Plädoyer 2/05

Die Rechtszersplitterung schadet dem Persönlichkeitsschutz

Markus Schefer, Professor für Öffentliches Recht, Basel

Niemand weiss, wie stark der Persönlichkeitsschutz nach einem allfälligen Beitritt der Schweiz zum Schengener Abkommen eingeschränkt wird (siehe auch Astrid Epiney in plädoyer 1/05). Besonders problematisch: die geheime Weiterentwicklung der Schengener Fahndungsdatenbank (SIS II). Einem wirksamen Persönlichkeitsschutz steht die Rechtszersplitterung auf Ebene des Gemeinschafts- und des schweizerischen Rechts entgegen. Möglicher Ausweg: eine Rechtsharmonisierung im Bereich polizeilicher Datenbanken, nicht zuletzt in der Schweiz selbst.

Protection de la personnalité et harmonisation du droit dans le cadre de Schengen

Les bilatérales II traitent un large éventail de sujets différents, comme la coopération dans le domaine de la justice, de la police, de l'asile et de la migration, ainsi que l'environnement, les statistiques, la lutte contre la fraude, l'éducation, etc. Tous ces thèmes soulèvent la problématique de la protection de la personnalité, en particulier par l'adhésion du Système d'information Schengen (SIS). Dans cet article, Markus Schefer nous présente – entre autre – cette base de données informatisée contenant des renseignements sur les personnes et les objets recherchés.

Die Bilateralen II erfassen einen breiten Kreis unterschiedlicher Themenbereiche. Von der polizeilichen und justiziellen Zusammenarbeit über die Probleme des Asyls, der Zinsbesteuerung und Betrugsbekämpfung, Umwelt, Statistik bis zum Detailproblem der Ruhegehälter von EG-Beamten in der Schweiz. In allen diesen Bereichen stellen sich auch Fragen des Persönlichkeitsschutzes. Der vorliegende Beitrag beschränkt sich auf jenen Bereich, in welchem diese Probleme am offensichtlichsten sind. Dies ist zweifellos im Dossier Schengen/Dublin der Fall, über das im Rahmen des Staatsvertragsreferendums voraussichtlich am 5. Juni dieses Jahres eine Volksabstimmung stattfinden wird. Innerhalb dieses Dossiers steht die elektronische Datenbank SIS – Schengen Information System – im Zentrum.

1. «Schengen»: Für die Schweiz rechtlich komplex

Zunächst ist die die rechtliche Struktur des Rechtsgebildes «Schengen» kurz zu skizzieren. Dies erscheint besonders deshalb erforderlich, weil diese Struktur direkte Auswirkungen auf das jeweils anwendbare Datenschutzrecht hat, aber auch etwa auf die Zuständigkeiten zur Weiterentwicklung des heutigen Rechtszustandes und auf die Möglichkeiten gerichtlicher Kontrolle im Rahmen von Europäischer Gemeinschaft (EG) und Europäischer Union (EU).

Das Schengener Durchführungsübereinkommen (SDÜ) war ursprünglich, im Jahr 1990, als völkerrechtlicher Vertrag unabhängig von der EG von fünf europäischen Staaten (Benelux, Deutschland und Frankreich) abgeschlossen worden. Es trat im Jahr 1995 in Kraft.[1] Sein primäres Ziel bestand im Abbau der Personenkontrollen an den Grenzen.

Mit dem Vertrag von Amsterdam wurden mit den Art. 61 ff. neue Bestimmungen über die Visaerteilung, das Asylrecht und die polizeiliche und justizielle Zusammenarbeit in Strafsachen in den EG-Vertrag (EGV) eingefügt. Damit wurden der Gemeinschaft Zuständigkeiten zuerkannt, die einen wesentlichen Teil der vom Schengen-Recht abgedeckten Bereiche betreffen. Daraufhin wurde das bis dahin im Rahmen des Schengener Vertragswerks völkerrechtlich entwickelte Recht – der so genannte Schengen-Besitzstand[2] – in das Recht der EG und der EU überführt. Dies geschah mit dem Schengen-Protokoll[4] in der Schlussakte des Vertrags von Amsterdam. Der Rat stellte daraufhin für jede einzelne Bestimmung des Schengen-Besitzstandes die Rechtsgrundlage im EGV – erste Säule – und im EUV – dritte Säule – fest. Keine Einigung konnte aber über die Zuordnung der Bestimmungen über das Schengener Informationssystem (SIS) erzielt werden.[5] Sie gehören aufgrund der Auffangvorschrift Art. 2 Abs. 1 U Abs. 4 Schengen-Protokoll der dritten Säule im Rahmen des EUV an.

Die Teilnahme der Schweiz am Schengener Rechtsstoff ist in rechtstechnischer Hinsicht aufgrund dieser – vereinfacht dargestellten – Struktur auf Ebene von EG und EU einigermassen komplex.

Ein Beitritt zum SDÜ kam für die Schweiz nicht in Frage, weil dieser Vertrag nur Mitgliedern der Gemeinschaft offen stand und als völkerrechtlicher Vertrag in rechtstechnischer Hinsicht seit der Integration in das Gemeinschaftsrecht nicht mehr besteht.[6]

Die Schweiz hat deshalb – analog zu den Nicht-EG-Ländern Norwegen und Island – ein so genanntes «Assoziierungsabkommen» mit der EG und EU geschlossen (SAÜ).[7] Darin übernimmt die Schweiz das bisher zum SDÜ entwickelte Recht

– den gegenwärtigen Schengen-Besitzstand – und «akzeptiert» seine Weiterentwicklungen durch EG und EU.[3] Sollte sich die Schweiz gegen die Übernahme solcher Weiterentwicklungen aussprechen und beschliesst der Gemischte Ausschuss im Anschluss an Verhandlungen mit der Schweiz nicht, das Abkommen fortzuführen, fällt es automatisch dahin.

2. Personenkontrollen ohne jeden Verdacht höchst problematisch

a) Abschaffung der Grenzkontrollen geplant

Die Schweiz verpflichtet sich mit dem Assoziierungsabkommen, die routinemässigen, verdachtsunabhängigen Personenkontrollen an den Grenzen abzuschaffen. Die Staaten dürfen – müssen aber nicht – dafür gewisse Ersatzmassnahmen im Landesinnern durchführen. So führt etwa die Bundesrepublik[4] in einem Grenzstreifen von 30 Kilometern mobile Personenkontrollen durch, die nicht an einen spezifischen Verdacht oder besonderes Ereignis anknüpfen.[10]

Die Übernahme einer solchen Regelung in der Schweiz erschiene höchst problematisch: Nicht nur in Grenzstädten wie Basel und Genf, sondern auch etwa in Zürich, St. Gallen, Biel oder Chur wären generell polizeiliche Personenkontrollen ohne jeden Anfangsverdacht möglich.[11] Innerhalb des Gebiets der Schweiz ist aber die Anhaltung von Personen zur Identitätsfeststellung nur aufgrund eines spezifischen Verdachts oder aufgrund besonderer Ereignisse zulässig.[12] Aus Sicht des Persönlichkeitsschutzes ist deshalb der Vorstoss der EG-Kommission vom 26. Mai 2004[13] zu begrüssen, die systematische Schleierfahndung im Grenzgebiet abzuschaffen.[14] Hier sind andere Massnahmen zu erwägen.[15]

b) SIS für Persönlichkeitsschutz bedrohlich

Als weitere Kompensation wird die Zusammenarbeit im Bereich der Polizei gestärkt. Eine für den verfassungsrechtlichen Persönlichkeitsschutz besonders bedeutsame Kooperation findet im Rahmen des Schengener Informationssystems SIS statt. Darauf ist im Folgenden näher einzugehen.

Das SIS stellt ein elektronisches Verbundsystem dar, in welchem Daten über Personen und Sachen gespeichert sind. Jeder Schengen-Staat verfügt über eine nationale Einheit (N-SIS), in die er selber Daten eingibt und über die er Daten abfragt. Eine zentrale, in Strassburg stationierte Einheit (C-SIS) gleicht die zahlreichen nationalen Einheiten stets ab, so dass diese immer auf dem gleichen Stand sind.[16]

Die Mitgliedsstaaten können in dieses System Daten unter anderem zu folgenden Zwecken eingeben: Ausschreibung einer Person zur Festnahme, Ausschreibung von Drittausländern zur Einreiseverweigerung, es können vermisste oder vorläufig in Gewahrsam genommene Personen ausgeschrieben werden, Zeugen oder Verdächtige zur Ermittlung ihres Aufenthaltsorts gespeichert, oder Personen zur verdeckten Registrierung oder gezielten Kontrolle eingegeben werden.[17] Heute enthält es zwischen 11 und 12 Millionen Einträge. Gegenwärtig sind rund 15 000 Personen zur Festnahme ausgeschrieben und rund 800 000 Personen mit ausländerrechtlichen Fernhaltemassnahmen. Die restlichen zehn Millionen Einträge betreffen Sachfahndungen, etwa gestohlene Fahrzeuge.[18] Im Bereich der Personendaten stellt das SIS dementsprechend nummerisch überwiegend ein ausländerrechtliches Instrument dar.

Im Bereich der Straftaten dient das SIS zudem nicht nur der Aufklärung vollendeter Taten, sondern hat auch

Ich danke meinen Mitarbeitern RA lic. iur. Andreas Reller, LL.M., und Alan Cleis herzlich für die intensive Literaturrsuche.

1 Am 14. Juni 1985 hatten die Regierungen der fünf Staaten das Übereinkommen betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen geschlossen.

2 Zur Entwicklung siehe Astrid Epiney, Das zweite Schengener Abkommen: Entstehung, Konzept und Einbettung in die Europäische Union, in: Achermann/Bieber/Epiney/Wehner, Schengen und die Folgen, Bern/München/Wien 1995, S. 22–26.

3 Der Schengen-Besitzstand findet sich zusammengetragen in: ABl. L 239 vom 22. September 2000, S. 1 ff.

4 Das Schengen-Protokoll steht als Primärrecht auf der selben Stufe wie EUV und EGV; siehe Astrid Epiney, Die Übernahme des «Schengen-Besitzstandes» in die Europäische Union, in: Waldemar Hummer (Hrsg.), Die Europäische Union nach dem Vertrag von Amsterdam, Wien 1998, S. 107.

5 Siehe Charles Elsen, Die Übernahme des «Schengen-acquis» in den Rahmen der EU, in: Waldemar Hummer (Hrsg.), Rechtsfragen in der Anwendung des Amsterdamer Vertrages, Wien 2001, S. 45.

6 Bieber/Epiney/Haag, Die Europäische Union, 6. Auflage Baden-Baden 2005, § 14, Rz. 72. Eine Ausnahme gilt mit Bezug auf Dänemark, das auch heute noch auf völkerrechtlicher Basis an Schengen teilhat, da es den Vertrag von Amsterdam nicht ratifiziert hat.

7 BBl 2004, S. 6447 ff.

8 Art. 2 Abs. 3 SAÜ.

9 Siehe im Bund § 2 Abs. 1 Ziff. 3 BGSG (Gesetz über den Bundesgrenzschutz vom 19. Oktober 1994, BGBl. 1994 I S. 2978 f.); in Bayern Art. 13 Abs. 5 PAG (Polizeiaufgabengesetz vom 14. September 1990).

10 Der Bayrische Verfassungsgerichtshof erachtet diese verdachts- und anlassunabhängigen Personenkontrollen im 30-Kilometer-Bereich als verfassungskonform; siehe BayVerfGH, Urteil vom 28. März 2003; Az.: 7-VII-00 und 8-VIII-00, VerfGH 56, 28, zugänglich unter www.bayern.verfassungsgerichtshof.de/ unter «Ausgewählte Entscheidungen». Als verfassungswidrig erachtet sie aber das Landesverfassungsgericht Mecklenburg-Vorpommern in einem Urteil vom 22. Oktober 1999, Az.: LVerfG 2/98, vgl. zu diesem Entscheid Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern, 4. Tätigkeitsbericht, S. 25 f., zugänglich unter www.lfd.m-v.de/taetberi/tb4/lfdmvtb4.pdf.
Kritisch zur Schleierfahndung etwa Martin Herrnkind, «Schleierfahndung» – Institutionalisierter Rassismus und weitere Implikationen so genannter verdachtsunabhängiger Polizeikontrollen, in: Komitee für

stark präventiven Charakter.[19] So lässt Art. 99 Abs. 3 SDÜ einen Eintrag schon dann zu, «wenn tatsächliche Anhaltspunkte dafür vorliegen, dass die (gespeicherten) Informationen zur Abwehr einer von dem Betroffenen ausgehenden erheblichen Gefährdung oder anderer erheblicher Gefahren für die innere oder äussere Sicherheit des Staates erforderlich sind». Diese Bestimmung erscheint zu unbestimmt, um als Grundlage für einen Eintrag zu dienen. Im schweizerischen Recht sind die Voraussetzungen an solche präventiven Einträge präziser und enger zu umschreiben.

3. SIS: Informationelle Selbstbestimmung in Frage gestellt

Im Folgenden ist näher auf den Schutz der informationellen Selbstbestimmung unter dem heute bestehenden SIS einzugehen. Dafür wird exemplarisch der Fall einer Ausschreibung zur Festnahme und Auslieferung herangezogen.

a) Zulässigkeit einer Ausschreibung

aa) Zulässigkeit der nachgesuchten Massnahme

Die Zulässigkeit einer Festnahme beurteilt sich nach dem Recht jenes Staates, der sie vornimmt.[20] Der Staat, der eine Person zur Festnahme ausschreibt, muss deshalb prüfen, ob die Festnahme nach dem Recht des ersuchten Staates zulässig ist.[21] Hat er Zweifel daran, muss er den ersuchten Staat konsultieren.[22]

Der ersuchte Staat kann zwar eine Ausschreibung, die gegen sein nationales Recht verstösst, kennzeichnen, so dass auf seinem Gebiet keine Festnahme erfolgt. Dies hat aber nicht zur Folge, dass die Ausschreibung gelöscht wird. Sie wird vielmehr als Ausschreibung zur Ermittlung des Aufenthalts der gesuchten Person behandelt. Damit bleibt ein klares Verdachtsmoment im SIS bestehen, obwohl im fraglichen Staat die Voraussetzungen zur Ausschreibung für eine Festnahme nicht vorliegen. Zudem hat eine Kennzeichnung keinen Einfluss auf die Fahndung in den übrigen Schengen-Staaten.[23]

bb) Zulässiger Inhalt der Eintragung: Anwendbares Recht

Die datenschutzrechtliche Zulässigkeit einer Ausschreibung beurteilt sich demgegenüber nicht nach dem Recht des ersuchten Staates. Grundsätzlich ist das nationale Recht der ausschreibenden Vertragspartei anwendbar.[24] Die Kriterien, die für einen Eintrag in das SIS erfüllt sein müssen, werden im SDÜ festgelegt und sind im nationalen Recht zu konkretisieren. Dieses muss zudem den Minimalstandards[25] des Übereinkommens des Europarats über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981[26] genügen.[27] Das SDÜ ist dabei wenig präzise gefasst, so dass den Staaten ein grosser Spielraum bleibt. So hat sich etwa die Praxis zur Eintragung von Drittausländern, die zur Einreiseverweigerung ausgeschrieben sind (Art. 96 SDÜ), höchst uneinheitlich entwickelt.[28]

Entsprechend der Anwendbarkeit des Datenschutzrechts des ausschreibenden Staates ist er auch verantwortlich dafür, dass die von ihm in das SIS eingegebenen Daten richtig und aktuell sind.[29] Schreibt beispielsweise eine französische Behörde einen Verdächtigen zur Verhaftung aus, ist sie für die dabei verwendeten Daten verantwortlich; nur sie kann diese Daten ändern, ergänzen, berichtigen oder löschen. Erachtet zum Beispiel die Schweiz, auf deren Gebiet sich der Gesuchte befindet, diese Daten für unrichtig oder ihre Speicherung als unrechtmässig, kann sie selber keine Korrekturen vornehmen. Sie teilt ihre Vorbehalte den französischen Behörden mit, die verpflichtet sind, diese Mitteilung unverzüglich zu prüfen und falls nötig zu korrigieren.

Eine wirksame gerichtliche Kontrolle bei Meinungsverschiedenheiten zwischen den Staaten fehlt jedoch: Es besteht nur die Möglichkeit, die Angelegenheit der «gemeinsamen Kontrollinstanz» zur Stellungnahme vorzulegen.[30] Diese prüft, ob das Europarats-Übereinkommen eingehalten wird.[31] Ihre Berichte sind jedoch für die Mitgliedstaaten rechtlich nicht bindend.[32] Daran hat die Überführung von Schengen in das Recht der EG und EU nichts geändert. Auch dem EuGH kommt in diesem Bereich keine Zuständigkeit zu.[33]

Die Schweiz kann aber im Falle der Weigerung Frankreichs, unzulässige Daten zu berichtigen oder zu löschen, die Ausschreibung kennzeichnen und auf ihrem Gebiet nicht vollziehen, wenn dies gegen ihr innerstaatliches Recht verstossen würde.[34]

b) Zugriff auf SIS-Daten nach Landesrecht

Der Zugriff auf Daten im SIS erfolgt nach dem Recht jedes einzelnen Staates und untersteht gewissen Vorschriften des SDÜ. Dieses regelt etwa, dass nur jene Behörden direkten Zugang zum SIS haben, die für Grenzkontrollen und sonstige polizeiliche und zollrechtliche Überprüfungen im Inland zuständig sind.[35] Daten über Drittausländer, die zur Einreiseverweigerung ausgeschrieben sind, dürfen auch von den Fremdenpolizei-Behörden eingesehen werden.[36]

Der Betrieb des SIS wird im schweizerischen Recht auf Ebene des formellen Gesetzes in einem neuen Art. 351^{decies} StGB geregelt. Diese Bestimmung ist mit acht Absätzen und gesamthaft 27 literas recht umfangreich. Sie umschreibt abschliessend die Zwecke, die mit dem SIS verfolgt werden dürfen. Die Fragen der Zugriffsberechtigung zu Daten des SIS,

der Aufbewahrungsdauer, die Rechte der Einzelnen unter anderem werden dagegen an den Bundesrat delegiert. Dies ist insbesondere deshalb von Bedeutung, weil damit eine Weiterentwicklung des SIS durch die EU im innerstaatlichen Verhältnis der Schweiz jedenfalls in datenschutzrechtlicher Hinsicht weit gehend durch blosse Anpassung einer bundesrätlichen Verordnung übernommen werden könnte.

c) Recht auf Einsicht, Löschung und Korrektur unpräzis

Art. 13 der Bundesverfassung[37] gewährleistet den Einzelnen direkt gewisse Ansprüche auf Einsicht, Berichtigung und allenfalls Löschung der über sie gespeicherten Daten.[38] Das SDÜ enthält analoge Ansprüche[39] und konkretisiert sie in gewissem Masse. Diese datenschutzrechtlichen Bestimmungen sind grossteils zwar direkt anwendbar (self-executing)[40], im Einzelnen aber wenig präzise gefasst. Deshalb verweist das SDÜ für deren konkrete Ausgestaltung aber auf das Recht der einzelnen Staaten.[41] In der Schweiz werden diese Ansprüche näher in der erwähnten Verordnung des Bundesrates geregelt.[42] Diese muss jedenfalls den Anforderungen von Art. 13 BV, des SDÜ sowie des Europarats-Übereinkommens genügen.

Der Einzelne kann die Rechte auf Einsicht, Berichtigung und Löschung in jedem Schengen-Staat geltend machen.[43] Anwendbar ist dabei das Recht jenes Staates, in dem er den Anspruch stellt.[44] Verlangt ein Betroffener Einsicht in Daten, die nicht vom Staat, in dem er den Fall anhängig macht, in das SIS eingegeben worden sind, muss der ersuchte Staat vor Erteilung der Auskunft dem ausschreibenden Staat Gelegenheit zur Stellungnahme geben.[45] Die Vertragsstaaten verpflichten sich, rechtskräftige Entscheide von Gerichten oder Behörden über solche Ansprüche zu vollziehen.[46]

Positiv ist dazu zu bemerken, dass diese Regelung dem Rechtsuchenden ermöglicht, seine datenschutzrechtlichen Ansprüche auch dann in seinem eigenen Land anhängig zu machen, wenn die fraglichen Daten über ihn von einem andern Staat in das SIS eingegeben worden sind. Der Staat, in dem etwa das Berichtigungsverfahren geführt worden ist, kann aber selber keine Berichtigungen vornehmen oder die Daten löschen. Dazu ist nur jener Staat zuständig, der die Daten eingegeben hat. Wenn dieser nun aber zum Vollzug fremder Urteile verpflichtet ist, das heisst, wenn etwa die französischen Behörden ein schweizerisches Urteil vollziehen müssen, das die Löschung anordnet, erscheint nicht ganz einsichtig, weshalb die schweizerischen Behörden nicht gleich selber auch für den Vollzug sorgen und die Berichtigung oder Löschung vornehmen können.

Die skizzierte Regelung weist aber auch auf ein grundlegendes Problem des gesamten Rechtsstoffes von Schengen und Dublin hin, nämlich die mangelnde Harmonisierung des Rechts und die dadurch entstehende enorme Komplexität der Regelungen: Indem die datenschutzrechtlichen Ansprüche primär je landesrechtlich geregelt sind, bleibt der Datenschutz im Zusammenhang mit den SIS äusserst stark fragmentiert. Diese Zersplitterung wird durch die Bindung der einzelnen Länder an das SDÜ und das Europarats-Übereinkommen nur unzureichend gemildert. Darunter kann die tatsächliche Umsetzung des notwendigen Datenschutzes in der täglichen Rechtspraxis leiden.

d) Staatshaftung zum Vorteil der Ratsuchenden geregelt

Wird die Persönlichkeit eines Betroffenen durch den Betrieb des SIS verletzt, stellt sich besonders die Frage nach einem allfälligen Schadenersatz. Sowohl das SDÜ selber als auch die Umsetzung im schweizerischen Recht regeln die Staatshaftung auf-

Grundrechte und Demokratie (Hrsg.), Verpolizeilichung der Bundesrepublik Deutschland, Polizei und Bürgerrechte in den Städten: Dokumentation einer Tagung des Komitees für Grundrechte und Demokratie in Kooperation mit der Evangelischen Akademie Arnoldshain, vom 15. bis 17. September 2000 in Arnoldshain, Köln 2002, S. 99 ff., Martina Kant, «Evaluation» der Schleierfahndung, in: Bürgerrechte & Polizei, CILIP 77 (1/2004), S. 46 ff.

11 Von den grösseren Schweizer Städten würden nur Bern, Luzern und Thun nicht in die 30-Kilometer-Zone fallen.

12 Siehe Robert Hauser / Erhard Schweri / Karl Hartmann, Schweizerisches Strafprozessrecht, 6. Auflage Basel/Genf/München 2005, § 68, Rz. 23a; Niklaus Schmid, Strafprozessrecht, 4. Auflage Zürich 2004, Rz. 710a. Auch der Uno-Menschenrechtsausschuss verlangt im Rahmen von Art. 17 Uno-Pakt II, dass ein Eingriff in den Schutz der Privatsphäre auf einer «case-by-case»-Basis vorgenommen wird; siehe General Comment 16 (1988), Ziff. 8.

13 Vorschlag für eine Verordnung des Rates über den Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen vom 26. Mai 2004, KOM(2004) 391 endg., Art. 19 lit. a.

14 Gegen eine Abschaffung der Schleierfahndung allerdings etwa die Bayerische Landesregierung, Pressemitteilung der Bayerischen Staatskanzlei vom 9. November 2004, Ziff. 3.

15 Einen Überblick über diskutierte kompensatorische Massnahmen gibt der Bericht des Bundesamtes für Polizei, Sicherheitssystem der Schweiz mit Schengen/Dublin: Vertiefung der Planungsvarianten Kombi und Kantone aus USIS IV vom 15. Juni 2004, S. 6, sowie den Bericht des Bundesamtes für Polizei, USIS: Überprüfung des Systems der inneren Sicherheit der Schweiz, Teil IV, vom 30. November 2003, S. 66.

16 Siehe etwa die Beschreibungen des SIS in Hans Claudius Taschner, Schengen: die Übereinkommen zum Abbau der Personenkontrollen an den Binnengrenzen von EU-Staaten, Baden-Baden 1997, S. 42 ff.; Susanne Scheller, Das Schengener Informationssystem – Rechtshilfeersuchen «per Computer», JZ 1992, S. 904; Ruth Wehner, Die polizeiliche Zusammenarbeit zwischen den Schengen-Staaten unter besonderer Berücksichtigung des SIS, in: Achermann/Bieber/Epiney/Wehner, Schengen und die Folgen, Bern/München/Wien 1995, S. 133 ff.

17 Art. 95100 SDÜ.

18 Siehe dazu die Botschaft zur Genehmigung der bilateralen Abkommen zwischen der Schweiz und der Europäischen Union, einschliesslich der Erlasse zur Umsetzung der Abkommen (Bilaterale II) vom 1. Oktober 2004, BBl 2004, S. 6083.

grund des Betriebs des SIS in einer für den Rechtsuchenden freundlichen Weise: Auf überstaatlicher Ebene haftet jeder Staat nach Massgabe seines eigenen Verantwortlichkeitsrechts. Dies besonders auch dann, wenn der Schaden durch fehlerhafte Dateneingabe oder unrechtmässige Speicherung verursacht worden ist, für die der belangte Staat nicht verantwortlich ist. Der zu Schadenersatz verpflichtete Staat kann in diesem Fall Regress auf den ausschreibenden Staat nehmen.[47]

Auf innerstaatlicher Ebene soll das Verantwortlichkeitsgesetz für Schäden aus dem Betrieb des SIS ergänzt werden.[48] Dessen Bestimmungen finden unabhängig davon Anwendung, ob die schädigende Handlung vom Bund oder einem Kanton ausgeht. Auch die Zuständigkeit zur Beurteilung von Staatshaftungsfragen liegt stets beim Bund. Mit der Möglichkeit des Regresses kann der Bund gegebenenfalls auf den fraglichen Kanton zurückgreifen. Dadurch besteht ein einheitlicher materieller Haftungsmassstab, der bei einem Gemeinwesen – dem Bund – mit einem Verfahrensrecht geltend gemacht werden kann.[49] Ohne diese Vereinheitlichung hätte der Persönlichkeitsschutz letztlich an den sowohl materiellen als auch formellen höchst unterschiedlichen Regelungen der 26 Kantone in der Praxis leicht scheitern können.

4. Weiterentwicklung SIS: Mehr Daten und neue Verknüpfungen

Die Schweiz wird das bisher skizzierte System des SIS auch im Falle der Ratifikation des Assoziierungsabkommens zu Schengen nicht übernehmen.[50] Es ist für maximal 18 Benutzerstaaten ausgelegt und stösst damit durch die Erweiterung der EU an seine technischen Grenzen. Der zuständige Rat der Europäischen Union wird Frühjahr 2005 über die Ausgestaltung eines neuen Systems entscheiden. Mit dem technischen Neuaufbau – SIS II genannt – geht voraussichtlich auch eine markante Ausdehnung sowohl der aufgenommenen Daten als auch der Möglichkeiten von Abfragen einher.

Zur Diskussion steht etwa, neue Ausschreibungskategorien aufzunehmen, automatisierte Verknüpfungsmöglichkeiten zwischen ihnen herzustellen[51], zusätzliche biografische und polizeiliche Personen- und Sachenmerkmale zu speichern, Recherchen nach bestimmten Personenprofilen europaweit zu ermöglichen (Rasterfahndung), oder etwa biometrische Daten wie Lichtbilder oder Gesichtserkennungsmerkmale aufzunehmen. Zudem soll der Kreis der Behörden erweitert werden, die eine Zugriffsberechtigung auf das SIS II haben. In der Literatur wird diesbezüglich verschiedentlich auch die Zugriffsberechtigung etwa von Kreditinstituten oder Fluggesellschaften erwähnt.[52]

Diese und weitere Vorschläge sind für die Öffentlichkeit nicht zugänglich und können deshalb auch nicht vertieft diskutiert werden. Darin kommt ein zentrales Problem dieses Projekts zum Ausdruck: So wurde im letzten Herbst mit einer privaten Firma ein Vertrag über 40 Millionen Euro für die technische Entwicklung von SIS II abgeschlossen.[53] Die Debatte über die materielle Erweiterung des neuen Systems findet aber ohne nennenswerte öffentliche Beteiligung statt.[54] Angesichts der enormen Tragweite von SIS II für den Schutz der Persönlichkeit der Einzelnen wäre eine vertiefte demokratische Auseinandersetzung darüber unabdingbar.

Auch in der Schweiz wäre eine vertiefte, offene Diskussion über diese Fragen zentral. Dass sie nicht möglich ist, hängt nicht nur mit den Eigenheiten des Rechtsetzungsverfahrens in der EU zusammen. Auch der Bundesrat deutet in seiner Botschaft zu den Bilateralen II die Entwicklung von SIS II nur sehr vorsichtig an,[55] ohne auf die grundrechtliche Tragweite dieser Weiterentwicklung des Schengen-Besitzstandes hinzuweisen. So hält er lakonisch fest: «Die laufenden Arbeiten zur Entwicklung des SIS II sowie die übrigen in Vorbereitung befindlichen Weiterentwicklungen werden nicht zu nennenswerten Veränderungen der aktuellen Schengener Zusammenarbeitsmechanismen führen. Auch der Datenschutzstandard wird aufrechterhalten.»[56] Dies erscheint angesichts des Ausbaus von SIS zu einem «umfassenden polizeilichen Informationssystem»[57] jedenfalls sehr zurückhaltend.

Im Schengener Assoziierungsabkommen verpflichtet sich die Schweiz, Weiterentwicklungen des Schengen-Besitzstandes zu übernehmen. Sie behält aber – wie eingangs erwähnt – die Möglichkeit, eine Übernahme zu verweigern, allerdings unter Umständen um den Preis des Wegfalls des ganzen Vertrages. Würde das SIS II gegenüber dem heutigen SIS den Kreis der Zwecke erweitern, für die es verwendet wird – was zu erwarten ist –, wäre eine Änderung des neuen Art. 351$^{\text{decies}}$ StGB erforderlich.[58] In diesem Rahmen wäre dann die hier geforderte vertiefte demokratische Auseinandersetzung zu führen.

Damit würde ein Kernpunkt des Schengener Abkommens in der Schweiz gleich zweimal dem Referendum unterstellt: Gegenwärtig im Rahmen der Ratifikation des Assoziierungsabkommens und in vielleicht zwei oder drei Jahren mit der Änderung von Art. 351$^{\text{decies}}$ StGB.

Die Schaffung automatisierter Verknüpfungsmöglichkeiten bei einer Suche auf dem SIS II, die Verlängerung der Fristen einer Ausschreibung und der Datenlöschung, oder etwa die Erfassung von biometrischen Daten von Personen, könnten dagegen wohl durch Anpassung

der bundesrätlichen Verordnung übernommen werden, ohne Referendumsmöglichkeit.[56]

5. Weitere sensible Bereiche: Asyl- und Visadatenbanken

Die bisherige Darstellung beschränkte sich auf einen Teilbereich eines der acht Abkommen, nämlich auf das SIS im Rahmen des umfassenden Abkommens zur Kooperation im Bereich von Polizei und Justiz. Dabei wurde deutlich, dass die Übernahme des Schengen-Besitzstandes ziemlich komplex ist, weil in wesentlichen Bereichen keine volle Harmonisierung des anwendbaren Rechts erfolgt. Darin besteht gerade im Hinblick auf den Persönlichkeitsschutz ein zentrales Problem des Assoziierungsabkommens mit Schengen, aber auch jenes mit Dublin. Dieser Eindruck verstärkt sich noch, wenn das weitere rechtliche Umfeld des SIS mit einbezogen wird.

Zusätzlich zum SIS besteht im Rahmen des SDÜ ein weiteres System zum Datenaustausch, das so genannte SIRENE (Supplementary information request at the national entry). Jeder Schengen-Staat richtet ein SIRENE-Büro ein, das die zentrale Anlauf-, Koordinations-, Konsultationsstelle im Umgang mit dem SIS darstellt.[58] Darüber hinaus dient es aber auch dazu, bei positiven Abfragen auf dem SIS den zuständigen Stellen einen zusätzlichen Informationsaustausch zu ermöglichen.[59] Diese weiteren Datenübermittlungen beruhen aber auf bilateralen Übereinkommen und dem jeweiligen nationalen Recht.[60]

Ebenfalls im Rahmen von Schengen werden Daten auch etwa im Zusammenhang mit den Möglichkeiten der Polizeiorgane zur Nacheile über die Grenze[61], der grenzüberschreitenden Observation[62], der Einsetzung von Verbindungsbeamten der Polizei[63] oder dem Informationsaustausch zwischen Polizeibehörden ausserhalb des SIS[64] zwischen den verschiedenen Staaten ausgetauscht. Auf diese Datenweitergaben finden spezifische Bestimmungen des SDÜ[65] und entsprechende Normen des innerstaatlichen Rechts[66] Anwendung. Das nationale Recht ist dabei nicht – wie beim SIS – an das Europarats-Übereinkommen gebunden, sondern an die EG-Datenschutzrichtlinie[67]. Darüber verfügt die Schweiz bereits heute – mit Deutschland, Österreich, Frankreich, Italien, Liechtenstein und Ungarn[68] – bilaterale Koopertionsabkommen, die über das SDÜ hinausgehen. Diese bleiben nach wie vor gültig und können auch neu geschlossen werden.[69] In ihrem Rahmen können wiederum spezifische Datenschutzregelungen zur Anwendung kommen. Darüber hinaus sind die spezifischen waffenrechtlichen Vorschriften von Schengen[70] innerstaatlich unter anderem mit besonderen datenschutzrechtlichen Bestimmungen im Waffengesetz[71] umzusetzen. Analoges gilt für die Schengen-Vorschriften über die Betäubungsmittel.[72]

Zudem entsteht mit dem VIS eine weitere neue Datenbank für den Bereich der Erteilung von Visa. Dieses neue System soll jedenfalls in technischer Hinsicht mit dem SIS II integriert werden.[73] Aber auch in inhaltlicher Hinsicht dürften sich das SIS II und das VIS einander stark annähern:[74] Schon das heutige SIS enthält eng damit zusammenhängend auch Daten über Drittausländer, die zur Einreiseverweigerung ausgeschrieben sind. Im Rahmen von SIS II soll diese Kategorie ausgedehnt werden.

Anders als beim SIS II legt aber beim VIS nicht das Europarats-Übereinkommen den datenschutzrechtlichen Minimalstandard fest; vielmehr findet die EG-Datenschutzrichtlinie Anwendung. Entsprechend entsteht die Situation,

16 Dazu etwa Nikolaos Lavranos, Datenschutz in Europa am Beispiel der Datenschutzrichtlinie, des Schengen Information System (SIS) und Europol, in: Datenschutz und Datensicherheit (DuD) 1996, S. 400 ff.
20 Art. 104 Abs. 3 Satz 1 SDÜ.
21 Art. 95 Abs. 2 Satz 1 SDÜ.
22 Art. 95 Abs. 2 Satz 2 SDÜ.
23 Zum Ganzen Rainer Oberleitner, Schengen und Europol: Kriminalitätsbekämpfung in einem Europa der inneren Sicherheit, Wien 1998, S. 76.
24 Art. 104 Abs. 1 SDÜ.
25 Siehe Art. 11 des Übereinkommens.
26 SR 0.235.1.
27 Darüber hinaus ist auch die Empfehlung R (87) 15 des Ministerkomitees des Europarates über die Nutzung personenbezogener Daten im Polizeibereich vom 17. September 1987 zu beachten; siehe Art. 117 Abs. 1 SDÜ.
28 Siehe dazu Madeleine Colvin, The Schengen Information System: A Human Rights Audit, European Human Rights Law Review 2001, S. 274 f. Deutschland trägt solche Personen regelmässig in das SIS ein. Der französische Conseil d'Etat erachtet dies als rechtswidrig; siehe Entscheid N° 190384 vom 9. Juni 1999.
29 Art. 105 SDÜ.
30 Art. 106 Abs. 3 SDÜ.
31 Art. 115 Abs. 1 SDÜ.
32 Siehe Botschaft (Anm. 18), S. 6092.
33 Der EuGH ist für solche Streitigkeiten nicht zuständig. Siehe Art. 35 Abs. 5 EUV, wonach Anordnungen der Polizei und anderer Strafverfolgungsbehörden im Einzelfall nicht auf ihre Gültigkeit und Verhältnismässigkeit überprüft werden können; dazu Martin Wasmeier, in: von der Groeben/Schwarze, Vertrag über die Europäische Union und Vertrag zur Gründung der Europäischen Gemeinschaft: Kommentar, Band 1 Baden-Baden 2003, Art. 35 EU, Rz. 13 ff. Dies gilt auch für die obligatorische Zuständigkeit nach Art. 35 Abs. 7 EUV. In anderen Bereichen des SDÜ kann dem EuGH demgegenüber eine Zuständigkeit zukommen; vgl. etwa Rs. C-187/01 – Gözütok und C-385/01 – Brügge, vom 11. Februar 2003.
34 Art. 94 Abs. 4 SDÜ.
35 Art. 101 Abs. 1 SDÜ.
36 Art. 101 Abs. 2 SDÜ.
37 Entsprechend auch Art. 8 EMRK, siehe etwa Christoph Grabenwarter, Europäische Menschenrechtskonvention, München 2003, S. 206–208, und Richard Clayton / Hugh Tomlinson, The Law of Human Rights, Oxford 2000, Rz. 12.88–12.94 und dazu Supplement 2003, Rz. 12.90–12.93; sowie Art. 17 Uno-Pakt II, siehe General Comment 16/1988, Ziff. 10. Aus der Literatur siehe Lee A. Bygrave, Data Protection Pursuant to the Right to Privacy in Human Rights Treaties, 6 Inter-

dass auf zwei Datenbanken, die auf der gleichen technischen Basis operieren und entsprechend von denselben Personen bedient werden, und die zum Teil dieselben Daten enthalten, zahlreiche unterschiedliche rechtliche Regelungen zum Persönlichkeitsschutz zur Anwendung kommen, sowohl auf europarechtlicher als auch auf schweizerischer Ebene.

Diese Rechtszersplitterung wird durch die weiteren Datenbanken, die mit Schengen und Dublin eingerichtet werden, noch verschärft. So tritt in engem sachlichen Zusammenhang mit SIS II und VIS im Rahmen des Dubliner Assoziierungsabkommens die Datenbank EURODAC hinzu[77], die den Austausch von Fingerabdrücken von Asylbewerbern und illegal eingereisten Ausländern ermöglicht[78]. Die Dublin-Verordnung des Rates[79], der sich die Schweiz anschliesst, enthält zahlreiche datenschutzrechtliche Bestimmungen[80], ebenfalls die EURODAC-Verordnung[81]. Subsidiär kommt die EG-Datenschutzrichtlinie zur Anwendung. Für die Erhebung und Übermittlung von Fingerabdrücken ist darüber hinaus das nationale Recht anwendbar, in der Schweiz etwa das entprechend revidierte ANAG[82] und AsylG[83].

6. Harmonisierung des Rechts auch in der Schweiz nötig

Das Recht zum Schutz der Persönlichkeit im Zusammenhang mit Schengen und Dublin ist sowohl auf der Ebene des Gemeinschaftsrechts als auch des allfälligen künftigen schweizerischen Rechts ausserordentlich stark zersplittert. Dies ruft die Gefahr hervor, dass die zahlreichen unterschiedlichen Regelungen im praktischen Alltag nicht mit der nötigen Stringenz angewandt werden und letztlich der Persönlichkeitsschutz darunter leidet.[84] Es drängt sich deshalb auf, in rechtlicher Hinsicht auf eine verstärkte Harmonisierung des Rechts hinzuwirken.[85]

Auf der Ebene des Gemeinschaftsrechts hat die Schweiz diesbezüglich nur sehr beschränkte Einflussmöglichkeiten. Auf innerstaatlicher Ebene steht es ihr aber frei, wie sie die europarechtlichen Minimalvorgaben umsetzen will. So wäre ernsthaft zu erwägen, zum Beispiel die zahlreichen unterschiedlichen Einzelbestimmungen über den Persönlichkeitsschutz im Zusammenhang mit polizeilichen Datenbanken nach Möglichkeit materiell zu harmonisieren und rechtstechnisch übersichtlich zusammenzufassen. Darüber hinaus wäre zu erwägen, dabei auch die heute schon stark fragmentierten Regelungen der verschiedenen nationalen Datenbanken[86] miteinzubeziehen. Der Bundesrat hat am 15. März 2005 eine entsprechende Vernehmlassung eröffnet.[87] Auch so blieben noch immer die 26 Kantone mit ihren je eigenen Bestimmungen.

national Journal of Law and Information Technology 247, 252 ff., 254 ff. (1998).

38 Siehe die Übersicht bei Jörg Paul Müller, Grundrechte in der Schweiz, 3. Aufl. Bern 1999, S. 44 ff., und Markus Schefer, Grundrechte in der Schweiz, Ergänzungsband, Bern 2005, S. 32–39 (erscheint Anfang April 2005).
Eingehend zur Geltung des entsprechenden Grundrechts nach Art. 2 Abs. 1 GG im grenzüberschreitenden Kontext siehe Manfred Baldus, Transnationales Polizeirecht, Baden-Baden 2001, S. 190 ff.

39 Art. 109 ff. SDÜ.

40 Botschaft (Anm. 18), S. 6151.

41 Dazu etwa Madeleine Colvin, The Schengen Information System: A Human Rights Audit, European Human Rights Law Review 2001, S. 273.

42 Siehe die Delegationsnorm in Art. 351^{decies} Abs. 7 StGB. Abs. 8 dieser Bestimmung hält fest, dass in jenen Fällen, in denen Daten aus dem JANUS in das SIS übertragen werden, weiterhin nur das «indirekte Auskunftsrecht» nach Art. 18 BWIS (SR 120) und Art. 14 ZentG (SR 360) gewährleistet wird.

43 Art. 111 Abs. 1 SDÜ.

44 Art. 109 SDÜ.

45 Art. 109 Abs. 1 Satz 3 SDÜ.

46 Art. 111 Abs. 2 SDÜ.

47 Siehe Art. 116 SDÜ. Dazu die Kritik von Ruth Wehner, Die polizeiliche Zusammenarbeit zwischen den Schengen-Staaten unter besonderer Berücksichtigung des SIS, in: Achermann/Bieber/Epiney/Wehner, Schengen und die Folgen, Bern/München/Wien 1995, S. 148.

48 Siehe Art. 19a–19c E-VG, Botschaft (Anm. 18), S. 6430.

49 Dazu Botschaft (Anm. 18), S. 6258 f.

50 Botschaft (Anm. 18), S. 6153 f.

51 Die technischen Anforderungen an die Möglichkeit der automatischen Verknüpfung werden in den zuständigen Arbeitsgruppen intensiv diskutiert; siehe etwa Dokument 12573/1/04 REV 1 SIRIS 94 COMIX 566 des Vorsitzes des Rats der Europäischen Union vom 18. Oktober 2004; Dokument 10125/04 SIRIS 69 COMIX 378 des Vorsitzes des Rats der Europäischen Union vom 3. Juni 2004.

52 Spiros Simitis, Der verkürzte Datenschutz, Baden-Baden 2004, S. 47; Sabine Leutheusser-Schnarrenberger, Ein System gerät ausser Kontrolle: Das Schengener Informationssystem, ZRP 2004, S. 99; 32. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten 2003, Ziff. 3.2.2 (einsehbar unter http://www.datenschutz.hessen.de – zuletzt besucht am 19. Januar 2005).

53 Vertragsabschluss der Kommission vom 26. Oktober 2004, mit einem multinationalen Team von IT-Unternehmen, angeführt von STERIA-France und HP-Belgium.

54 Dazu auch, Sabine Leutheusser-Schnarrenberger, Ein System gerät ausser Kontrolle: Das Schengener Informationssystem, ZRP 2004, S. 99.

55 Siehe etwa Botschaft (Anm. 18), S. 6071, 6109, 6139, 6153 f., 6178 und 6225 f.

56 Botschaft (Anm. 18), S. 6081.

57 So die Beurteilung des deutschen Bundesbeauftragten für Datenschutz in seinem 19. Tätigkeitsbericht (2000–2001), S. 107 und die Gemeinsame Kontrollinstanz in ihrem 5. Jahresbericht (März 2000 bis Dezember 2001), S. 15 ff.

58 So auch Botschaft (Anm. 18), S. 6154.

59 Die Regelung der Fristen wird von Art. 351^{decies} Abs. 7 lit. b StGB an den Bundesrat delegiert. Art. 351^{decies} Abs. 1 StGB regelt die im SIS gespeicherten Daten nur sehr allgemein und müsste entsprechend in der Verordnung konkretisiert werden. Diese Regelungen können im schweizerischen Recht deshalb ohne Referendum angepasst werden.

60 Botschaft (Anm. 18), S. 6085.

61 Rainer Oberleitner, Schengen und Europol: Kriminalitätsbekämpfung in einem Europa der inneren Sicherheit, Wien 1998, S. 77.

62 Dazu die kritische Sicht von Madeleine Colvin, The Schengen Information System: A Human Rights Audit, European Human Rights Law Review 2001, S. 279.

63 Art. 41 i. V. m. Art. 42 und 43 SDÜ.

64 Art. 40 i. V. m. Art. 42 und 43 SDÜ.

65 Art. 47 SDÜ.

66 Art. 39 und 46 SDÜ.

67 Art. 126–130 SDÜ.

68 Siehe etwa Art. 351^{quinquies} ff. StGB und die neuen Art. 351^{octies} Abs. 3 lit. f und Abs. 7 sowie Art. 351^{novies} StGB.

69 Diese Bereiche fallen unter Art. 61 ff. EGV, so dass die Datenschutzrichtlinie Anwendung findet; siehe 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. November 1995, S. 31–50.

70 Siehe die Fundstellen in Botschaft (Anm. 18), S. 6064 mit Fn. 93.

71 Siehe Art. 39 Abs. 5, Art. 40 Abs. 4 und Art. 41 Abs. 10 SDÜ.

72 Siehe Art. 82 und 91 SDÜ und die Richtlinie 91/477/EWG des Rates vom 18. Juni 1991 über die Kontrolle des Erwerbs und des Besitzes von Waffen, ABl. L 256 vom 13. September 1991, S. 51 ff.

73 Siehe den Entwurf für die neuen Art. 32a ff. Waffengesetz, Botschaft (Anm. 18), S. 6438 ff.

74 Siehe Art. 70–76 SDÜ und dazu den Entwurf für die neuen Art. 18a ff. Betäubungsmittelgesetz, Botschaft (Anm. 18), S. 6444 ff.

75 Entsprechend wird der technische Aufbau des VIS vom selben Ausschuss unterstützt, der auch für SIS II zuständig ist; siehe den Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über das Visa-Informationssystem VIS vom 28. Dezember 2004, KOM(2004) 835 endg., S. 2 und 50, sowie Art. 39.

76 So schlägt die Kommission in ihrem Verordnungsentwurf für das VIS vom 28. Dezember 2004 vor, das VIS auch zur Identifizierung und Rückführung illegaler Einwanderer zu verwenden; siehe Art. 17 E-VIS.

77 Die EU baut darüber hinaus auf derselben Plattform etwa das aus zwei Datenbanken bestehende Zollinformationssystem ZIS auf, das den Zollbeamten europaweit einen unmittelbaren Zugriff auf Informationen über verdächtige Grenzüberquerungen ermöglichen soll. Siehe Übereinkommen aufgrund von Art. K.3 des Vertrags über die Europäische Union über den Einsatz der Informationstechnologie im Zollbereich, ABl. C 316 vom 27. November 1995, S. 34–47.

78 Eingehend Christian Schmid, EURODAC-Verordnung, Wien/Graz 2003.

79 Verordnung (EG) Nr. 343/2003 des Rates vom 18. Februar 2003, ABl. L 50 vom 25. Februar 2003, S. 1.

80 Siehe Art. 21 Dublin-Verordnung.

81 Siehe Art. 13 ff. EURODAC-Verordnung. Verordnung (EG) Nr. 2725/2000 des Rates vom 11. Dezember 2000 über die Einrichtung von «EURODAC» für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl. L 316 vom 15. Dezember 2000.

82 Siehe Art. 22a^{bis} ff. ANAG, Botschaft (Anm. 18), S. 6416 ff.

83 Art. 99 Abs. 1 und Art. 102a ff. AsylG Botschaft (Anm. 18), S. 6422 ff.

84 Siehe etwa Mads Andenas / Stefan Zleptnig, Surveillance and Data Protection: Regulatory Approaches in the EU and Member States, European Business Law Review 2003, S. 809 f.

85 Zur Notwendigkeit einer Harmonisierung in institutioneller Hinsicht eindringlich etwa Spiros Simitis, Der verkürzte Datenschutz, Baden-Baden 2004, S. 40.

86 Wie etwa RIPOL (Verordnung über das automatisierte Fahndungssystem vom 19. Juni 1995, SR 172.213.61), ZAR (Verordnung über das Zentrale Ausländerregis-.ter vom 23. November 1994, SR 142.215), oder IPAS (Verordnung über das informatisierte Personennachweis, Aktennachweis- und Verwaltungssystem im Bundesamt für Polizei vom 21. November 2001, SR 361.2).

87 BBL 2005, S. 2100.