BT-Drs. 16/14150 vom 22.10.2009, S. 7.

herausstellt, dass die übermittelten Daten unrichtig sind oder zu löschen wären, Art. 28 I S. 4, 5 Prümer Ratsbeschluss. Gem. Principle 6.3 der Rec. R (87) 15 besteht zusätzlich die Möglichkeit, einen richtigstellenden Zusatz an das Datum anzufügen, sofern die Daten überschüssig, ungenau oder unwichtig sind. Art. 28 II Prümer Ratsbeschluss enthält ebenfalls eine Regelung, wonach Daten, deren Richtigkeit bestritten wird und nicht feststellbar ist, zu kennzeichnen sind. Diese Kennzeichnung darf nur unter den in Art. 28 II S. 2 Prümer Ratsbeschluss genannten Bedingungen aufgehoben werden. Ferner sieht Art. 28 III UAbs. 2 auch die Möglichkeit einer Sperrung von Daten vor, wenn es Grund zu der Annahme gibt, dass durch die Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Dies kann bspw. dann vorliegen, wenn der Betroffene die Daten zum Zwecke seiner Verteidigung benötigt, aber möglicherweise die zulässigen Speicherungshöchstfristen abgelaufen sind. Aber auch wenn Zweifel an der Richtigkeit der Daten vorliegen (non liquet), sollte eine Sperrung erfolgen.

Dem Betroffenen steht gem. Art. 8 lit. d) DSK auch ein Recht auf ein Rechtsmittel bei einer unabhängigen Beschwerdeinstanz oder im Rahmen des normalen Instanzenzuges bei unzulässiger Verweigerung seiner in Art. 8 lit. b) und c) DSK gewährten Rechte zu. Dies wurde auch in Art. 31 I S. 3 Prümer Ratsbeschluss festgelegt. Jedoch wurde nicht festgelegt, an welches Gericht welchen Mitgliedstaates er sich wenden kann. Vielmehr besteht die Möglichkeit, dass der Betroffene sich den günstigsten Gerichtsstand auswählt. Dementsprechend kann gem. Art. 31 II Prümer Ratsbeschluss auch der Gerichtsstand bei der empfangenden Stelle herangezogen werden, sowohl zur Geltendmachung des Primäranspruchs als auch des Sekundäranspruchs. Die Einzelheiten des Verfahrens richten sich

gem. Art. 31 I S. 4 Prümer Ratsbeschluss nach innerstaatlichem Recht.

b) WEITERE SANKTIONEN UND RECHTSMITTEL

Gem. Art. 10 DSK sind die Mitgliedstaaten zur Bereitstellung von Sanktionen oder Rechtsmitteln im Falle der Verletzung der datenschutzrechtlichen Vorschriften verpflichtet. Solche Sanktionen fänden sich u.a. in Art. 21-23 Prümer Ratsbeschluss. Diese Artikel sind jedoch nach der Systematik des Beschlusses nur auf Kapitel 5, d.h. auf „Weitere Formen der Zusammenarbeit" beschränkt und damit für den Bereich des Abgleichs von DNA- und Fingerabdruckspuren nicht anwendbar. Damit sind nur die üblichen Rechtsmittel auf Überprüfung der Rechtsmäßigkeit der Datenverarbeitung gem. Art. 31 I S. 3 Prümer Ratsbeschluss vorhanden. Eine weitere Sanktion ist in Art. 31 II S. 2 Prümer Ratsbeschluss enthalten. Sind Daten bereits unrichtig übermittelt worden, hat die übermittelnde Stelle den Schaden zu erstatten, der der empfangenden Stelle aufgrund ihrer Haftung entstanden ist. Dies stellt aber lediglich die Erstattung eines Schadens eines anderen Mitgliedstaates dar. Ferner sieht Art. 31 I S. 3 Prümer Ratsbeschluss die Möglichkeit vor, Schadensersatz (aufgrund Staatshaftungsrecht) oder Abhilfe anderer Art gerichtlich geltend machen zu können. Beim Abgleich von DNA- und daktyloskopischen Daten mag zwar kein zivilrechtlicher Schaden entstehen, weswegen eine zivilrechtliche Haftung überflüssig wäre, allerdings fehlen sowohl strafrechtliche als auch disziplinarrechtliche Vorschriften. Werden bspw. personenbezogene Daten unrechtmäßig übertragen, so fehlt es hierzu an entsprechenden Vorschriften im Prümer Ratsbeschluss. Theoretisch wäre die Haftung nach innerstaatlichem Recht zu bestimmen. Dabei ist aber fraglich, ob jeder Staat einen staatshaftungsrechtlichen Anspruch bereitstellt. Gleiches wäre

zum Beispiel auch bei der Gewinnung von molekulargenetischem Material gem. Art. 7 Prümer Ratsbeschluss zu diskutieren; auch hier könnte eine unrechtmäßige Erhebung erfolgen, was wiederum nach nationalem Recht geltend zu machen wäre. Entsprechende Regelungen fehlen jedoch im Prümer Ratsbeschluss. Des Weiteren könnte man bei einer rechtswidrigen Datenerhebung bzw. -übermittlung ein Beweisverwertungsverbot anzunehmen.[649] Gerade bei einem derart gravierenden Austausch von Daten muss es Konsequenzen haben, wenn die Verfahrensvorschriften und die materiellen Voraussetzungen nicht eingehalten werden. Der Betroffene hat außerdem bspw. in Deutschland einen Schadensersatzanspruch nach § 7,8 BDSG sowie nach Art. 34 GG, § 839 BGB.

c) GEGENSEITIGE HILFELEISTUNG

Nach Art. 14 DSK haben die Behörden „Personen, die im Ausland wohnen, bei der Ausübung ihrer Rechte zu unterstützen", d.h. der Betroffene sollte seinen Antrag auch an die Behörde eines anderen Staates stellen können. Dies ist besonders wichtig für die Ausübung seiner Rechte aufgrund des Prümer Ratsbeschlusses. Art. 31 I S. 1 Prümer Ratsbeschluss regelt, dass der Betroffene einen Antrag gemäß innerstaatlichem Recht stellen kann, d.h. jedoch, dass der Betroffene sich an die innerstaatlichen Datenschutzbehörden wenden muss, da nur solche im innerstaatlichen Recht vorgesehen sind. Dies reicht allerdings aus, denn gem. Art. 32 Prümer Ratsbeschluss ist der übermittelnde, also der dateiführende Staat, über die Verarbeitung der übermittelten Daten und das erzielte Ergebnis zu informieren. Die dafür erforderliche Anfrage erfolgt dann im Rahmen des Auskunftsantrags. Somit wäre Art. 14 DSK nur ein zeitlich umfangreicher Umweg, den der Betroffene nicht gehen muss, da

[649] S. auch Gusy, VerwArch 74 (1983), 91 (104).

ihm alle Auskünfte im Rahmen seines innerstaatlichen Auskunftsanspruchs erteilt werden können. Weitere Vorschriften zur gegenseitigen Hilfeleistung sind im Prümer Ratsbeschluss nicht zu finden.

d) EINRICHTUNG VON KONTROLLSTELLEN

Art. 1 I DSK-ZP verlangt die Einrichtung von Kontrollstellen. Nach Principle 1.1 der Rec. R (87) 15 sollen diese außerhalb der Polizeibehörden eingerichtet werden. Art. 30 III und V sowie Art. 31 I S. 3 Prümer Ratsbeschluss setzen das Bestehen einer unabhängigen Datenschutzbehörde voraus. Insbesondere ist zu beachten, dass alle Mitgliedstaaten auch die Datenschutzrichtlinie 95/46/EG zu beachten haben, in welcher die Einrichtung von unabhängigen Kontrollstellen vorgeschrieben ist. Art. 1 II DSK-ZP sichert den Kontrollbehörden umfangreiche Untersuchungs- und Einwirkungsbefugnisse zu. Auch Art. 30 III und V UAbs. 1 S. 1 und 3 Prümer Ratsbeschluss geben den Datenschutzbehörden solche Befugnisse an die Hand. Die Datenschutzbehörden haben demnach Zugriff auf die Protokolldaten und können diese kontrollieren. Des Weiteren kann die Datenschutzbehörde eine Datenschutzbehörde eines anderen Mitgliedstaates um die Ausübung ihrer Befugnisse ersuchen. Im Prümer Ratsbeschluss wurde hingegen nicht geregelt, welche Einwirkungsbefugnisse die Datenschutzbehörde hat. Auch hier ist daher wiederum auf die Datenschutzrichtlinie zu verweisen, welche sicherstellt, dass die Mitgliedstaaten entsprechende Einwirkungsbefugnisse vorzusehen haben. Dennoch fehlen Regelungen, wonach die Datenschutzbehörden Einwirkungsbefugnisse auf die Behörden anderer Mitgliedstaaten haben, z.B. um Berichtigungs- oder Löschungsansprüche durchsetzen zu können. Dazu reicht nicht die bloße Regelung des Art. 30 V UAbs. 2 S. 3 Prümer Ratsbeschluss. Die Unabhängigkeit der Datenschutzbehörden gem. Art. 1 III DSK-ZP wird unterstellt, wie sich aus dem Wortlaut der

Art. 30 III UAbs. 1 S. 1 und Art. 31 I S. 3 Prümer Ratsbeschluss ergibt. Das Vorliegen eines Rechtsweges gegen beschwerende Entscheidungen der Kontrollstellen (d.h. bspw. bei Ablehnung des Antrags auf Auskunft) gem. Art. 1 IV DSK-ZP ergibt sich nicht aus dem Wortlaut des Prümer Ratsbeschlusses. Zwar kann sich der Betroffene gem. Art. 31 I S. 3 Prümer Ratsbeschluss im Falle der Verletzung seiner Datenschutzrechte an ein Gericht oder an eine Kontrollstelle i.S.d. Datenschutzrichtlinie wenden. Allerdings zeigt die Formulierung „oder", dass nur eine Möglichkeit besteht. Sollte dies vom Gesetzgeber gewollt sein, so ist dies zu wenig. Vielmehr muss auch gegen beschwerende Entscheidungen der Kontrollstelle der Rechtsweg offen stehen. Sollte dies jedoch inbegriffen sein, so sollte der Gesetzgeber dies klarstellen. Nach Art. 1 V DSK-ZP sollen die Kontrollstellen zusammenarbeiten. Art. 30 V UAbs. 2 S. 4 Prümer Ratsbeschluss verlangt ebenfalls die gegenseitige Zusammenarbeit der Kontrollstellen; damit wurde Art. 1 V DSK-ZP beachtet.

4. FAZIT

Art. 8 lit. a) DSK wird nach den vorangegangenen Darstellungen sowohl durch den Prümer Ratsbeschluss als auch durch die ePass-Verordnung gewahrt. Beide geben sowohl das Bestehen als auch die Zwecke der Datei bekannt. Der Verantwortliche wird jeweils durch das innerstaatliche Recht (bspw. in Deutschland durch das BKAG) bzw. durch die Praxis bestimmt, d.h. durch die Sachnähe der Behörden. Allerdings wurden beim Prümer Ratsbeschluss weder Principle 1.4 noch 6.1 der Rec. R (87) 15 eingehalten, da er keine Regelungen enthält, wonach neu einzurichtende Dateien der Aufsichtsbehörde bekanntzugeben sind, damit diese die Öffentlichkeit unterrichten kann.

Allerdings wird sowohl durch den Prümer Ratsbeschluss als auch durch die ePass-Verordnung dem Betroffenen ein Recht auf Auskunft über seine Daten gewährt. Wie dies geschieht, bleibt den Mitgliedstaaten überlassen. Einschränkungen, wie bspw. ein Nachweis über die Identität des Anfragenden, sind gem. § 9 II DSK gerechtfertigt.

Ebenso haben die Betroffenen nach beiden Rechtsgrundlagen ein Recht auf Berichtigung und Löschung. Fraglich ist beim ePass nur, wer die Kosten einer solchen Berichtigung zu tragen hat. Dies wird in der Regel der Betroffene sein, weshalb problematisch ist, ob das Recht auf Berichtigung mit Kosten verbunden sein darf. Da die DSK hierzu jedoch keine Vorgaben enthält, kann man auch nicht davon ausgehen, dass dies unverhältnismäßig ist. Außerdem ist Folgendes zu berücksichtigen: wenn man nach der DSK für die Auskunft die Erstattung eines geringen Kostenaufwands verlangen kann, so müsste dies auch für die Berichtigung möglich sein. Statt Berichtigung des Passes bestünde auch die Möglichkeit einer Erhöhung der FAR. Der Prümer Ratsbeschluss erfüllt zudem auch Principle 6.3 der Rec. R (87) 15, wonach ein richtigstellender Zusatz zu einer Information möglich ist. Der Prümer Ratsbeschluss stellt hierfür die Möglichkeit einer Kennzeichnung bzw. Sperrung bereit.

Dem Betroffenen steht entsprechend Art. 8 lit. d) DSK sowohl nach dem Prümer Ratsbeschluss als auch beim ePass ein Rechtsmittel zur Verfügung. Dies ergibt sich schon aus der Umsetzung der Datenschutzrichtlinie.

Nach Art. 10 DSK sind die Mitgliedstaaten zur Bereitstellung von Sanktionen und Rechtsmitteln verpflichtet. Dies gilt auch für den ePass. Hier wurde jedoch überhaupt nichts festgelegt, obwohl ein Schadensersatzanspruch durchaus notwendig gewesen wäre; dieser richtet sich daher nach innerstaatlichem Recht. Ebenso fehlen Vorschriften zur strafrechtlichen und disziplinarrechtlichen

Verantwortlichkeit. Im Prümer Ratsbeschluss wurde die Möglichkeit von Schadensersatzansprüchen ausdrücklich festgehalten. Allerdings fehlen auch hier sowohl strafrechtliche als auch disziplinarrechtliche Vorschriften. Jedoch ist hierbei auch zu beachten, dass den Mitgliedstaaten aufgrund des Grundsatzes der Subsidiarität die eigenständige Ausgestaltung ihrer Rechtsordnung obliegt. Problematisch ist dies nur, sofern ein Staat keine Regelung hierzu trifft, da dann aufgrund der fehlenden Abschreckungswirkung eine Missbrauchsneigung erhöht werden könnte. Wie bereits oben in Teil D. B. I. 4. b) ausgeführt, sollte daher zumindest das „Ob" einer strafrechtlichen und/oder disziplinarrechtlichen Verantwortlichkeit in der ePass-Verordnung und im Prümer Ratsbeschluss festgelegt werden. Ebenso ist zu überlegen, ob sich infolge rechtswidriger Datenerhebung bzw. -übermittlung ein Beweisverwertungsverbot ergeben könnte.

Vorschriften zur gegenseitigen Hilfeleistung wurden weder in der ePass-Verordnung noch im Prümer Ratsbeschluss geregelt. Der Prümer Ratsbeschluss macht jedoch zumindest die Vorschrift des Art. 14 DSK obsolet durch seine – auch staatenübergreifenden – Informationsrechte. Beim ePass ist fraglich, ob solche Vorschriften überhaupt benötigt werden, da nur der Passinhaber im Besitz des ePasses ist und in anderen Mitgliedstaaten keine Datenspeicherung stattfindet.

Betreffend Art. 1 DSK-ZP wurde festgestellt, dass für den ePass alle Voraussetzungen vorliegen, insbesondere aufgrund der Umsetzung der Datenschutzrichtlinie. Auch hinsichtlich des Prümer Ratsbeschlusses liegen die wesentlichen Voraussetzungen vor. Allerdings mangelt es an Einwirkungsbefugnissen auf die Behörden anderer Mitgliedstaaten. Des Weiteren ergibt sich aus dem Prümer Ratsbeschluss nicht, dass gegen beschwerende Entscheidungen der Kontrollstelle der Rechtsweg offen steht. Diesbezüglich gibt es jedoch in Art. 28 III der Datenschutzrichtlinie eine Regelung,

welche von den Mitgliedstaaten des Prümer Ratsbeschlusses zu beachten ist.

III. ZWISCHENERGEBNIS

Die verfahrensrechtlichen Vorgaben des Völkerrechts sind durch die ePass-Verordnung und den Prümer Ratsbeschluss weitgehend erfüllt.

Sowohl der ePass als auch der Prümer Ratsbeschluss erfüllen die verfahrensrechtlichen Voraussetzungen, welche von der Rechtsprechung in den Art. 6, 8 und 13 EMRK festgestellt wurden. Somit besteht nach Art. 8 EMRK sowohl ein Auskunft- als auch ein Löschungsrecht. Ebenso sind durch die beiden Rechtsvorschriften die Vorgaben des Art. 13 EMRK insoweit erfüllt, als eine unabhängige und unparteiliche Kontrollinstanz besteht, welche ausreichende innerstaatliche Einwirkungsbefugnisse hat. Will der Betroffene dagegen staatenübergreifende Einwirkungsbefugnisse umsetzen, so ist dies mangels des Bestehens solcher Befugnisse nicht möglich und daher nicht mit Art. 13 EMRK vereinbar. Dass es nach dem Prümer Ratsbeschluss noch die Möglichkeit der Anrufung eines Gerichts gibt, löst dieses Problem nicht, sondern stellt vielmehr ein Mehr an Rechtsschutzmöglichkeit dar.

Im Vergleich des Prümer Ratsbeschlusses mit der DSK und den Empfehlungen stellten sich mehrere Mängel heraus. So wurden weder Principle 1.4 noch 6.1 der Rec. R (87) 15 eingehalten, da keine Regelungen existieren, wonach die Dateien einer Aufsichtsbehörde bekanntgegeben werden müssen, damit diese die Öffentlichkeit informieren kann. Des Weiteren mangelt es an Vorschriften zur strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit und damit an der Umsetzung des Art. 10 DSK. Auch stellt sich die Frage eines Beweisverwertungsverbots, sofern Daten unrechtmäßig übermittelt oder verarbeitet wurden. Vorschriften zur Hilfeleistung sind nicht zu finden. Ferner fehlt es bereits an – und dies wurde

auch schon im Bereich der Rechtsprechung angesprochen – Einwirkungsbefugnissen auf die Behörden anderer Mitgliedstaaten, wenn Daten staatenübergreifend verarbeitet werden.

Der ePass weist hingegen nur wenige Mängel auf. So wäre in der ePass-Verordnung die Regelung eines Schadensersatzanspruches oder die Regelung strafrechtlicher und disziplinarrechtlicher Verantwortung erforderlich gewesen, was einen Verstoß gegen Art. 10 DSK darstellt.

D. ERGEBNIS

Ungeachtet der zahlreichen Mängel (vgl. Zwischenergebnisse Pkt. B. III. und C. III.) wurden viele völkerrechtliche Bestimmungen beachtet, insbesondere der ePass hat hierbei gut abgeschnitten. Nicht zu vergessen ist auch, dass gerade die Änderung der ePass-Verordnung einige Mängel behoben hat. Im Gegensatz war der Prümer Ratsbeschluss nur ein „Schnellschuss", der genau genommen die Vorschriften des Vertrags von Prüm übernommen hat. Jedoch sollte letzterer eigentlich als Vorlage gelten, anhand deren Umsetzung überprüft wird, ob die Bestimmungen des Vertrages ausreichen oder ob noch Verbesserungen angestrebt werden müssen.

Verbesserungen sind tatsächlich auf mehreren Ebenen notwendig. Am wichtigsten ist jedoch die Aufstellung eines Straftatenkataloges, nach welchem die Gewinnung und Untersuchung molekulargenetischen Materials bzw. der Abruf von DNA-Profilen oder daktyloskopischen Daten von bestimmten Straftaten abhängen. Hierzu reicht es nicht aus, dass dem Täter eine negative Prognose in dem Sinne ausgestellt wurde, dass er voraussichtlich eine Wiederholungstat begehen wird. Es reicht auch nicht aus, wenn er bereits eine Wiederholungstat begangen

hat, denn man muss sich die Frage stellen: Ist es wirklich vertretbar, wenn ein Abgleich von DNA-Profilen und daktyloskopischen Daten bereits bei Ladendiebstählen oder gar Beleidigungen zulässig ist? Leider ist das derzeit gängige Praxis.

Ferner wäre es ein Leichtes gewesen, Vorschriften zur strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit festzulegen oder zumindest festzulegen, dass solche Regelungen zu treffen sind. Dass der Rat grundsätzlich daran gedacht hat, lässt sich anhand der Art. 22 f. Prümer Ratsbeschluss erkennen. Warum also nicht auch für den Abgleich/Abruf bzw. die Übermittlung von Daten? Darüber hinaus fehlen Vorschriften zu einer festen Aufbewahrungszeit der Daten, aufgrund weswegen Großbritannien die DNA-Profile bislang unbegrenzt aufbewahrt hat.[650] Da die Empfehlung (92) 1 nicht verbindlich ist, fehlen außerdem Bestimmungen zu den Anforderungen an die Laboratorien, welche die DNA untersuchen. Auch diese Anforderungen sollten vereinheitlicht werden, um ein hohes Maß an Sicherheit und Richtigkeit der DNA-Ergebnisse sicherzustellen.

Ferner wäre manchmal eine genauere Formulierung wünschenswert gewesen, so z.B. in Art. 26 I Prümer Ratsbeschluss, der sehr vage ausgedrückt ist. Dieser müsste v.a. die Zwecke erkennen lassen, für welche die personenbezogenen Daten noch verwendet werden dürften. Es dürfte kein Problem darstellen, diese Zwecke im Rahmen der Verhinderung und Verfolgung von Straftaten zu belassen.

Da ein automatisierter Abgleich stattfindet, liegt es in der Natur der Sache, dass eine vorherige Qualitätsüberprüfung der Daten nicht möglich ist. Es ist auch nicht ausreichend, dass die empfangende Behörde die Qualität überprüft, da diese die Richtigkeit und Aktualität gar nicht überprüfen kann. Aus diesem

[650] Koydl, „Englische Sammelwut“ vom 06.12.2008.

Grund sollte die sachnähere, nämlich die dateiführende Behörde die Überprüfung vornehmen. Dies kann entweder bereits bei der Speicherung der Daten oder vor Übermittlung des Fundstellendatensatzes geschehen.

Für das Problem der mangelnden staatenübergreifenden Einwirkungsbefugnisse ergibt sich ebenfalls ein Lösungsansatz. Nach dem Prümer Ratsbeschluss stellen die Datenschutzbehörden der Mitgliedstaaten die zur Erfüllung ihrer Kontrollaufgaben notwendige Zusammenarbeit sicher, vgl. Art. 30 V UAbs. 2 S. 4 Prümer Ratsbeschluss. Würde man darin eine Verpflichtung zur gegenseitigen Zusammenarbeit bzw. zur Auskunft festschreiben, so wäre damit nicht nur das Problem der fehlenden staatenübergreifenden Einwirkungsbefugnisse, sondern auch das Fehlen einer Regelung entsprechend Art. 13 DSK gelöst. Darüber hinaus wäre der Prümer Ratsbeschluss damit mit Art. 13 EMRK vereinbar.

Eine weitere Frage stellt sich nach dem Beweisverwertungsverbot. In den USA gilt der Grundsatz, dass rechtswidrig erlangte Daten nicht verwertet werden dürfen. Warum besteht also nicht auch dann ein Verwertungsverbot, wenn Daten unrechtmäßig übermittelt oder unrechtmäßig abgeglichen werden? Oder muss erst die Rechtsprechung ein solches Verwertungsverbot ausformen?

Abschließend ist zum Austausch nach dem Prümer Ratsbeschluss zu bemerken, dass ein solcher durchaus einen Sinn ergibt und wie die Statistiken zeigen, auch zu den gewünschten Ergebnissen führt. Gerade aufgrund des immer weiter zusammenwachsenden Europas ist ein solcher Austausch der Polizeibehörden sogar wünschenswert. Allerdings sollten dabei nicht die wesentlichen Bestimmungen zum Schutz des Einzelnen missachtet werden. Was aber auch zu berücksichtigen ist und was leider aufgrund der

Abneigung gegen den Datenschutz oftmals vergessen wird, ist die Tatsache, dass nur bei einer ordnungsgemäßen Ermittlung sämtliche Beweise vor Gericht Bestand haben und dass die Arbeit der Polizeibehörden nur dann erfolgversprechend ist.

Auch beim ePass wären Vorschriften zur strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit notwendig gewesen. Es kann durchaus sein, dass eine Kontrolle des ePasses durchgeführt wird, ohne dass dies gesetzlich festgelegt wird. Der Betroffene sollte nicht rechtelos gestellt werden. Es ist außerdem im Sinne der Polizeibehörden, Missbrauchsfälle zu vermeiden, damit die Seriosität ihrer Arbeit nicht in Frage gestellt wird.

Ferner stellt sich die Frage, warum keine Templates im ePass verarbeitet werden. Seit Jahren werden daktyloskopischen Daten in den Dateien der Polizeibehörden verarbeitet, welche nicht nur Bilddateien enthalten, sondern aufgrund ihrer automatisierten Suchfunktion auch Templates enthalten müssen. Warum wurde also bei der Erstellung der ePass-Verordnung kein vernünftiges Template-Verfahren festgelegt.

Letztlich bleibt nur noch sicherzustellen, dass bei der Ausstellung des ePasses die Vorlage ordnungsgemäßer Dokumente verlangt wird und dass die Sicherung der Daten durch regelmäßige Checks, geschultes Personal sowie durch Maßnahmen gegen unbefugtes Auslesen verbessert wird.

Zum Schluss bleibt noch die Frage offen, warum kein einheitliches Verbot der Speicherung der Daten in einem Register festgelegt wurde. Jede Person muss sich einen Ausweis besorgen, weswegen die Passbehörden umfangreiche Informationen und Daten über eine Person zur Verfügung haben. Wie lange wird es dauern, bis – auch in Deutschland – Fingerabdrücke gespeichert werden und diese den Polizeibehörden zur Verfügung stehen, ohne dass hierfür

eine richterliche Genehmigung etc. erforderlich ist und ohne dass der Betroffene erfährt, dass seine Daten verwendet werden?

Trotz aller Kritik, die dem ePass bei dessen Einführung entgegengebracht wurde, erfüllt er schlussendlich in etwa die völkerrechtlichen Voraussetzungen.

TEIL E Ausblick

I. WEITERE BIOMETRISCHE MERKMALE DER ZUKUNFT

1. IRISERKENNUNG

Die Iris besteht u.a. aus Muskeln. Die Funktion der Iris liegt in der Regulierung des Lichteinfalls, d.h. ist es zu hell, zieht sie sich zusammen; ist es zu dunkel, weitet sie sich, damit mehr Licht ins Auge einfallen kann. Die Form und die Augenfarbe sind genetisch bedingt. Die Muster, auf die es bei der Iriserkennung ankommt, sind hingegen individuell. Die Bildung dieser Muster beginnt bereits im dritten Schwangerschaftsmonat. Ein chirurgischer Eingriff zur Veränderung der Iris ist zu gefährlich, um tatsächlich durchgeführt zu werden, da das Gewebe hierfür zu fein ist.[651]

Da die Iris eine niedrige Falscherkennungsrate hat und sehr unterscheidungskräftig ist, ist sie als biometrisches Merkmal sehr geeignet. Ferner ist die Iriserkennung sehr stabil, da diese bereits in den ersten Lebensjahren ausgeprägt ist.[652]

Die Farbe der Iris hängt von Anzahl der Pigmente, d.h. dem Melanin, ab. Je mehr Melanin vorhanden ist, desto dunkler ist die Augenfarbe. Das Problem dabei ist jedoch, dass bei dunklen Augen die für die Iriserkennung erforderlichen Muster – wenn überhaupt – nur schwer erkennbar sind. Daher wird zur Iriserkennung Licht im Infrarot-Bereich verwendet.

Bei der Iriserkennung wird die Iris zunächst spiralförmig von außen nach innen abgescannt. Der Scanner speichert Äderchen, Vertiefungen, Flecken, Rillen, Ringe, etc. als markierte Punkte auf

651 Herbold, Iriserkennung, S. 6 f.
652 Petermann/Scherz/Sauter, TAB Nr. 93, S. 65.

einer Linie. Rollt man diese Linie dann wieder aus, erhält man einen Barcode. Dieser wird im System gespeichert und kann zum Vergleich herangezogen werden. Für ein „Matching“ müssen mindestens 14 Punkte der zu vergleichenden Barcodes übereinstimmen.

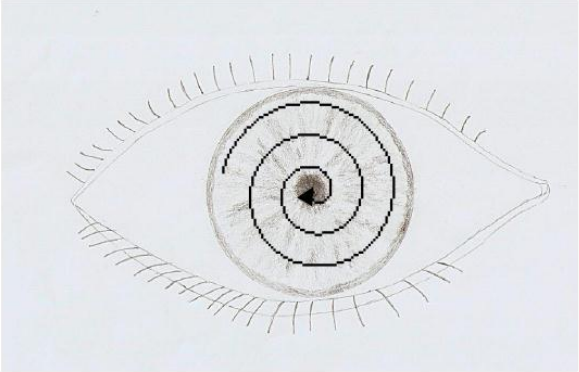


Abb. 11: Iriserkennung 1

Im Weiteren existiert ein Verfahren, wonach die Iris in einen Streifen transformiert wird. Dieser Streifen wird mathematisch aufbearbeitet und anschließend in ein Template umgewandelt.[653]

[653] Vgl. zu den vorhergehenden Abschnitten BSI, Iriserkennung, s. unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Biometrie/Iriserkennung_pdf.pdf;jsessionid=2D37A67E58512238527390C8E4C93883.2_cid156?__blob=publicationFile.

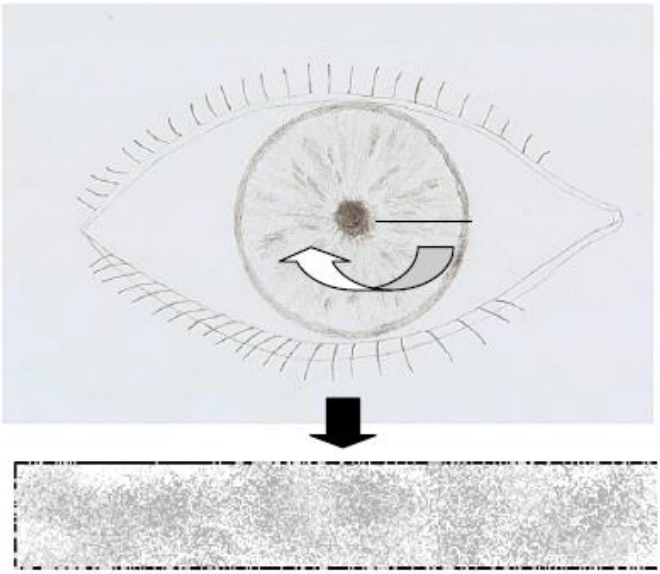


Abb. 12: Iriserkennung 2

Letztlich sind beide Verfahren aber ähnlich, da sämtliche Pigmente aufgenommen und zum Vergleich herangezogen werden.

Entscheidender Vorteil der Iriserkennung ist, dass diese zwischen lebenden und toten Augen unterscheiden kann. Die Pupille eines Toten dehnt sich auf über 80 % aus. Dies besagt allerdings noch nichts darüber, dass man Kontaktlinsen zur Vorspiegelung einer anderen Iris verwenden kann. Letzterem kann allerdings bspw. durch spektrographische Verfahren entgegengewirkt werden. Licht, welches auf Gewebe, Fett oder Blut trifft, wird bei Anwendung verschiedener Wellenlängen unterschiedlich stark absorbiert. Dieser Effekt tritt bei einer Kopie nicht auf.[654]

[654] Vgl. Herbold, Iriserkennung, S. 13.

Anhand der Iris kann bspw. eine Regenbogenhautentzündung erkannt werden. Des Weiteren kann es sein, dass eine Iris für die Erkennung gar nicht vorhanden ist. Dies kann an einem fehlenden Auge oder einer fehlenden Iris (lat. Aniridia) liegen. Auch Liedflimmern macht eine Iriserkennung unmöglich. Angeblich soll auch Diabetes erkennbar sein.[655] Solche Erkrankungen können vielfach Vermutungen über das Leben der Person auslösen. Eine erweiterte Iris kann bspw. auf den Genuss von Drogen oder Alkohol schließen.

Durch Kurz- bzw. Weitsichtigkeit oder Brillen wird die Iris-Erkennung jedoch generell nicht beeinträchtigt; allerdings kann bei starker Sehschwäche die Erfassung fehlschlagen.[656] Auch sind oftmals Teile der Iris durch Wimpern oder Augenlider (sog. „Schlupflider“) verdeckt. Dabei kommt es jedoch meist auf die richtige Kopfneigung an. Die Erfassbarkeit kann auch bei der Einnahme gewisser Medikamente (bspw. Atropin[657]) stark beeinträchtigt sein. Bei bestimmten Augenerkrankungen, wie bspw. dem Grünen Star, ist die Erfassung des Datums schlechthin unmöglich.[658] Weitere Probleme sind noch nicht hinreichend erforscht. Es lassen sich bspw. bisher noch keine Aussagen darüber treffen, inwiefern sich Laser-Behandlungen zur Verbesserung der Sehkraft auf die Erkennung auswirken.

Ein wichtiges Problem ist die richtige Beleuchtung der Iris. Ist die Beleuchtung zu stark, wird der Betroffene zurückweichen; ist sie zu schwach, können die feinen Muster nicht erkannt werden. Aus diesem Grund wird Licht im Infrarot-Bereich verwendet. Dieses kann der Betroffene allerdings nicht wahrnehmen, wodurch die Gefahr einer verdeckten Datenerhebung besteht.

---

655 Meuth, S. 22.
656 BSI, BioP II, S. 17.
657 Durch die Einnahme von Atropin dehnt sich die Iris sehr stark aus.
658 Petermann/Scherz/Sauter, TAB Nr. 93, S. 63.

Amerikanische Forscher arbeiten derzeit an neuen Iriserkennungssystemen. In der Zukunft soll man die Iris unbemerkt aus einer Entfernung von zwei Metern auslesen können.[659] Dies ist v.a. deshalb bedenklich, weil damit der Grundsatz, dass der Betroffene Kenntnis vom Eingriff haben muss, schwer unterlaufen wird. Zudem stellt sich die Frage, wofür eine solche Erweiterung notwendig sein soll. Es gibt derzeit schon Gesichtserkennungssysteme, welche den Betroffenen weitaus besser auslesen können.

Außerdem erfordert die Iriserkennung derzeit noch größeren Aufwand als die anderen Methoden. Das liegt daran, dass der Betroffene absolut still stehen muss und viele Personen Probleme damit haben, wenn etwas am Auge gemacht wird. Daher kann es sein, dass viele die Iriserkennung aufgrund des „Lichtes" ablehnen. Zudem wird der ungeübte Benutzer am Anfang immer Bedienungsschwierigkeiten haben.[660]

2. HANDSCHRIFTENERKENNUNG

Bei der Handschrift handelt es sich um ein verhaltensbasiertes Merkmal. Auch dieses kann zur Identifizierung des Urhebers verwendet werden. Zwar können Handschriften in gewisser Weise gefälscht werden, allerdings enthält das Original immer typische Merkmale wie bspw. das Druckverhalten, welches nicht kopiert werden kann.[661]

Zunächst werden Vergleichsproben genommen. Der Betroffene muss dabei eine Schriftprobe auf einem Tableau (Grafiktablett oder Touchscreen) geben. Die Handschriftenerkennung beruht auf der Annahme, dass der Mensch ein ihn charakterisierende,

[659] Siehe Frey, „"Kampf gegen den Terrorismus – FBI will künftig sogar Hirnströme scannen", in: Welt-Online v. 11.01.2008.
[660] BSI, BioP II, S. 16 f.
[661] Vielhauer/Steinmetz/Scheidat, in: Horster, S. 192.

typische Schreibweise besitzt, welche zwar mit Schwankungen verbunden ist, in der Regel aber automatisiert geschieht. Danach wird die Echtheit des ursprünglichen Schriftstücks und der Schrift überprüft. Dies geschieht mittels physikalisch-technischer Methoden. Anschließend werden die Vergleichsprobe und die strittige Schrift mittels Mikroskopie und nicht zerstörender physikalisch-technischer Methoden auf Personenübereinstimmungen untersucht.

Die Untersuchung erfolgt nach den Grundkomponenten von Michel (1982), welche nicht nur einen reinen Formenvergleich anstreben, sondern auch weitere Aspekte wie „Strichbeschaffenheit, Druckgebung, Bewegungsfluss, Bewegungsführung und Formgebung, Bewegungsrichtung, vertikale und horizontale Ausdehnung, vertikale und horizontale Flächengliederung“ sowie sonstige Merkmale berücksichtigt. [662]

Weitere Beachtung bei der Handschriften-Erkennung findet der Vorgang des Schreibens selbst. Dazu werden Kriterien wie bspw. die Schreibdauer sowie die Geschwindigkeit herangezogen.[663]

Aussagen zur Urheberschaft werden erst gemacht, wenn kein Widerspruch auftritt und die Schrift spezifisch genug ist. Dem Sachverständigen steht dabei eine Bewertung in verschiedenen Wahrscheinlichkeitsgraden zur Verfügung, welche seinen Überzeugungsgrad widergibt.[664] Theoretisch sind anhand der Linienstärke und der Farbablagerungen auch Fälschungen erkennbar.[665] Allerdings sind verschiedene Faktoren wie altersbedingter Schriftabbau, Alkoholeinnahme, ungewisse

[662] Michel, S. 244 ff.; Vielhauer/Steinmetz/Scheidat, in: Horster, S. 194 ff.
[663] Otten, S. 14.
[664] S. LKA Rheinland-Pfalz, „Handschriften“, s. unter www.polizei.rlp.de/internet/nav/cfb/cfb7bf5e-99fe-0014-4b94-615af5711f80&_ic_uCon=cb730033-51c6-d001-44b9-4615af5711f8&conPage=1&conPageSize=50.htm.
[665] Otten, S. 14.

Schreibsituationen (Zug, Flugzeug, etc.) Behinderung des Arms, Nachahmung, Verstellung, usw. zu berücksichtigen.

Beim BKA existiert mittlerweile ein spezielles System zur Handschriftenerkennung namens FISH (Forensisches Informationssystem Handschriften). Dieses System dient der Klassifizierung und dem Merkmalsvergleich.

3. FORENSISCHE SPRECHERKENNUNG (PHONETIK) UND TONTRÄGERAUSWERTUNG

Die forensische Sprecherkennung wird im Bundeskriminalamt seit den 70er Jahren durchgeführt. [666]

Heute gibt es bereits Forschungsorganisationen, welche sich nur mit der forensischen Sprecherkennung auseinandersetzen und Richtlinien ausarbeiten. Hierzu gehört bspw. die "International Association for Forensic Phonetics und Acoustics", welche u.a. den Code of Practice (ethische Richtlinien) für wissenschaftliches Verhalten der Sachverständigen erstellt hat.

Die forensische Spracherkennung verläuft folgendermaßen:

Die Stimme wird zunächst per Mikrofon aufgenommen.

Zumeist geht der Sprecherkennung jedoch die Tonträgerauswertung voran. Durch die Tonträgerauswertung wird zunächst die Qualität verbessert. Des Weiteren erfolgt bei schlecht verständlichen Teilen eine sog. Spracherkennung. Diese ist jedoch nicht zu verwechseln mit der Sprecherkennung. Erstere versucht das gesprochene Wort in schriftliche Worte umzuwandeln. Im Rahmen der Tonträgerauswertung wird auch geprüft, ob eine Manipulation der Aufzeichnung vorgenommen wurde und ob

[666] S. *Jessen & Jessen,* Teil 1, in: Die Kriminalpolizei, Dez. 2008.

andere akustische Geräusche neben der Sprache erkennbar sind, wie bspw. Schüsse, Umgebungsgeräusche, etc. [667]

Bei der forensischen Sprecherkennung geht es vorrangig um die Stimmenanalyse. Dies kann eine Analyse einer unbekannten Stimme oder eines Vergleichsmaterials sein. Theoretisch gehört dazu auch die Stimmenanalyse durch einen Zeugen. Abhängig von der Qualität und Dauer der Aufzeichnung können gewisse Aussagen über den Sprecher getroffen werden[668]:

- Geschlecht: In der Regel ist das Geschlecht eindeutig bestimmbar, es sei denn der Sprecher ist aufgrund seiner untypischen Stimmlage (bspw. hohe Stimme bei Männern, tiefe Stimme bei Frauen) nicht erkennbar oder flüstert oder verstellt seine Stimme absichtlich.

  Letztere Situation lag bei einer Bombendrohung im Jahr 2003 am Düsseldorfer Flughafen vor. Der Flughafen wurde aufgrund der Bombendrohung für ca. sieben Stunden geschlossen, da man eine Beteiligung von Al Quaida nicht ausschließen konnte. Allerdings lag auch die Möglichkeit nahe, dass die Stimme von einer Frau kam, welche ihre Stimme verstellt hat. Letztlich kam der Anruf tatsächlich von einer Frau, welche den Flughafen nur deswegen stilllegte, um nicht mit ihrem Freund in den Urlaub fahren zu müssen.[669] *Die Studentin muss nun 207.000 Euro Schadensersatz an den*

[667] S. *Jessen & Jessen,* Teil 1, in: Die Kriminalpolizei, Dez. 2008.
[668] S. hierzu und auch im Weiteren *Jessen & Jessen*, Teil 1, in: Die Kriminalpolizei, Dez. 2008.
[669] Spiegel-Online v. 07.04.2004, „Prozess um falsche Bombendrohung – Studentin wollte mit Warnung Urlaub verhindern".

Flughafen zahlen und wird ihr Leben lang an der Pfändungsgrenze leben.[670]

- Alter: Eine Einteilung in Kindheit, Jugend, Erwachsenenalter und Seniorenalter ist meist ohne Probleme möglich. Allerdings sind die meisten Untersuchungen im Bereich des Erwachsenenalters. Eine genaue Einordnung wird hier schwierig, weshalb meist „nur" ein Intervall von 10 bis 15 Jahren angegeben wird. Die Schwierigkeit bei der Einordnung ergibt sich meistens aus dem Lebensstil des Sprechers. Während manche ihre Stimme pflegen, setzen andere wiederum ihre Stimme zahlreichen Belastungen wie bspw. Rauchen, Alkohol oder Strapazen durch lautes Sprechen aus. Dadurch wirkt die Stimme unfreiwillig älter.

- Regionale Herkunft und Muttersprache: Hierbei werden Dialekte und regionale Einflüsse untersucht. Merkmalsprägend können auch Einflüsse bei der Verwendung einer Zweitsprache, welche nicht die Muttersprache ist, sein, bspw. wenn ein Franzose versucht, Deutsch zu sprechen.

- Weitere Sprechereigenschaften: Hierzu gehören Sprachstörungen, welche nicht nur zeitweilig auftreten wie bspw. Erkältungen. Vielmehr fallen hierunter organische Störungen, also Stottern oder Sigmatismus (Lispeln). Des Weiteren sind sprachliche Qualitäten des Sprechers, d.h. Eloquenz, Anwendung korrekter Grammatik, Wortwahl, Satzbau, Verwendung von Fachsprache, etc zu beachten.

[670] Spiegel-Online v. 08.06.2007, „Bombendrohung aus Liebeskummer – Studentin muss 207.000 Euro Schadensersatz zahlen".

> Auch stimmliche Besonderheiten (besonders hohe/tiefe Stimme oder schnelle/langsame Sprechweise, Pausenverhalten) sind für die Sprecherkennung wichtig.

Anhand dieser Aussagen kann zwar meist keine Identifikation durchgeführt werden. Allerdings kann ein solcher Stimmenvergleich Beweise erhärten bzw. den Täter aus einer kleinen Gruppe von Verdächtigen herausfiltern.

Eine Auswertung ist nur erschwert möglich, wenn die Aufzeichnung von zu kurzer Dauer ist oder eine schlechte Qualität (Hintergrundgeräusche) aufweist. Aufgrund der heutigen Technik in der Tonträgerbestimmung können jedoch viele qualitative Fehler behoben werden. Allerdings ist das System sehr anfällig für Veränderungen durch Erkrankungen (bspw. Halsentzündungen) oder Außengeräusche.[671]

Bei der Analyse der Stimme durch einen Zeugen muss beachtet werden, dass die Erinnerung an eine akustische Wahrnehmung nicht sehr lange anhält. Aus diesem Grund muss ein Stimmenvergleich möglichst bald durchgeführt werden.

Da auch bei der Stimmerkennung Möglichkeiten des Missbrauchs vorhanden sind, bspw. durch den Einsatz einer Tonbandaufzeichnung, sind auch hier Vorkehrungen zu treffen. So kann bspw. ein sich ständig verändernder Text verwendet werden, wobei hierbei an die Software hohe Anforderungen gestellt werden müssen.[672]

---

[671] Petermann/Sauter, TAB Nr. 76, S. 34.
[672] Bothe/Kilian, S. 572 f.

4. HANDGEOMETRIE

Die Handgeometrie wurde bereits bei den Olympischen Spielen in Atlanta (1996) angewendet.[673]

Die zeitliche Stabilität der Handerkennung wird als gering eingeschätzt, da die Hand erst mit 12-14 Jahren einigermaßen stabil oder sogar erst mit 20 Jahren stabil ist. Ab dann wird die Hand meist nur durch Krankheiten, Verstümmelungen oder Schwellungen (bspw. nach langen Flügen) verändert.[674]

Bei der Handgeometrie werden Handcharakteristika wie Länge, Breite und Dicke der Finger, die Fingerkrümmung sowie die Eigenschaften der Hautoberfläche vermossen. Daher gibt es, u.a. bei Menschen, die an Arthritis leiden, Probleme bei der Erfassung.[675]

Fehler können dadurch entstehen, dass die Hand falsch positioniert wird. Außerdem kann der Nutzer hygienische Bedenken hegen.

Auch die Hand enthält überschüssige Informationen. So ist erkennbar, ob die betreffende Person am Marfan-Syndrom leidet. Dies zeigt sich in einer besonders länglichen Hand. Ferner kann man mithilfe der Hand feststellen, ob jemand an Gicht oder Arthritis leidet.[676]

5. OHRGEOMETRIE

Jede Ohrmuschel ist aufgrund ihrer Form und Größe einzigartig. Vergleiche von Ohrmuscheln wurden bereits erfolgreich eingesetzt, allerdings ist dies bisher nur möglich, wenn eine Spur am Tatort vorlag und bereits ein Verdächtigter bestimmt ist. Leider

673 Petermann/Sauter, TAB Nr. 76, S. 62.
674 Petermann/Scherz/Sauter, TAB Nr. 93, S. 65; Petermann/Sauter, TAB Nr. 76, S. 26.
675 Petermann/Scherz/Sauter, TAB Nr. 93, S. 62.
676 S. Meints, Folien 31 f.

hat diese Technologie vor Gericht noch keine Beweiskraft. Daher werden derzeit nur Beschreibungen von Ohrmuscheln im Rahmen der ED-Behandlung verwendet.

6. KÖRPERGERUCH

Dieses Merkmal ist erst noch in der Entwicklung. Allerdings ist klar, dass jeder Körper eine einzigartiges Geruchsmuster besitzt, welches durchaus biometriefähig wäre.

II. BILATERALES ABKOMMEN ZWISCHEN DEN USA UND DER BUNDESREPUBLIK DEUTSCHLAND

Am 01.10.2008 wurde zwischen den Vereinigten Staaten von Amerika und der Bundesrepublik ein Abkommen[677] zur Vertiefung der grenzüberschreitenden Zusammenarbeit geschlossen. Dieses regelt u.a. den Austausch von daktyloskopischen und DNA-Daten und baut damit den Informationsaustausch aus.

Das Abkommen wurde in Deutschland am 03.07.2009 mit dem *Gesetz zu dem Abkommen vom 01.10.2008 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität*[678] sowie mit dem *Gesetz zur Umsetzung des Abkommens zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika vom 01.10.2008 über die Vertiefung*

[677] *Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität*; BGBl. 2009 II, Nr. 30, S. 1011 ff.

[678] BGBl. II 2009, Nr. 30, S. 1010 ff.

der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität[679] umgesetzt.[680]

Das Abkommen soll die Grundlage für den automatischen Abgleich von DNA- und Fingerabdruckdaten im Hit-/ No Hit-Verfahren per Direktzugriff schaffen. Die Fundstellendatensätze sollen neben den entsprechenden Daten eine Kennung enthalten. Anhand letzterer können im Fall eines Treffers weitere Informationen über den Weg der internationalen Rechtshilfe ausgetauscht werden.

Das Abkommen regelt nicht nur den automatisierten Abruf der DNA- und Fingerabdruck-Daten, sondern auch die Übermittlung weiterer personenbezogener Daten (u.a. Daten, aus denen die Rasse, Überzeugungen, etc. hervorgehen), deren Verwendung, die Rechte des Betroffenen sowie Dokumentationspflichten.

Anders als der Prümer Ratsbeschluss sieht das Abkommen nur eine Übermittlung für Fälle „schwerwiegender Kriminalität" vor, wobei dieser Ausdruck jedoch nicht definiert wird. Zwar können die Parteien gem. Art. 10 III in einer gesonderten Erklärung diese Straftaten festlegen. Dazu besteht aufgrund des eindeutigen Wortlauts jedoch keine Verpflichtung. Ferner kann die Erklärung gem. Art. 10 III S. 2 jederzeit geändert werden.

Das Abkommen ist sehr kritisch zu betrachten, da es z.T. sehr unklar formuliert ist. Das Abkommen klärt z.B. nicht, welche Behörden genau Zugriff auf die Systeme haben dürfen. Damit fragt man sich, ob letztlich nicht jeder „Dorfsheriff" auf diese Daten zugreifen kann. Des Weiteren dürfen Daten aus Deutschland gemäß den bestehenden Datenschutzvorschriften bisher nur an Staaten mit angemessenem Datenschutzniveau weitergegeben

[679] BGBl. I 2009, Nr. 59, S. 2998 f.
[680] Siehe Gesetzesbeschluss, BR-Drs. 637/09 vom 03.07.09 sowie Gesetzesbeschluss, BR-Drs. 638/09 vom 03.07.09.

werden. Ob die USA ein solches Niveau hat, ist äußerst fraglich, wenn man einen Blick auf die Untersuchung der britischen Bürgerrechtsorganisation „Privacy International“[681] wirft. Des Weiteren wurde leider oftmals eine allzu schwammige Wortwahl vorgenommen. Hierzu vergleicht man bspw. Art. 11 II lit. b). Danach dürfen die Daten nur so lange aufbewahrt werden, „als dies für den Zweck (...) nötig ist“. Als Zweck wurde u.a. bereits in Art. 4 I sowie in Art. 10 I die Verhinderung schwerwiegender bzw. terroristischer Straftaten aufgeführt. Aber ist es nicht gerade zur Bekämpfung terroristischer Straftaten erforderlich, diese dauerhaft zu sammeln, um dadurch bestimmte Strukturen aufzudecken und mögliche Attentäter bzw. Attentate zu verhindern. Wo ist hier die zeitliche Grenze für die Aufbewahrung? Wer legt hierbei fest, wann es nicht mehr nötig ist? Soll dies tatsächlich eine Behörde machen, welche daran interessiert ist, über Jahre hinweg ein Terrornetz ausfindig zu machen und deren Aktivitäten vorauszuschauen? Datenschutzbeauftragte existieren in den USA derzeit noch nicht, sodass es auch keine unabhängige Behörde zur Überprüfung der Verarbeitungsvorgänge gibt. Auch die Stellung des Betroffenen ist sehr schwach ausgeprägt. Aufgrund dessen, dass Deutschen in den USA derzeit kein Datenschutzrecht zur Verfügung steht, haben sie keine wirksame Möglichkeit, Auskunftsansprüche, Berichtigungen oder Löschungen durchzusetzen. Ferner wird im Abkommen auch kein Gericht genannt, welches eine Kontrollfunktion ausüben könnte, von unabhängigen Datenschutzbeauftragten ganz zu schweigen. Darüber hinaus ist fraglich, ob die Datenschutzregelungen ausreichend sind. Angesichts der Tatsache, dass die USA dem Datenschutzübereinkommen des Europarats nicht beigetreten sind und auch sonst keine Datenschutzregelungen zwischen der Bundesrepublik Deutschland und den USA bestehen, wären

[681] S. http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597.

eigentlich konkrete Regelungen im Abkommen erforderlich gewesen. Die dort vorhandenen Regelungen in den Art. 11-18 reichen hierzu nicht aus.

III. WEITERE AUSWEISE

Neben den ePässen wurden auch Änderungen beim Personalausweis und beim Führerschein geschaffen.

1. DER NEUE PERSONALAUSWEIS

Während in der Zeit vor 1987 ausschließlich Papierausweise hergestellt und verwendet wurden, wurden mit dem Gesetz über Personalausweise vom 21.04.1986 maschinenlesbare Dokumente eingeführt. Bereits damals gab es zahlreiche Diskussionen aufgrund der Maschinenlesbarkeit.[682] Bis zur Neufassung des PersAuswG im Jahre 2002 waren Fingerabdrücke und die Aufnahme verschlüsselter Merkmale im Ausweis verboten.[683] Schließlich sollte der Ausweis keine Daten enthalten, die für den Inhaber nicht lesbar sind.[684]

Am 09.01.2002 wurde mit Art. 8 Terrorismusbekämpfungsgesetz[685] die Änderung des Personalausweisgesetzes beschlossen. Künftig sollen hier gem. § 1 IV PersAuswG biometrische Daten zum Einsatz kommen. Damit werden künftig die computergestützte

[682] Vgl. Diskussion in Hornung, S. 405 ff.
[683] S. § 1 II 2 PersAuswG von 1950 (BGBl. I 1950, Nr. 53, S. 807).
[684] „Beschlussempfehlung und Bericht des Innenausschusses zu dem (…) Entwurf eines Gesetzes zur Änderung des Gesetzes über Personalausweise", BT-Drs. 8/3498 v. 12.12.1979, S. 9.
[685] *„Gesetz zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz) v. 09.01.2002",* BGBl. I 2002, Nr. 3, S. 361 ff.

Identifizierung des Ausweisinhabers sowie die Prüfung der Authentizität des Ausweises ermöglicht.[686]

Die Ausfertigung des *Gesetzes über Personalausweise und den elektronischen Identitätsnachweis sowie zur Änderung weiterer Vorschriften* erfolgte am 18.06.2009[687]. Die Regelungen zum elektronischen Personalausweis treten am 01.11.2010 in Kraft. Im Gegensatz zum vorherigen Ausweis werden nun u.a. biometrische Daten verwendet. Anfangs sind nur digitale Fotos verpflichtend, Fingerabdrücke dagegen freiwillig. Ob sich das noch ändern wird, bleibt offen.

Motiv für die Änderung des Ausweisrechts war die Änderung des Passrechts. Da der Personalausweis in Europa ein vollwertiges Reisedokument ist, könnte dies – sofern der Personalausweis unverändert bliebe – eine Lücke nach sich zu ziehen.[688] Es wurde daher für ratsam gehalten, auch hier die Anforderungen der ICAO anzuwenden.[689] Da die EU für den Personalausweis jedoch keine Regelungskompetenz besitzt, verblieb die Entscheidung darüber bei den Mitgliedstaaten.[690]

Erwähnenswert sind in diesem Zusammenhang die neuen Funktionen des Personalausweises: Mithilfe der Biometriefunktion soll der Personalausweis auch ersatzweise als Reisedokument dienen können. Die weiteren personenbezogenen Daten (Name, Anschrift, Alter und Gültigkeit) sollen zukünftig im E-Business und im E-Gouvernment Anwendung finden. Durch die Eingabe eines PINs wird der Nutzer des Ausweises authentisiert und die Daten an den Empfänger übermittelt. Mit der zusätzlichen

---

686 Gesetzesbegründung zum „Entwurf eines Gesetzes zur Bekämpfung des internationalen Terrorismus (Terrorismusbekämpfungsgesetz)", BT-Drs. 14/7386 v. 08.11.2001, S. 4f f.
687 BGBl. I 2009, Nr. 33, S. 1346 ff.
688 Siehe Engel, in: DuD 30/2006, S. 207 (208).
689 So auch Hornung, S. 39.
690 Siehe Hornung, S. 96.

Signaturfunktion sollen zudem zahlreiche Behördengänge über das Internet abgewickelt und damit überflüssig werden.

Der Personalausweis fand im Rahmen dieser Arbeit keine Beachtung, da dieser an den ePass hinsichtlich der biometrischen Daten angeglichen wurde und daher die gleichen Grundsätze gelten.

2. BIOMETRISCHER FÜHRERSCHEIN

Daneben wurde am 13.06.2008 die *Vierte Verordnung zur Änderung der Fahrerlaubnis-Verordnung und anderer straßenverkehrsrechtlicher Vorschriften*[691] beschlossen. Gem. Art. 1 Nr. 13 wurde festgelegt, dass der Führerschein mit einem biometrischen Lichtbild auszustatten ist (siehe nun § 21 III S. 1 Nr. 2 Fahrerlaubnis-Verordnung). Die Begründung für diese Änderung ist recht dürftig. Demnach sei die Einführung eines solchen Lichtbildes erforderlich, um den Inhaber der Fahrerlaubnis mit dem Fahrzeugführer abzugleichen. Da es jedoch in Deutschland keine Verpflichtung gäbe, neben der Fahrerlaubnis einen Personalausweis mitzuführen, sei ein biometrisches Lichtbild erforderlich.[692]

Dies ist in mehrfacher Hinsicht zu kritisieren. Zum einen stellt sich die Frage, ob ein biometrisches Lichtbild überhaupt erforderlich ist. Bis jetzt haben die Polizeidienststellen, welche zur Kontrolle des Führerscheins befugt sind, nicht die hierfür benötigten Geräte. Abgesehen davon ist auch die Angemessenheit einer solchen Maßnahme höchst bedenklich. Schließlich soll überprüft werden, ob die Person auf dem Führerschein auch wirklich der Inhaber des Führerscheins ist. Sollte dies nicht der Fall sein, läge damit

[691] BGBl. I 2008 Nr. 31, S. 1338 ff.
[692] BR-Drs. 302/08 vom 30.04.2008 zur „Vierten Verordnung zur Änderung der Fahrerlaubnis-Verordnung und anderer straßenrechtlicher Vorschriften", S. 64.

lediglich ein Vergehen gem. § 21 StVG vor. Damit ist bereits die Angemessenheit hinsichtlich der Einführung eines Lichtbildes im Führerschein fraglich. Zum anderen wurde diese Änderung so still vollzogen, dass weder eine Diskussion in der Bevölkerung stattfand noch Informationen durch die regionalen Führerscheinstellen ausgegeben wurden.

IV. ÄNDERUNG DER DATENSCHUTZRECHTLICHEN REGELUNGEN AUF EUROPÄISCHER UND INTERNATIONALER EBENE

Die Europäische Gemeinschaft hat mit der Datenschutzrichtlinie 95/46/EG[693] vom 13.12.1995 Datenschutzregelungen für die erste Säule geschaffen. Mit der Datenschutzverordnung 45/2001[694] vom 18.12.2000 sind diese Regelungen auch auf die Organe der Europäischen Gemeinschaft anzuwenden.

Für die dritte Säule wurde ein Rahmenbeschluss[695] zum Datenschutz beschlossen. Dieser gilt jedoch nur für den grenzüberschreitenden Austausch von personenbezogenen Daten

[693] *Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,* Abl. L 281 vom 23.11.1995, S. 31 ff.
[694] *Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18.12.2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr;* Abl. L 8 vom 12.01.2001, S. 1 ff.
[695] *Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden*, Abl. L 350 vom 30.12.2008, S. 60 ff.

innerhalb der EU. Darüber hinaus hat die Kommission weitere Defizite festgestellt.[696]

Auch wenn mit dem Vertrag von Lissabon die Säulenstruktur aufgehoben wurde und damit auch die ehemalige dritte Säule dem Unionsrecht unterworfen wird, so sind dennoch unterschiedliche Datenschutzregelungen vorhanden, welche angepasst werden müssen. Im Übrigen ist auch den Besonderheiten im Bereich der polizeilichen und justiziellen Zusammenarbeit Rechnung zu tragen. Die Kommission hat nun ein „Gesamtkonzept für den Datenschutz in der Europäischen Union“[697] erarbeitet, welches die Änderung und Verbesserung des Datenschutzes vorsieht. Vorschläge für eine neue Grundlage gibt es bislang noch nicht.[698]

Der Europarat sieht ebenfalls eine Änderung der Datenschutzkonvention vor, wobei jedoch auch hier bislang noch kein Entwurf vorliegt.[699] Hierbei sollen insbesondere die Empfehlungen R(87) 15 und (92) 1 eingearbeitet werden.

[696] Siehe Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Gesamtkonzept für den Datenschutz in der Europäischen Union“, KOM (2010) 609 endg. vom 04.11.2010, S. 15 f.
[697] Mitteilung der Kommission an das Europäische Parlament, den Rat, den europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen „Gesamtkonzept für den Datenschutz in der Europäischen Union“, KOM (2010) 609 endg. vom 04.11.2010.
[698] Stand: 22.08.2011.
[699] Stand: 22.08.2011.

TEIL F Schluss

Zusammenfassend hat sich ergeben, dass der ePass durchaus den völkerrechtlichen Anforderungen genügt, sofern die Verwendung von daktyloskopischen Bilddaten zugunsten von Templates aufgegeben wird. Des Weiteren ist festzulegen, dass strafrechtliche und disziplinarrechtliche Konsequenzen für den Fall des Missbrauchs bzw. der unrechtmäßigen Datenverarbeitung drohen. Da der ePass nur so sicher ist, wie die Überprüfung der für die Beantragung erforderlichen Dokumente, ist auch eine dahingehende Regelung zu treffen, welche Dokumente vorzulegen sind und wie deren Echtheit überprüft werden kann. Auch sind bislang keine Regelungen hinsichtlich eines nationalen Passregisters unter Verwendung aller biometrischen Daten getroffen werden, so dass dies bislang bei den Mitgliedstaaten verbleibt. Auch hier gilt ungeachtet des Subsidiaritätsprinzips, dass eine Regelung hinsichtlich des „OBs“ einer solchen Errichtung zu treffen ist. Letztlich kann der ePass bzgl. der Datensicherung gerügt werden, wobei hier eine Behebung bereits durch einfache Mittel möglich ist. Zum einen sollte eine Art Faradayscher Käfig eingebaut werden bzw. dem Betroffenen ein zusätzliches Passwort an die Hand gegeben werden, um unbefugtes Auslesen zu Verhindern; zum anderen sind geschultes Personal aufzustellen und regelmäßige Checks durchzuführen. Alle diese Maßnahmen nützen natürlich nichts, wenn der Betroffene nicht über die Verwendung des ePasses und über Möglichkeiten im Falle eines Verlusts aufgeklärt wird.

Im Gegensatz zum ePass leidet der Prümer Ratsbeschluss an wesentlich mehr und weitreichenderen Mängeln. So wird bspw. sowohl aufgrund der Rechtsprechung als auch aufgrund den internationalen Regelungen ein Straftatenkatalog zu fordern sein, da ansonsten sowohl der Ermessensspielraum zu weit ist als auch die Vorhersehbarkeit einer Maßnahme deutlich leidet als auch die Verhältnismäßigkeit einer Maßnahme fraglich ist. Ein Austausch von Daten nach dem Prümer Ratsbeschluss ist sicherlich dann nicht verhältnismäßig, wenn es sich um Beleidigungen, Ladendiebstähle etc. handelt; dies gilt auch dann, wenn es sich um Wiederholungstaten handelt. Daran ändert auch der Grundsatz der Subsidiarität nichts, da hier eine staatenübergreifende Vereinheitlichung zu fordern ist. Ansonsten bestünde die gleiche Situation wie bei Interpol (s. Teil C Pkt. B. II. 3.), nämlich dass manche Staaten eine Beschränkung auf bestimmte Straftaten vorsehen und andere nicht und infolgedessen nur ein Abgleich zwischen „willkürlich" erhobenen Daten möglich ist. Auch Vorschriften zur strafrechtlichen und disziplinarrechtlichen Verantwortlichkeit fehlen, was gerade beim Prümer Ratsbeschluss aufgrund dessen Reichweite wichtiger ist als beim ePass. Es stellt sich nämlich beim Prümer Ratsbeschluss die Frage, warum solche Regelungen im Bereich der „Weiteren Formen der Zusammenarbeit" getroffen wurden, aber nicht im Zusammenhang mit der Verarbeitung biometrischer Daten. Auch hier gilt wiederum, dass zumindest Vorschriften hinsichtlich des „OB" zu treffen sind; das „WIE" dagegen kann auch hier im Sinne der Subsidiarität den Mitgliedstaaten überlassen werden. Im Übrigen sollte die Formulierung von Art. 26 I Prümer Ratsbeschluss überdacht werden, welcher derzeit noch recht vage ist.

Fraglich ist, ob vor der Übermittlung eine Qualitätsprüfung stattfinden sollte. Da dies vor einem Abgleich logischerweise nicht möglich ist, sollte eine Prüfung bei der Speicherung der Daten oder

spätestens vor Übermittlung der Fundstellendatensätze vorgenommen werden. Auch ein Beweisverwertungsverbot rechtswidrig verarbeiteter Daten ist zu durchzusetzen. Zu guter Letzt fehlen staatenübergreifende Einwirkungsbefugnisse der Kontrollbehörden. Diese haben nur die Möglichkeit, Anfragen zu stellen und auf deren Beantwortung zu hoffen, ohne dass eine Weisung möglich ist. Um jedoch die Rechte eines Betroffenen umfassend durchsetzen zu können, sind Einwirkungsbefugnisse unbedingt erforderlich, entweder durch den Europäischen Datenschutzbeauftragten oder mittels eine Verbindungsbeamten. Anhand dieser Mängelliste ist zu erkennen, dass trotz der Tatsache, dass der Vertrag von Prüm als Versuchsmodell gelten sollte, keine Verbesserung dieser Vorschriften vorgenommen worden ist; diese sind vielmehr unverändert in den Prümer Ratsbeschluss übernommen worden.

Hinsichtlich des EU-Führerscheins sowie hinsichtlich des Personalausweises stellen sich mittlerweile aufgrund der Aufnahme der biometrischen Daten die gleichen Fragen wie beim ePass. Auch hinsichtlich des Abkommens zwischen den USA und der Bundesrepublik Deutschland dürften die gleichen Probleme bestehen wie beim Prümer Ratsbeschluss, jedoch aufgrund der Drittstaatenübermittlung in wesentlich erhöhtem Maße.

Es wird sich zeigen, ob der internationale Datenschutz weitere Regelungen aufstellt und ob der ePass und der Prümer Ratsbeschluss dann nicht noch weitere Schwächen aufzuarbeiten haben.

LITERATURVERZEICHNIS

Adlbrecht, Katja

„Auf die Finger geschaut! Personenidentifikation durch das Automatische Fingerabdruck-Identifikationssystem AFIS“, 2009, www.ai.wu.ac.at/~koch/courses/wuw/archive/inf-sem-ss-09/adlbrecht.pdf

Akmann, Torsten

„Die Zusammenarbeit in den Bereichen Justiz und Inneres als „3.Säule“ des Maastrichter Unionsvertrages“, in: JA 1994, S. 49 ff.

Baldus, Manfred

Transnationales Polizeirecht – Verfassungsrechtliche Grundlagen und einfach-gesetzliche Ausgestaltung polizeilicher Eingriffsbefugnisse in grenzüberschreitenden Sachverhalten, 2001

BBC News

„My fake passport and me“, 01.12.2006, http://news.bbc.co.uk/2/hi/programmes/panorama/6158927.stm

Berg, Jeremy M. / Tymoczko, John, L. / Stryer, Lubert

Biochemie, 5. Auflage 2003

Berns, Eva

Statistische Probleme der forensischen DNA-Analyse, Diplomarbeit, März 2006, www.ruhr-uni-bochum.de/malakow/Download/Diplomarbeit_EvaBerns.pdf

Bittner, Jochen / Staud, Toralf

„Vorsicht-Sammelwut“, Bericht der Zeit-online, 15.02.2009, www.zeit.de/2001/37/Vorsicht_Sammelwut

Böse, Martin

Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007

Böse, Martin

Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der EU, in: EuZ 4/2007, S. 62 ff.

Bothe, Michael / Kilian, Wolfgang

Rechtsfragen grenzüberschreitender Datenflüsse, 1992

Breitenmoser, Stephan

Der Schutz der Privatsphäre gemäß Art. 8 EMRK, 1986

Brodersen, Kilian / Anslinger, Katja / Rolf, Burkhard

DNA-Analyse und Strafverfolgung – Rechtliche und biologische Grundlagen der DNA-Analyse, 2003

BSI – Bundesamt für Sicherheit in der Informationstechnik

Evaluierung biometrischer Systeme Finderabdrucktechnologien – BioFinger", Öffentlicher Abschlussbericht, 06.08.2004, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFinger/BioFinger_I_I_pdf.pdf?__blob=publicationFile

BSI – Bundesamt für Sicherheit in der Informationstechnik

Studie: Untersuchung der Leistungsfähigkeit von Gesichtserkennungssystemen zum geplanten Einsatz in Lichtbilddokumenten – BioP I, Öffentlicher Abschlussbericht, 07.04.2004, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioP/biopabschluss_pdf.pdf?__blob=publicationFile

BSI – Bundesamt für Sicherheit in der Informationstechnik

Studie: Untersuchung der Leistungsfähigkeit von biometrischen Verifikationssystemen – BioP II, Öffentlicher Abschlussbericht, 23.08.2005, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioP/biopabschluss2_pdf.pdf?__blob=publicationFile

BSI – Bundesamt für Sicherheit in der Informationstechnik

BioFace – Vergleichende Untersuchung von Gesichtserkennungssystemen, Öffentlicher Abschlussbericht BioFace I & II, Juni 2003, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/BioFace/BioFaceIIBericht_pdf.pdf;jsessionid=1E4CE5143DD1BE1C1A58FED0030FAF5C.2_cid165?__blob=publicationFile

Chaos Computer Club (CCC)

„Wie können Fingerabdrücke nachgebildet werden?“, 09.10.2004, www.ccc.de/de/campaigns/aktivitaeten_biometrie/fingerabdruck_kopieren

Connors, Edward et al.

Convicted by Juries, Exonerated by Science: Case studies in the Use of DNA Evidence to Establish Innocence After Trial, Untersuchungsbericht, Juni 1996

Ehlers, Dirk (Hrsg.)

Europäische Grundrechte und Grundfreiheiten, 3. Auflage, 2005

Ellger, Reinhard

Der Datenschutz im grenzüberschreitenden Datenverkehr, 1990

Engel, Christian

„Auf dem Weg zum elektronischen Personalausweis – Der elektronische Personalausweis (ePA) als universelles Identifikationsdokument“, in: DuD 30/2006, S. 207 ff.

Focus-Online

„Diabetes Typ 1 – Fingerabdruck zeigt Zuckerrisiko“, 05.12.2005, www.focus.de/gesundheit/ratgeber/diabetes/diabetes-typ-1_aid_102145.html

Focus-Online

„Leiche mit weiblicher und männlicher DNA entdeckt“, 19.10.2008, www.focus.de/panorama/welt/muenchen-leiche-mit-maennlicher-und-weiblicher-dna-entdeckt_aid_341833.html

Frenz, Walter

Handbuch Europarecht, Band 4, Europäische Grundrechte, 2009

Frey, Peter

„Kampf gegen den Terrorismus – FBI will künftig sogar Hirnströme scannen“; Bericht auf welt-online.de, 11.01.2008, www.welt.de/wissenschaft/article1541476/FBI_will_kuenftig_sogar_Hirnstroeme_scannen.html

Frowein, Jochen / Peukert, Wolfgang

Europäische Menschenrechtskonvention, EMRK-Kommentar, 3. Auflage, 2009

Genz, Alexander

Datenschutz in Europa und den USA – Eine rechtsvergleichende Untersuchung unter besonderer Berücksichtigung der Safe-Harbour-Lösung, 2004

Grabenwarter, Christoph

Europäische Menschenrechtskonvention, 4. Auflage, 2008

Gusy, Christoph

„Grundrechtsschutz vor staatlichen Informationseingriffen“, in: VerwArch 74 (1983), S. 91 ff.

Hamann, Alexander

„Geschichte(n) der Biometrie“, Studienarbeit, 17.05.2007, http://www2.informatik.hu-berlin.de/~ahamann/studies/Geschichte%28n%29_der_Biometrie.pdf

Harings, Lothar

Grenzüberschreitende Zusammenarbeit der Polizei- und Zollverwaltungen und Rechtsschutz in Deutschland, 1998

Heilmann, Eric

„Die Bertillonage und die Stigmata der Entartung“, in: KrimJ 1/1994, S. 36 ff.

Heise online

„Neue Videoüberwachung beim Super Bowl getestet“ vom 01.02.2001

Heise online

„Sicherheitsexperte führt Klonen von RFID-Reisepässen vor“, 03.08.2006, www.heise.de/security/meldung/Sicherheitsexperte-fuehrt-Klonen-von-RFID-Reisepaessen-vor-148641.html

Henke, Ferdinand

Die Datenschutzkonvention des Europarats, 1986

Herb, Marc

„Ethische Aspekte der DNA-Analyse in der Strafverfolgung“, Hausarbeit, Januar 2004, http://v.hdm-stuttgart.de/seminare/ie2003/W_MarcHerb.pdf

Herbold, Klaus

Iriserkennung, 31.05.2007, www.csipc2.de/docs/klaus.herbold-elaboration.pdf

Herdegen, Matthias

Europarecht, 2009

Heselhaus, Sebastian M. / Nowak, Carsten

Handbuch der Europäischen Grundrechte, 2006

Hofmann, Jens

Rechtsschutz und Haftung im Europäischen Verwaltungsverbund, 2004

Hornung, Gerrit

Die digitale Identität – Rechtsprobleme von Chipkartenausweisen: Digitaler Personalausweis, elektronische Gesundheitskarte, JobCard-Verfahren, 2005

Horster, Patrick

D-A-CH Security 2004 – Bestandaufnahme, Konzepte, Anwendungen, Perspektiven, 2004

Howard, John

„UK DNA Mismatch“, in: Scoop, Newzealand News vom 10.02.2000, www.scoop.co.nz/stories/HL0002/S00053.htm

Huke, Björn

„Erfolgreiche Einführung der Version INPOL-Bayern 6.0“, in: Bayerns Polizei 1/2009, S. 19 ff.

Jain, Anil K./Ross, Arun/Prabhakar, Salil

“An Introduction to Biometric Recognition”, in: IEEE Transactions on circuits and systems for video technology, Vol. 14, No. 1, Januar 2004, siehe unter www.csee.wvu.edu/~ross/BiometricsTextBook/Papers/Introduction/JainRossPrabhakar_BiometricsIntro_CSVT04.pdf

Jessen, Marianne / Jessen, Michael

„Forensische Sprecherkennung und Tonträgerauswertung in Praxis und Forschung – Teil 1“, in: Die Kriminalpolizei Dezember 2008, s. auch unter www.kriminalpolizei.de/articles,forensische_sprechererkennung_und_tontraegerauswertung_in_praxis_und_forschung,1,223.htm

Kämper, Gregor

Polizeiliche Zusammenarbeit in der Europäischen Union, 2001

Kietz, Daniela / Maurer, Andreas

„Die Folgen der Prümer Ratsbeschluss Vertragsavantgarde – Fragmentierung und Entdemokratisierung der europäischen Justiz- und Innenpolitik?“, Diskussionspapier, 01.01.2007, www.swp-berlin.org/fileadmin/contents/products/arbeitspapiere/Pruem_KS_JBOES_final_word.pdf

Koydl, Wolfgang

„Englische Sammelwut“, Bericht in der Süddeutschen Zeitung vom 06.12.2008, www.sueddeutsche.de/politik/datenschutz-in-grossbritannien-englische-sammelwut-1.361203

Kübler, Johanna

Die Säulen der Europäischen Union: einheitliche Grundrechte?, 2002

Lindner, Franz Josef

„Grundrechtsschutz in Europa – System einer Kollisionsdogmatik“, in: EuR 2007, S. 160 ff.

Lorscheid, Helmut

„Kinder-DNA-Datei für «Klau-Kids»“, in: telepolis vom 09.01.2004, www.heise.de/tp/artikel/16/16481/1.html

Mähring, Matthias

„Das Recht auf informationelle Selbstbestimmung im europäischen Gemeinschaftsrecht“, in: EuR 1991, S. 369 ff.

Meints, Martin

„Biometrie – Datenschutz- und Datensicherheitsaspekte“, Vortrag, 2008, https://www.datenschutzzentrum.de/vortraege/20080304-meints-cebit-biometrie-datenschutz-datensicherheit.pdf

Meints, Martin

„Implementierung großer biometrischer Systeme“, DuD 2007, S. 189 ff.

Merkur-online

„Mordfall Wudy: 1500 Männer zum Speicheltest“, 13.09.2002, www.merkur-online.de/lokales/nachrichten/mordfall-wudy-1500-maenner-speicheltest-116485.html

Merkur-Online

„Speicheltest: Ein Mann fehlt“, 13.09.2002, www.merkur-online.de/lokales/nachrichten/speicheltest-mann-fehlt-149787.html

Merkur-Online

„Zweiter Speicheltest im Fall Wudy“, 18.03.2003, www.merkur-online.de/lokales/nachrichten/zweiter-speicheltest-fall-wudy-136428.html

Merkur-Online

„Nur Gewalt und Porno im Kopf“, 18.10.2004, www.merkur-online.de/lokales/nachrichten/gewalt-porno-kopf-170691.html

Meuters, Stefan

Leitung und Kontrolle grenzüberschreitender Ermittlungen, 2004

Meuth, Lotte

Zulässigkeit von Identitätsfeststellungen mittels biometrischer Systeme durch öffentliche Stellen, 2006

Meyer-Ladewig, Jens

Europäische Menschenrechtskonvention – Handkommentar, 2. Auflage, 2006

Meyer-Ladewig, Jens

Europäische Menschenrechtskonvention – Handkommentar, 3. Auflage, 2011

Michel, Lothar

Gerichtliche Schriftvergleichung – Eine Einführung in Grundlagen, Methoden und Praxis, 1982

Milke, Tile

Europol und Eurojust – Zwei Institutionen zur internationalen zur Verbrechensbekämpfung und ihre justizielle Kontrolle, 2003

Mitteleuropäische Polizeiakademie

MEPA-Buch, Stand: November 2008

Mitteleuropäische Polizeiakademie

MEPA-Buch, Stand: November 2010, www.mepa.net/Deutsch/publikationen/MEPADokumente/1B.pdf

Münch, Peter

Technisch-organisatorischer Datenschutz – Leitfaden für Praktiker, 2007

Nachrichtenagentur GmbH

„Britischer Experte knackt elektronischen Reisepass", Pressetext, 08.03.2007, www.pressetext.com/news/20070308015

Neukamm, Katrin

Bildnisschutz in Europa – Zugleich ein Beitrag zur Bedeutung der Verfassungsüberlieferungen der EU-Mitgliedstaaten und der EMRK für die Auslegung der Unionsgrundrechte, 2007

Nogala, Detlef

„DNA-Analyse und DNA-Datenbanken", in: CILIP Nr. 61, www.cilip.de/ausgabe/61/dna.htm

Orantek, Kerstin

Datenschutz im Informationszeitalter – Herausforderungen durch technische, politische und gesellschaftliche Entwicklungen, 2008

Otten, Bettina

„3D Gesichtserkennung – Merkmalsdetektion in 3D-Scans und merkmalsbasierter Vergleich von Gesichtern", Diplomarbeit. März 2006, www.uni-koblenz.de/~cg/Diplomarbeiten/DAOtten.pdf

Papayannis, Donatos

„Die polizeiliche Zusammenarbeit und der Vertrag von Prüm“, in: ZEuS 2/2008, S. 219 ff.

Petermann, Thomas / Sauter, Arnold

TAB Nr. 76, Biometrische Identifikationssysteme, Sachstandsbericht, Februar 2002

Petermann, Thomas / Scherz, Constanze / Sauter, Arnold

TAB Nr. 93, Biometrie und Ausweisdokumente – Leistungsfähigkeit, politische Rahmenbedingungen, rechtliche Ausgestaltung, 2. Sachstandsbericht, Dezember 2003

Peters, Anne

Einführung in die Europäische Menschenrechtskonvention, 2003

Riegel, Reinhard

Datenschutz bei den Sicherheitsbehörden, 1992

Rohleder, Kerstin

Grundrechtsschutz im europäischen Mehrebene-System, 2009

Satzger, Helmut

Internationales und Europäisches Strafrecht, 2010

Schaar, Peter

Das Ende der Privatsphäre – Der Weg in die Überwachungsgesellschaft, 2007

Schaar, Peter (Hrsg.)

Biometrie und Datenschutz – Der vermessene Mensch, Tagungsband des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am 27.06.2006

Schaar, Peter

„Datenaustausch und Datenschutz im Vertrag von Prüm", in: DUD 2006, S. 691 ff.

Schmitz, Peter / Eckhardt, Jens

„Einsatz von RFID nach dem BDSG – Bedarf es einer speziellen Regulierung von RFID-Tags?", in: CR 3/2007, S. 171 ff.

Schrepfer, Thomas W.

Datenschutz und Verfassung – Eine Untersuchung zur verfassungsrechtlichen Relevanz der Erfassung, Aufbewahrung und Weitergabe personenbezogener Daten, 1985

Schubert, Frank

„Verräterische Rillen", 08.05.2007, www.tagesspiegel.de/weltspiegel/gesundheit/verraeterische-rillen/843750.html

Schulzki-Haddouti, Christiane

Im Netz der inneren Sicherheit – Die neuen Methoden der Überwachung, 2004

Siemen, Birte

Datenschutz als europäisches Grundrecht, 2004

Sokol, Bettina (Hrsg.)

Der gläserne Mensch – DNA-Analysen, eine Herausforderung an den Datenschutz, 2003, https://www.ldi.nrw.de/mainmenu_Service/submenu_Tagungsbaende/Inhalt/2003_Der_glaeserne_Mensch_-_DNA-Analysen__eine_Herausforderung_an_den_Datenschutz/2003_Der_glaeserne_Mensch.pdf

Spiegel-Online

„Biometrie-Pannen. Die Probleme kleiner asiatischer Frauen", 28.02.2004, www.spiegel.de/netzwelt/tech/0,1518,288462,00.html

Spiegel-Online

„Prozess um falsche Bombendrohung – Studentin wollte mit Warnung Urlaub verhindern", Bericht vom 07.04.2004, www.spiegel.de/panorama/0,1518,294410,00.html

Spiegel-Online

„Bombendrohung aus Liebeskummer – Studentin muss 207.000 Euro Schadensersatz zahlen", Bericht vom 08.06.2007, www.spiegel.de/reise/aktuell/0,1518,487524,00.html

Streinz, Rudolf

EUV/EGV Beck'sche Kurzkommentare, 2003

Sule, Satish

Europol und europäischer Datenschutz, 1999

TeleTrust Deutschland e.V.

Kriterienkatalog, Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, 18.08.2006

Tettinger, Peter / Stern, Klaus

Kölner Gemeinschaftskommentar zur Europäischen Grundrechte-Charta, 2006

Thalheim, Lisa / Krissler, Jan / Ziegler, Peter-Michael

„Körperkontrolle – Biometrische Zugangssicherungen auf die Probe gestellt", in: c't 11/2002, S. 114 ff.

Unger, Barbara

Datenschutz in internationalen Organisationen, 1991

Vollkommer, Max (Hrsg.)

Datenverarbeitung und Persönlichkeitsschutz, 1986

Wilkesmann, Peter

„Plädoyer für das Schengener Informationssystem (SIS)", in: NStZ 1999, 68 ff.

Winkels, Heinz-Michael

„Manipulationsmöglichkeiten biometrischer Verfahren", Vortrag, Oktober 2004, www1.logistik.fh-dortmund.de/IT-Sicherheit/33_ManBioVerf.pdf

Wirth, Antonia

„Inpol-neu – Folgen für den Datenschutz", CILIP 62 (1/1999), www.cilip.de/ausgabe/62/inpol.htm

Wolter, Jürgen / Schenke, Wolf-Rüdiger / Hilger, Hans / Ruthig, Josef / Zöller Mark A. (Hrsg.)

Alternativentwurf Europol und europäischer Datenschutz, 2008

Zuleeg, Manfred

„Die Europäische Gemeinschaft als Rechtsgemeinschaft“, in: NJW 1994, S. 545 ff.

Zykla-Menhorn, Vera

„DNA-Analysen in der Forensischen Medizin: Nur die Länge „funktionsloser“ Genabschnitte wird bestimmt“, in: Deutsches Ärzteblatt 4/2005 vom 28.01.2005, www.aerzteblatt.de/v4/archiv/artikel.asp?src=heft&id=45126

RECHTSPRECHUNGSÜBERSICHT EKMR und EGMR

A, B, C und D./.BRD	EKMR , Entscheidung vom 13.12.79 Nr. 8290/78 DR 18, 176
Amann ./. Schweiz	EGMR, Urteil vom 16.02.00 Nr. 27798/95 RJD 2000-II
Arnaud Campion./ .Frankreich	EKMR, Entscheidung vom 06.09.95 Nr. 25547/94
Ashingdane./.Vereinigtes Königreich	EGMR, Urteil vom 28.05.85 Nr. 8225/78 Serie A93
Atlan./.Vereinigtes Königreich	EGMR, Urteil vom 19.06.01 Nr. 36533/97
Boyle&Rice./.Vereinigtes Königreich	EGMR, Urteil vom 27.04.88 Nr. 9659/82 und 9658/82 Serie A131
Bosphorus Hava Yollari Turizm ve Ticaret Anonim ./. Irland	EGMR, Urteil vom 30.06.2012 Nr. 45036/98 NJW 2006, S. 197 ff.

Brüggemann und Scheuten./.BRD	EKMR, Bericht vom 12.07.77 Nr. 6959/75 DR 10, 100
Bykov./.Russland	EGMR, Urteil vom 10.03.09 Nr. 4378/02
Camenzind./.Schweiz	EGMR, Urteil vom 16.12.97 Nr. 21353/93 Rep. 1997-VIII
Campbell & Fell ./. Vereinigtes Königreich	EGMR, Urteil vom 28.06.84 Nr. 7819/77, 7878/77 Serie A 80
Caroline von Hannover ./. Deutschland	EGMR, Urteil vom 24.06.04 Nr. 59320/00 RJD 2004-VI
Census Regulations	EKMR, Entscheidung vom 06.10.82 Nr. 9702/82 DR 30, 239
Chave née Julien./.Frankreich	EKMR, Entscheidung vom 09.07.91 Nr. 14461/88 DR 71, 150

Ciubotaru./.Moldavien	EGMR, Urteil vom 27.04.10 Nr. 27138/04
Copland./.Vereinigtes Königreich	EGMR, Urteil vom 03.04.07 Nr. 62617/00
Connors. /.Vereinigtes Königreich	EGMR, Urteil vom 27.05.04 Nr. 66746/01
Costello-Roberts./.Vereinigtes Königreich	EGMR, Urteil vom 25.03.93 Nr. 13134/87 Serie A 247-C
Domenichini./.Italien	EGMR, Urteil vom 21.10.96 Nr. 15943/90 Rep. 1996-V
Dudgeon./.Vereinigtes Königreich	EGMR, Urteil vom 22.10.81 Nr. 7525/76 Serie A45
Edwards & Lewis./.Vereinigtes Königreich	EGMR, Urteil vom 22.07.03 Nr. 39647/98 und 40461/98
Elsholz ./. Deutschland	EGMR, Urteil vom 13.07.00 Nr. 25735/94 RJD 2000-VIII
Friedl ./. Österreich	EKMR, Bericht vom 19.05.94 Nr. 15225/89

G.W./.BRD	EKMR, Entscheidung vom 04.10.62 Nr. 1307/61 CD 9, 53
Gaskin./.Frankreich	EGMR, Urteil vom 07.07.89 Nr. 10454/83 Serie A 160
Guerra u.a./Italien	EGMR, Urteil vom 19.02.98 Nr. 14967/89 Rep. 1998-I
Haase./.BRD	EGMR, Urteil vom 08.04.04 Nr. 11057/02 RJD 2004-III
Herczegfalvy./.Österreich	EGMR, Urteil vom 24.09.92 Nr. 10533/83 Serie A 244
Hewitt + Harman./.Vereinigtes Königreich	EKMR, Urteil vom 09.05.89 Nr. 12175/86
Hilton./.Vereinigtes Königreich	EKMR, Entscheidung vom 06.07.88 Nr. 12015/86

Huvig./.Frankreich	EGMR, Urteil vom 24.04.90 Nr. 11105/84 Serie A 176-B
K.U./.Finnland	EGMR, Urteil vom 02.12.08 Nr. 2872/02
Kennedy./.Vereinigtes Königreich	EGMR, Urteil vom 18.05.10 Nr. 26839/05
Khan./.Vereinigtes Königreich	EGMR, Urteil vom 12.05.00 Nr. 35394/97 RJD 2000-V
Klass u.a. /. BRD	EGMR, Urteil vom 06.09.78 Nr. 5029/71 Serie A 28
Kopp./.Schweiz	EGMR, Urteil vom 25.03.98 Nr. 23224/94 Rep. 1998-II
Kreuz./.Polen	EGMR, Urteil vom 19.06.01 Nr. 28249/95 RJD 2001-VI
Kruslin./.Frankreich	EGMR, Urteil vom 24.04.90 Nr. 11801/85 Serie A 176-A

Kvasnica./.Slovakei	EGMR, Urteil vom 09.06.09 Nr. 72094/01
L./.BRD	EKMR, Entscheidung vom 13.10.88 Nr. 12793/87
Lamy./.Belgien	EGMR, Urteil vom 30.03.89 Nr. 10444/83 Serie A 151
Leander./.Schweden	EGMR, Urteil vom 26.03.87 Nr. 9248/81 Serie A 116
Leander./.Schweden	EKMR, Bericht vom 17.05.85 Nr. 9248/81 Serie B99
Liberty./.Vereinigtes Königreich	EGMR, Urteil vom 01.07.08 Nr. 58243/00
Lundvall./.Schweden	EKMR, Entscheidung vom 01.12.85 Nr. 10473/83
Lupker./.Niederlande	EKMR, Entscheidung vom 07.12.92 Nr. 18395/91

M.G./.Vereinigtes Königreich	EGMR, Urteil vom 24.09.02 Nr. 39393/98
M.S./.Schweden	EGMR, Urteil vom 27.08.97 Nr. 20837/92 Rep. 1997-IV
Malone./.Vereinigtes Königreich	EGMR, Urteil vom 02.08.84 Nr. 8691/79 Serie A 82
Martin./.Schweiz	EKMR, Entscheidung vom 05.04.96 Nr. 25099/94 DR 81-B, 136
Martin./.Vereinigtes Königreich	EKMR, Entscheidung vom 28.02.96 Nr. 27533/95
McMichael./.Vereinigtes Königreich	EGMR, Urteil vom 24.02.95 Nr. 16424/90 Serie A 307-B
McVeigh u.a./. Vereinigtes Königreich	EKMR, Entscheidung vom 18.03.81 Nr. 8022/77, 8025/77 und 8027/77

Murray./.Vereinigtes Königreich	EGMR, Urteil vom 28.10.94 Nr. 14310/88 Serie A 300-A
Niedbala./.Polen	EGMR, Urteil vom 04.07.00 Nr. 27915/95
P.G. und J.H. /. Vereinigtes Königreich	EGMR, Urteil vom 25.09.01 Nr. 44787/98 RJD 2001-IX
Peck ./. Vereinigtes Königreich	EGMR, Urteil vom 28.01.03 Nr. 44647/98 RJD 2003-I
Perry./.Vereinigtes Königreich	EGMR, Urteil vom 17.07.03 Nr. 63737/00 RJD 2003-IX
Powell & Rayner./.Vereinigtes Königreich	EGMR, Urteil vom 21.02.90 Nr. 9310/81 Serie A 172
Pretty./.Vereinigtes Königreich	EGMR, Urteil vom 29.04.02 Nr. 2346/02 RJD 2002-III
Rasmussen./.Dänemark	EGMR, Urteil vom 28.11.84 Nr. 8777/79 Serie A 87

Rees./.Vereinigtes Königreich	EGMR, Urteil vom 17.10.86 Nr. 9532/81 Serie A 106
Rekvényi./.Ungarn	EGMR, Urteil vom 20.05.99 Nr. 25390/94 RJD 1999-III
Reyntjens./.Belgien	EKMR, Entscheidung vom 09.09.92 Nr. 16810/90
Rotaru./.Rumänien	EGMR, Urteil vom 04.05.00 Nr. 28341/95 RJD 2000-V
Rowe & Davis./.Vereinigtes Königreich	EGMR, Urteil vom 16.02.00 Nr. 28901/95 RJD 2000-II
Ruiz-Mateos./.Spanien	EGMR, Urteil vom 23.06.93 Nr. 12952/87 Serie A262
S. & Marper./.Vereinigtes Königreich	EGMR, Urteil vom 04.12.08 Nr. 30562/04 und 30566/04
Schüssel./.Österreich	EGMR, Urteil vom 21.02.02 Nr. 42409/98

Sciacca./.Italien	EGMR, Urteil vom 11.01.05 Nr. 50774/99 RJD 2005-I
Silver./.Vereinigtes Königreich	EGMR, Urteil vom 25.03.83 Nr. 5947/72 u.a. Serie A 61
Sporrong & Lönnroth./.Schweden	EGMR, Urteil vom 23.09.82 Nr. 7151/75, 7152/75 Serie A52
Sunday Times (Nr. 1)./.Vereinigtes Königreich	EGMR, Urteil vom 26.04.79 Nr. 6538/74 Serie A 30
Tsavachidis./.Griechenland	EKMR, Bericht vom 28.10.97 Nr. 28802/95
Tyrer ./. Vereinigtes Königreich	EGMR, Urteil vom 28.04.1978 Nr. 5856/72 Serie A 26
U./.BRD	EGMR, Urteil vom 02.09.10 Nr. 35623/05
Van der Velden./.Niederlande	EGMR, Urteil vom 07.12.06 Nr. 29514/05 RJD 2006-XV

Van Kück./.BRD	EGMR, Urteil vom 12.06.03 Nr. 35968/97 RJD 2003-VIII
Williams./.Vereinigtes Königreich	EKMR, Entscheidung vom 01.07.92 Nr. 19404/92
X./.Vereinigtes Königreich	EKMR, Entscheidung vom 12.10.73 Nr. 5877/72 CD 45, 90 ff.
X./.Österreich	EKMR, Entscheidung vom 13.11.79 Nr. 7987/77 DR 18, 41
X und Y ./. Niederlande	EGMR, Urteil vom 26.03.85 Nr. 8978/80 Serie A 91
Y.F./.Türkei	EGMR, Urteil vom 22.07.03 Nr. 24209/94 RJD 2003-IX
Z./.Finnland	EGMR, Urteil vom 25.02.97 Nr. 22009/93 Rep. 1997-I

Zumtobel./.Österreich	EGMR, Urteil vom 21.09.93 Nr. 12235/86 Serie A268-A

Lebenslauf

Persönliche Daten:

Name:	Carmen Fritz, geb. Hangl
Anschrift:	Althausstr. 4, 87544 Blaichach
Geburtsdatum/-ort:	04.11.1983/Immenstadt im Allgäu

Ausbildung:

09/1994 – 06/2003	Gertrud-von-le-Fort-Gymnasium Oberstdorf
09/2003 – 09/2007	Studium der Rechtswissenschaften an der Universität Regensburg
09/2007 – 01/2008	1. Juristische Staatsprüfung: „Dipl.-iur. (univ.)“
04/2010 – 04/2012	Rechtsreferendariat beim OLG München: „Ass. iur.“
10/2008 – 07/2012	Promotion zum Thema „Datenschutz und Rechtsschutz beim Austausch biometrischer Daten“

Referendariat:

04/2010 – 08/2010	Zivilstation beim Landgericht Kempten
09/2010 – 11/2010	Strafrechtsstation bei der StA Kempten
12/2010 – 03/2011	Verwaltungsstation beim LRA Oberallgäu
04/2011 – 12/2011	Station bei der Rechtsanwalts- und Patentkanzlei Kroher/Strobel in München im Markenrecht
01/2012 – 03/2012	Wahlstation beim Richard Boorberg Verlag in Stuttgart im Bereich Lektorat und Zeitschriftenredaktion

Beruf:

06/2007 – 12/2011	Berufliche Erfahrung als juristische Sachbearbeiterin in der Kanzlei Dr. Schmidt in Sonthofen
seit Oktober 2012	Gründung einer eigenen Rechtsanwaltskanzlei in Kempten

Eigene Vorträge:

18.12.2008	FOS Sonthofen: „Datenschutz im Internet: Communities, Chats und sonstige Problembereiche“
19.03.2010	FOS Sonthofen: „Sicher im Netz – Gefahren und Vorbeugung“
24.03.2010	Diskurs der Kanzlei Dr. Schmidt in Kempten: „Datenschutz im Unternehmen“ und „Recht und Internet – Ein Streifzug durch ausgewählte Rechtsgebiete“
30.07.2012	FOS Sonthofen: „Urheberrecht im Internet“

Schwerpunkte:	Urheber- und Medienrecht, Opferstrafrecht, Arbeitsrecht, Verkehrsrecht

Ausgewählte Artikel in Zeitschriften:

Publicus 03/2012	„Datenschutz im Wandel der Zeit“ – Interview mit Prof. Dr. Heckmann von der Universität Passau
Publicus 04/2012	„Polizei-Kompetenz in Europa“ – in Zusammenarbeit mit Hr. Hans-Jörn Bury

12. November 2012 Carmen Fritz