# Datenschutzrechtliche Spaltung in Europa? Teil 2

*Andreas Günther*

## Italien, das Schengener Abkommen und der Schutz personenbezogener Daten

*Schengen I: „Laboratorium für Europa 1993"*

In seinem Vortrag, der den Auftakt des Workshops bildete, schilderte Profi Losano Aspekte des Schutzes personenbezogener Daten in einem geeinteren Europa sowie die italienischen Ansätze im Datenschutzrecht. Ausgangspunkt seiner Analyse war das „als Laboratorium für das Europa von 1993" gedachte sog. Schengener Übereinkommen.[21]- Dieses am 14. Juni 1985 zwischen den Beneluxstaaten, Frankreich und Deutschland geschlossene Regierungsabkommen (Schengen I) sieht mit Blick auf den europäischen Binnenmarkt den progressiven Abbau und schließlich die Abschaffung der Personenkontrollen an den Grenzen zwischen den beteiligten Staaten vor. Obwohl Grenzkontrollen heute nur noch eine bedingt wirksame Abschreckung für moderne Kriminalität darstellen, waren sich die Regierungsvertreter dennoch darin einig, die durch den Grenzabbau entfallenden Kontrollinstrumentarien und den damit verbundenen Verlust an „innerer Sicherheit" durch Ausgleichsmaßnahmen kompensieren zu müssen. Nur dann ließen sich die Freizügigkeit der Bürger mit der Sicherheit für Personen und Güter sowie die Großzügigkeit des Asylrechts mit der Kontrolle der illegalen Einwanderung in Einklang bringen.

*Schengen II: Konkrete Ausgestaltung*

Schengen I besteht aber nur aus Programmsätzen. Seit 1985 verhandelten Experten der fünf Staaten daher über die konkrete Ausgestaltung der Reduzierung von Grenzkontrollen und die Schaffung der zu deren Kompensation notwendigen Infrastrukturen, einer Fahndungsunion mit dem Fernziel einer „Europäischen Polizeibehörde". Die Ergebnisse flossen in das Übereinkommen zur Durchführung des Schengener Übereinkommens (Schengen II) ein. Dieses sollte zunächst am 15. Dezember 1989 unterzeichnet werden, Unwägbarkeiten, die sich aus den unvorhersehbaren Ereignissen in Deutschland seit dem 9. November 1989 im Hinblick auf die Einbeziehung der damaligen „Noch-DDR" ergaben, verzögerten den Abschluß durch die fünf Regierungsvertreter jedoch kurzfristig bis zum 19. Juni 1990. Solange die nun vereinbarten Ausgleichsmaßnahmen noch nicht umgesetzt seien, sahen sich die beteiligten Staaten in Anbetracht der befürchteten Sicherheitsdefizite auch noch nicht in der Lage, den gem. Art. 30 Schengen I ursprünglich schon für den 1. Januar 1990 vorgesehenen vollständigen Abbau der Grenzkontrollen zu verwirklichen; nun scheint sicher, daß zumindest im vielzitierten Jahr 1993 die Bürger Frankreichs, Deutschlands und der Beneluxstaaten die Grenzen ohne Paßkontrolle überschreiten werden können.

*Ausgleichsmaßnahmen für den mit dem Grenzabbau verbundenen Verlust an „innerer Sicherheit"*

Schengen II sieht als Ausgleichsmaßnahmen unter anderem eine verstärkte polizeiliche Zusammenarbeit (z.B. im Bereich der polizeilichen Observation und der Nacheile von Polizeibeamten bei der Verfolgung von Straftätern über Staatsgrenzen hinweg), eine Vereinfachung des Rechtshilfeverkehrs in Strafsachen, der Auslieferung und der Vollstrekkungshilfe, die Angleichung von Gesetzen (z.B. im Betäubungsmittel- oder im Waffen-und Sprengstoffrecht) sowie eine Verlagerung der Kontrollen an die Außengrenzen verbunden mit einer entsprechenden Sichtvermerks- und Asylpolitik vor. Unter datenschutzrechtlichen Aspekten besonders sensibel ist der polizeiliche Informationsaustausch im Rahmen eines europäischen elektronischen Fahndungsverbundes. Herz der gemeinsamen Verbrechensbekämpfung soll das sog. Schengener Informationssystem (SIS) werden.[22] Ein zentraler Rechner in Straßburg (geplante Speicherkapazität: 1,5 GByte), an den die nationalen Polizeidienststellen angeschlossen sind, soll die für die Durchführung der polizeilichen Aufgaben relevanten Daten enthalten. Vorgesehen sind eine Sachfahndungs- sowie eine Personenfahndungsdatei, wobei der Sachfahndung wegen der angeblich geringeren Datenschutzprobleme der Vorrang eingeräumt werden soll. In der Personendatei werden Identifizierungsangaben (Namen, Geburt, Geschlecht, Staatsangehörigkeit) und die personengebundenen Hinweise „bewaffnet" und „gewalt-

*Das Schengener Informationssystem (SIS)*

[21] Siehe oben Fn. 2. = jur-pc 5/91, 1094

[22] Hierzu im einzelnen Weichert, CR 1990, S. 62ff m.w.N.

tätig" über bis zu 800.000 Personen gespeichert, die vorbeugend verhaftet oder in Untersuchungshaft zu nehmen sind, denen der Zugang zum Gebiet der Vertragsparteien nicht gestattet ist bzw. gegen die eine Ausweisung vorliegt sowie die zu observieren sind und deren Aufenthaltsort zu ermitteln ist (Art. 94ff Schengen II). Zusätzlich zu diesen im engeren Sinne personenbezogenen Daten soll die Sachfahndungsdatei (mit ca. 6,7 Millionen Gegenständen) solche enthalten, die mittelbar personenbezogen sein können: Daten über gestohlene Kraftfahrzeuge, Feuerwaffen, Blanko-Dokumente, Identitätspapiere und Banknoten (Art. 100 Schengen II).

*Demokratiedefizit*

Neben einem immer wieder bemängelten Rechtsstaats- und Demokratiedefizit im Hinblick darauf, daß beide Abkommen „hinter verschlossenen Türen" von Exekutiv-Experten ohne parlamentarische Beteiligung ausgearbeitet wurden,[23] formulierten insbesondere Datenschutzbeauftragte aus Frankreich und Deutschland schon früh Vorbehalte in Bezug auf den Schutz personenbezogener Daten im SIS. Zwei Gesichtspunkte sind erwähnenswert: Zum einen ist ein supranationales Informationssystem wie das SIS nicht direkt der nationalen Datenschutzgesetzgebung – auch nicht der des Gastlandes, hier Frankreich – unterworfen. Das bedeutet, daß allein die Harmonisierung und Fortschreibung nationaler Gesetze nicht genügt, für internationale Behörden und deren Datenbanken bedarf es eines eigenen Datenschutzrechts. Daher sind in den Art. 102 bis 118 Schengen II detaillierte Regelungen des Datenschutzes und der Datensicherung im SIS vorgesehen, z.B. das Recht auf Auskunft, Berichtigung und Beschwerde seitens des Betroffenen, nationale und internationale Kontrollinstanzen sowie die Verpflichtung zur zweckgebundenen Verwendung der Daten. Diese bedürfen aber nach Ansicht der Datenschutzbeauftragten weiterer Verbesserungen und Vervollständigungen.

*Datenschutzbedenken*

*Problem: Unterschiedlicher Datenschutzstandard in den Vertragsstaaten*

Problem: Unterschiedlicher Datenschutzstandard. Zum anderen besteht im Hinblick auf ein unterschiedliches Datenschutzniveau in den Vertragsstaaten die Gefahr einer Aushöhlung bereits bestehender nationaler Gesetze über den Schutz personenbezogener Daten durch eine Übermittlung in jene Staaten, die keine äquivalente gesetzliche Regelung besitzen, und damit Anlaß zur Sorge um eine Einbuße an Datenschutz durch den grenzüberschreitenden Datenverkehr. Die Schengener Übereinkommen erkennen an, daß der automatisierte Austausch personenbezogener Daten grundsätzlich auch nationalen Regelungen untersteht. Und diese verbieten z.B. in Frankreich und Deutschland prinzipiell, daß personenbezogene Daten aus dem öffentlichen Bereich in Länder übermittelt werden, die keinen dem Schutz im Ursprungsland entsprechenden Standard gewährleisten.[24] Daher sieht Art. 126 Abs. 1 Schengen II vor, daß jede Vertragspartei in ihrem nationalen Recht in Bezug auf die automatische Verarbeitung personenbezogener Daten, die nach dem Übereinkommen übermittelt werden, die erforderlichen Maßnahmen zur Gewährleistung eines Datenschutzstandards trifft, der zumindest dem entspricht, der sich aus der Verwirklichung der Grundsätze der Datenschutzkonvention des Europarates[25] ergibt. Die Übermittlung personenbezogener Daten darf erst beginnen, wenn in dem Hoheitsgebiet der an der Übermittlung beteiligten Vertragsstaaten die entsprechenden Regelungen in Kraft getreten sind (Art. 126 Abs. 2) und wenn die Vertragsparteien einer nationalen Kontrollinstanz die Aufgabe übertragen haben, in unabhängiger Weise die Einhaltung der Bestimmungen in bezug auf die Verarbeitung personenbezogener Daten in Dateien zu überwachen (Art. 128 Abs. 1).

*Schutzniveauklausel*

---

[23] Der Bundestag war am Zustandekommen von Schengen I als reinem Regierungsabkommen überhaupt nicht beteiligt und seine Rolle bei Schengen II beschränkt sich im Hinblick auf die inzwischen geschaffenen Fakten wohl auf die eines „Ja-Sagers", was im übrigen auch für die Länderparlamente gilt, die nach der bundesdeutschen Kompetenzverteilung für die im Bereich des Sicherheits- und Polizeirechts vorgesehenen Regelungen weitgehend zuständig sind.
Mit der Rolle des „Ja-Sagers" hat sich zumindest der niederländische Staatsrat, ein einflußreiches Beratungsorgan der Haager Regierung, dem die Königin vorsitzt, im übrigen nicht abgefunden: Wie aus der Tagespresse zu entnehmen war, hat der im Hinblick auf die Verabschiedung eines Ratifikationsgesetzes durch das Parlament von der Regierung konsultierte Staatsrat Schengen II am 8. April 1991 in einem Gutachten vernichtend beurteilt und durch seine Empfehlung, den Vertrag in dieser Form abzuweisen, die Ratifikation durch die Niederlande zunächst in Frage gestellt. Das Votum wurde unter anderem auch mit dem mangelhaften Schutz der Privatsphäre bei der Datenweitergabe an ausländische Polizeistellen begründet. Unter den Parlamentariern der meisten Fraktionen in Den Haag herrsche zudem Verärgerung darüber, daß die Regierung den Vertrag mehr oder weniger geheim ausgehandelt habe, ohne daß das Parlament eine Mitwirkungsmöglichkeit gehabt hätte (s. z.B. F.A.Z. Nr. 90 v. 18.4.91, S. 14).

[24] Siehe oben die Ausführungen von Dr. Schneider zur Zulässigkeit des Im- und Exports personenbezogener Daten nach deutschem Recht.

[25] Siehe oben Fn. 10. = jur-pc 5/91, 1096

*Heterogene nationale Regelungen*

Die als Maßstab herangezogene europäische Datenschutzkonvention enthält zumindest einige allgemeine Prinzipien, begründet aber als lediglich völkerrechtlich bindender Vertrag für den einzelnen Bürger mangels Unmittelbarkeit keine subjektiven Rechte und Pflichten, so daß sie in jedem Fall in ein einschlägiges nationales Gesetz umgesetzt werden muß. Obwohl alle Schengen-Staaten die Konvention gezeichnet und die meisten diese inzwischen auch ratifiziert haben, kann schon im Hinblick auf die bestehenden Regelungen in den ursprünglichen Vertragsstaaten nicht von einem einheitlichen Datenschutzstandard gesprochen werden: Frankreich und Deutschland besitzen insgesamt vergleichbare Datenschutzvorschriften, die Niederlande und Luxemburg haben zwar allgemeine Datenschutzgesetze, aber noch keine bereichsspezifischen Vorschriften für die Sicherheitsbehörden erlassen, und Belgien wurde bislang als „Datenschutzoase" bezeichnet, da es an einer gesetzlichen Regelung des Datenschutzes noch völlig fehlte; nicht zuletzt im Hinblick auf die Mitwirkung am SIS ist Anfang 1990 endlich der Entwurf eines Datenschutzgesetzes auf den parlamentarischen Weg gebracht worden.[26]

*Ausdehnung der Schengener Abkommen auf südeuropäische EG-Mitglieder*

Die Schengener Übereinkommen zwischen den „Kernstaaten" Europas sind aber nur ein notwendiger Schritt in Richtung gesamteuropäische Integration und ein Modell, daß früher oder später auch auf die südeuropäischen Mitglieder der EG ausgedehnt werden muß. Die damit verbundenen Schwierigkeiten – insbesondere im Hinblick auf den Stand der Datenschutzgesetzgebung in Italien – schilderte Prof. Losano sehr anschaulich.

*„Barriere" innerhalb der EG*

Da der Verkehr innerhalb der Staaten des Schengener Übereinkommens freier werde, sei an den Außengrenzen erhöhte Wachsamkeit geboten. Die südeuropäischen Staaten hätten erkannt, daß sich innerhalb der EG eine Barriere aufbaue: Der „harte Kern" Europas laufe Gefahr, die „mediterranen, weniger gut organisierten und ein wenig schlampigen Staaten" auszusperren. Man befürchte nicht nur, daß über Südeuropa eine große Zahl illegaler Einwanderer in die Gemeinschaft zu kommen drohe, auch könnten die Mittelmeerstaaten dem SIS bislang nicht beitreten, ohne das Daten aus Straßburg, die dorthin übermittelt würden, den ursprünglich Schutz verlören.

*Aufnahme Italiens in die Schengen-Runde*

Trotzdem hätten Italien (1988) und Spanien (1990) um Aufnahme in die Schengen-Runde nachgesucht und auch Portugal möchte nicht ausgeschlossen bleiben. Nachdem der gegen Italien vorgebrachte Einwand der fehlenden Kontrolle der Einwanderung aus den arabischen Mittelmeerstaaten durch die Einführung eines (zumindest formalen) Visumzwangs vom Tisch war, hätten die italienischen Medien vom Beitritt Italiens zum Schengener Übereinkommen am 27. November 1990 berichten können; im übrigen habe die italienische Fachpresse die Schengener Übereinkommen jedoch noch nicht zur Kenntnis genommen. Aber nicht nur im Hinblick auf die besondere geographische Lage und Struktur sowie die geringe Effizienz der Polizei in den Staaten im Mittelmeerraum – Prof. Losano sprach von drei süditalienischen Regionen, die dem Staat „entglitten" seien – werfe ein vollständiger Beitritt zu den Schengener Übereinkommen für die europäischen Partner schwerwiegende Probleme auf.

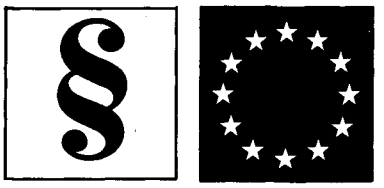
*Italien: Kein Datenschutzgesetz*

In Italien gäbe es bislang zudem kein Datenschutzgesetz; mehrere Gesetzesvorhaben seien seit 1981 gescheitert, Regierung und Parlament gelänge es nicht, ein solch langfristiges Gesetzesvorhaben zu Ende zu führen.[27] Selbst im Hinblick auf die Europarats-Konvention, der Italien zwar 1983 beigetreten sei, für die es aber erst 1989 ein Gesetz erlassen habe, daß den Präsidenten der Republik ermächtigte, das Übereinkommen zu ratifizieren, und dessen Ratifikation als solche wohl immer noch nicht vollzogen sei, befinde sich Italien im Verzug. Dies verdeutliche exemplarisch den Kontrast zwischen dem verbal bekundeten und real erlebten Europäismus Italiens. Aber auch in Spanien und Portugal stelle sich die Lage nicht viel anders dar.

---

[26] CR 1990, S. 367.

[27] Auf die Frage, ob nicht die Rechtsprechung in Italien zumindest unter verfassungsrechtlichen Gesichtspunkten dem Bürger ein Mindestmaß an Datenschutz garantieren könne, antwortete Prof. Losano, dies sei für italienische Richter ein viel zu politisches Thema, als daß man von dieser Seite konkrete Entscheidungen erwarten könne. Zudem sei ein allgemeines Persönlichkeitsrecht der in Deutschland herrschenden dogmatischen Prägung der italienischen Verfassungslehre noch fremd. Nicht viel anders stelle sich die Lage z.B. auch in Spanien dar: Dort sei zwar sogar ein Grundrecht auf Datenschutz in der Verfassung vorgesehen (Art. 18 Abs. 4 der Spanischen Verfassung von 1978), dieses sei aber unzweideutig als Gesetzgebungsauftrag an den Gesetzgeber gerichtet. Solange dieser jedoch nicht tätig geworden ist, sei allenfalls ein minimaler und materieller Kern eines Rechts auf informationelle Selbstbestimmungen garantiert.



Würden diese Staaten, ohne eine rechtliche und organisatorische Struktur zum Schutz personenbezogener Daten zu besitzen, an das SIS angeschlossen, so könnten Auskünfte aus diesen Ländern im Hinblick auf ihre Zuverlässigkeit die Datenbank belasten und in umgekehrter Richtung würden Daten aus Straßburg nach Südeuropa in einen rechtsfreien Raum fallen. Um eine solche Situation zu verhindern, seien gerade die schon genannten Art. 126ff in Schengen II aufgenommen worden. Die Versäumnisse nicht nur Italiens, sondern auch Spaniens und Portugals im Bereich des Datenschutzes müßten demnach dazu führen, daß die Beteiligung dieser Staaten an den Schengener Übereinkommen vorerst eine abstrakte Vorstellung bliebe. Die „Asymmetrie" auf diesem Gebiet sei schwer zu überwinden und würde faktisch zunächst zu einem Ausschluß der betroffenen Staaten vom Zugang zum SIS führen müssen. Mit dem politischen Wert einer Unterzeichnung könne die konkrete Anwendung der Übereinkommen im Mittelmeerraum demnach vorerst nicht Schritt halten.

*Asymmetrie im Datenschutz und die Folgen*

Prof. Losano schloß sein Referat mit einem Appell an die südeuropäischen Staaten zu versuchen, gesetzgeberisch und institutionell zur Kerngruppe aus Benelux, Frankreich und Deutschland aufzuschließen und im „Europa der zwei Geschwindigkeiten" den Kontakt zum „schnellen Europa" nicht zu verlieren. Allein die Unterzeichnung des Schengener Übereinkommens werde Italien nicht in den „harten Kern" Europas hineinbringen, sie sei nur einer der zahlreichen Akte symbolischer Politik, die „bella Italia" heimsuchten; sie nährten die Illusion, Teil eines Europas zu sein, mit dem der italienische Staat nur immer schwerer Schritt halten könne.

*Appell an die Mittelmeerstaaten*

Ergänzend wurde in den Diskussionen unter anderem hervorgehoben, daß gerade Schengen II auch als Instrument gedacht ist, die bislang im Rahmen der EG noch „faulen" Länder zu mehr als bloßen „Lippenbekenntnissen" im Datenschutz zu mobilisieren. Hingewiesen wurde auch immer wieder darauf, daß in naher Zukunft neben Schengen II zudem von der als Kommissionsvorschlag inzwischen vorliegenden Datenschutzrichtlinie[28] ein starker Harmonisierungsdruck ausgehen wird. Im Hinblick auf Befürchtungen in Bezug auf das Niveau eines dann einheitlichen Schutzes in der Gemeinschaft zitierte Prof. Losano aber eine Äußerungen des ehemaligen Staatssekretärs im Bundeskanzleramt Prof. Waldemar Schreckenberger, nach der die Deutschen in ihrem neuen Überlegenheitsgefühl sich nicht einbilden dürften, daß Datenschutz, auch wenn noch nicht überall durch Gesetz geregelt, eine deutsche Erfindung sei und man sich nicht hinter einem praxisfernen Perfektionismus verschanzen dürfe.[29] Und auch Prof. Gallwas äußerte Bedenken dahingehend, daß das Volkszählungsurteil im Hinblick auf eine internationale Harmonisierung unter Umständen einen zu hohen Standard festgeschrieben haben könnte, insbesondere dadurch, daß nicht zwischen sensiblen und weniger sensiblen Daten differenziert, sondern pauschal angenommen würde, es gäbe kein belangloses Datum. Internationale Angleichung sei jedoch in Anbetracht des derzeit herrschenden Nord-Süd-Gefälles wahrscheinlich eher mit einer Rücknahme des Schutzniveaus verbunden. Die geplante EG-Richtlinie sehe aber wohl nur einen Minimalstandard vor, der weitergehende nationale Regelungen nicht ausschließe.[30]

*Harmonisierungsdruck durch die geplante EG-Richtlinie*

## Der grenzüberschreitende Datenverkehr aus öffentlichen und privaten Datenbanken – eine italienische Sicht

Nach einem einführenden Video über CERVED, einen privaten Online-Anbieter der in den italienischen Handelsregistern gespeicherten Informationen (vergleichbar Creditreform, Ecodata oder Schimmelpfeng in der Bundesrepublik), der eng mit den italienischen Industrie- und Handelskammern zusammenarbeitet, erläuterte Dr. Borrello,

*CERVED: Italienisches Handelsregister Online*

[28] Siehe oben Fn. 1 und Fn. 9.

[29] Zur Diskussion üm Datenschutz in der EG und den Richtlinienvorschlag vgl. Riegel, ZRP 1990, S. 132ff; Simitis, RDV 1990, S. 3ff; jeweils m.w.N. sowie CR 1990, S. 80ff, 621f, 686, 750, 813; CR 1991, S. 61, 124f; Einwag, DSB 2/91, S. 1ff (7f).

[30] Anderer Ansicht in dieser Hinsicht ist der Vizepräsident der EG-Kommission, Martin Bangemann (CR 1990, S. 813): Zumindest für grenzüberschreitenden Datenverkehr sollen über den EG-Datenschutz hinausgehende nationale Vorschriften im Hinblick auf eine potentielle Beeinträchtigung des Binnenmarktes nicht mehr zulässig sein (vgl. auch Art. 1 Abs. 2 und Erwägungsgrund 12 des Richtlinienvorschlages); häufig anzutreffenden Vorstellungen deutscher Datenschützer, wonach die EG-Vorschriften nur einen Mindeststandard darstellen sollen, über den der nationale Gesetzgeber hinausgehen könne, wenn er dies für richtig halte, habe Bangemann eine klare Absage erteilen wollen. Auf der anderen Seite ist aber zu vermerken, daß die Kommission sich selber verpflichtet fühlt, bei Ihren Vorschlägen zur Harmonisierung des Datenschutzrechts von einem hohen Schutzniveau auszugehen (Erwägungsgrund 7 und Begründung III.), eine sich im übrigen auch aus Art. 100a Abs. 3 EWGV ergebende Notwendigkeit.

*Personenbezogene Daten*

Wissenschaftlicher Mitarbeiter von CERVED, seine von eher wirtschaftlicher Betrachtungsweise geprägte Position. Dabei unterschied er streng zwischen Daten, die sich auf natürliche Personen beziehen, und solchen über juristische Personen. Der Schutz personenbezogener Daten müsse zweifellos auch im grenzüberschreitenden Datenverkehr auf einem hohen Niveau durch detaillierte Datenschutzregelungen gesichert werden; entsprechende Gegenseitigkeitsklauseln in den nationalen Datenschutzgesetzen seien deshalb so lange sinnvoll, wie es Staaten gebe, in denen Datenschutz nicht gewährleistet sei. Diese und die mit ihnen verbundenen Beschränkungen des freien Datenverkehrs würden aber voraussichtlich in Zukunft hinfällig, sobald durch die geplante EG-Richtlinie ein einheitliches Schutzniveau gesichert und der Abbau juristischer Hemmnisse im grenzüberschreitenden Transfer von Daten über natürliche Personen zumindest auf EG-Ebene möglich sei.

*Unternehmensbezogene Daten*

Zudem beträfe aber der wirtschaftliche Informationsbedarf auf internationaler Ebene derzeit auch beinah ausschließlich juristische Personen (insb. Gesellschaften) und bezöge sich selten unmittelbar auf natürliche Personen bzw. auf juristische Personen, hinter denen eine natürliche Person wie bei einer Einzelfirma ausgemacht werden könne. Und hinsichtlich solcher unternehmensbezogener Daten stelle sich die Situation anders dar: Hier berichtete er aus seiner Praxis, daß das in Italien, einem Land ohne Datenschutzbestimmungen, ansässige CERVED schon derzeit überhaupt keine Schwierigkeiten hätte, Daten aus dem Ausland zu beschaffen. Die gewerbliche Nutzung unternehmensbezogener administrativer Daten sei mittlerweile alltägliches 'business' in Europa. Als Grund hierfür und gleichzeitig als unabdingbare Voraussetzung für grenzüberschreitenden Datenverkehr nannte er die Qualität der Informationen. Leitgedanke zukünftiger Datenschutzpolitik müsse demnach unter besonderer Berücksichtigung der realen Dimension ein nicht mehr eigentümer- sondern vielmehr verfahrensbezogener Schutz sein. Datenschutz im Bereich nicht sensitiver Daten dürfe nicht das unvermeidbare Zusammentragen und Verwenden von Informationen verbieten, sondern müsse sich darauf beschränken, den Informationsfluß auf der Grundlage von Modalitäten, Prozeduren und Kontrollen zu kanalisieren (was rechtlich im übrigen viel komplexer sei) und so eine vernünftige Sicherheit bieten, daß die Informationen 'wahr' seien und nicht in unvollständiger Weise verwendet würden: Datenschutz als Sicherung der Datenqualität im Sinne von Wahrheit und Vollständigkeit; allein Informationsqualität genieße Vorrang vor der Notwendigkeit eines freien Datenverkehrs. Darüber hinausgehende Regelungen wären unnötig und würden unweigerlich zu einer Behinderung des internationalen Wirtschaftsverkehrs führen. Ausgeschlossen bzw. eingeschränkt werden müsse allenfalls der Austausch bzw. die gewerbliche Nutzung als vertraulich einzustufender Unternehmensdaten. Qualitätsorientierte Information (im Sinne von Wahrhaftigkeit und Vollständigkeit) führe demnach unmittelbar zu einer Reduzierung rechtlicher Schwierigkeiten für den freien Datenverkehr.

*Grenzüberschreitender Datentransfer und gewerbliche Nutzung: Alltägliches 'business'*

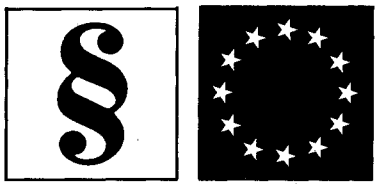
*Datenschutz als Schutz vor falschen Daten*

*Qualitätsorientierte Information*

*„Stimme des Gemeinschaftsrechts" im Hinblick auf den Schutz unternehmensbezogener Daten auch weiterhin gewollt „matt"*

Konsequenterweise bezöge sich der jüngste EG-Richtlinienentwurf mit dem Ziel eines Abbaus der juristischen Hemmnisse im grenzüberschreitenden Datenverkehr ausschließlich auf natürliche Personen.[31] Die EG hätte ein allgemeines Interesse an einem 'laissez faire' in der Verbreitung von Daten über juristische Personen. Die „Stimme des Gemeinschaftsrechts" sei in diesem Punkt gewollt „matt" und alles deute darauf hin, daß man auch weiterhin den Schutz juristischer Personen ausklammern werde. Diese liberale Politik im Hinblick auf unternehmensbezogene Daten funktioniere sehr gut und werfe auch keine besonderen Probleme auf. Der Gesetzgeber müsse nur dort eingreifen, wo Selbstschutz nicht möglich sei, ansonsten könne er sich auf die Selbstregulierung des freien Datenverkehr innerhalb des Wirtschaftssystemes der Gemeinschaft verlassen. Für Daten über juristische Personen, insbesondere über Unternehmen, würden die wirtschaftlichen Erwägungen die rechtlichen Beschränkungen des internationalen Datenverkehrs überwiegen. Signifikant sei eine starke Nachfrage nach immer höherwertigeren, stärker anwendungsorientierten Informationen. Diese Nachfrage spiegele eine wirtschaftliche Macht wieder, die immer der Macht des rechtlichen Instrumentariums zur Regelung von Datenflüssen überlegen sei (sie!).

[31] Die Europarats-Konvention (s.o. Fn. 10) sieht demgegenüber in Art. 3 Abs. 2 Buchstabe b) vor, daß die Mitgliedsstaaten bei ihrem Beitritt vorsehen können, das Übereinkommen nicht nur auf unmittelbar personenbezogene Daten anzuwenden, sondern auch auf Informationen über Personengruppen, Vereinigungen, Stiftungen, Gesellschaften, Körperschaften oder andere Stellen, die unmittelbar oder mittelbar aus natürlichen Personen bestehen, unabhängig davon, ob diese Stellen Rechtspersönlichkeit besitzen oder nicht.



Zudem bestehe eine starke Tendenz zur Förderung der effizienten Nutzung von Datenquellen in der gesamten Gemeinschaft durch Standardisierungen, die den Vergleich von unterschiedlichen Informationen vereinfachen. Dieses Ziel sei z.B. von der Vierten Richtlinie des Rates zur Angleichung des Gesellschaftsrechts vom 25. Juli 1978[32] verfolgt worden: Sie führte die Harmonisierung der rechtlichen Bestimmungen in den Mitgliedsstaaten über die formale Struktur, den substantiellen Inhalt, die Kontrolle und die Veröffentlichung der externen Informationsdokumente über Vermögens-, Finanz- und Ertragslage von in der Gemeinschaft tätigen Kapitalgesellschaften herbei, um einen möglichst sicheren Einblick, einen „true and fair view" zu gewährleisten. Auch das Projekt eines europäischen Handelsregisters gehe in diese Richtung. Kurz: Freiheit des Informationsverkehrs sei gut, wichtiger sei allein die Qualität und Standardisierung der Daten.

In der anschließenden Diskussion wurde aber angemerkt, daß die Grenze zwischen Daten über eine natürliche Person und unternehmensbezogenen Daten nicht eindeutig zu ziehen sei und es in Handelsregistern durchaus zumindest mittelbar personenbezogene Daten gebe.

So hat der BGH im Hinblick auf die Nutzung der Handelsregister durch private Wirtschaftsinformationsdienste in Deutschland erst kürzlich entschieden, daß in der Bundesrepublik das Recht auf Einsicht in die Handelsregister zwar weit gefaßt sei und auch die Durchsicht großer Teile oder der gesamten Register sowie die Dokumentation durch selbstgefertigte Abschriften und gegebenenfalls auch Fotokopien umfasse, daß § 9 HGB aber keinen Anspruch auf Gestattung der Mikroverfilmung des gesamten Bestandes eines Handelsregisters mit dem Zweck der Errichtung einer privaten zentralen Datei in gewerblicher Konkurrenz zu den Handelsregistern gebe; es sei nicht ermessensfehlerhaft, wenn die Justizverwaltungen ohne eine insbesondere auch den Datenschutz hinreichend berücksichtigende gesetzliche Grundlage die Gestattung ablehnen[33].

Die Problematik hat im übrigen auch einen europarechtlichen Aspekt: Die Kommission hat in einer als erstem Schritt im Rahmen eines Verfahren nach Art. 169 EWGV gedachten Aufforderung zur Stellungnahme Zweifel angemeldet, ob § 9 HGB in der vom BGH bestätigten engen Auslegung mit der Ersten gesellschaftsrechtlichen Richtlinie des Rates vom 9. März 1968 (sog. Publizitätsrichtlinie 68/151/EWG) in Einklang steht. Die Bundesregierung hat in ihrer Äußerung vom 9. Oktober 1989 daraufhin die Auffassung vertreten, auch aus Art. 3 Abs. 3 Satz 1 der genannten Richtlinie ließe sich kein Anspruch auf Mikroverfilmung des gesamten Handelsregisters zum Aufbau einer privaten Datenbank und zu deren wirtschaftlicher Verwertung herleiten; insofern bestehe kein Anlaß, die geltende Rechtslage zu ändern[34]; die Kommission scheint bislang keine weiteren Schritte unternommen zu haben.

*Leitsätze der BGH-Entscheidung auf der nächsten Seite*

Schließlich wurde in der Diskussion auch noch hervorgehoben, daß die Kriterien „Vollständigkeit" und „Wahrheit" schwer faßbar seien. Zudem wurde darauf hingewiesen, daß einem rein qualitätsorientierten Schutz unternehmensbezogener Daten (Datenschutz als Schutz vor falschen Daten) die Gefahr innewohne, daß diese Maßstäbe auf die Dauer im Hinblick auf das allgemeine Datenschutzbewußtsein auch auf den Schutz personenbezogener Daten übertragen würden.

*Kriterien „Vollständigkeit" und „Wahrheit" schwerfaßbar*

*Gefahr: Übertragung dieser Maßstäbe auf den Schutz personenbezogener Daten*

## Fazit

Im Hinblick auf die Ausgangsfrage ist festzuhalten, daß eine datenschutzrechtliche Spaltung Europas bereits besteht. Zweifellos ist es aber im Zeitalter der Informationstechnik weder sinnvoll noch möglich, eine supranationale Integration zu verwirklichen, in der der Fluß personenbezogener Daten innerhalb eines informationellen Großraumes Europa nicht auf einer sicheren rechtlichen Grundlage ruht. Die Unterzeichnung von Schengen II durch die südeuropäischen Staaten wird demnach so lange auf sich beruhen müssen, bis entsprechende datenschutzrechtliche und auch datenschutzpraktische

[32] Sog. Jahresabschlußrichtlinie 78/660/EWG, ergänzt durch die Siebte gesellschaftsrechtliche Richtlinie vom 13. Juni 1983 (sog. Richtlinie über den konsolidierten Jahresabschluß 83/349/EWG), in das deutsche Handels- und Gesellschaftsrecht inkorporiert durch das Bilanzrichtlinien-Gesetz vom 19. Dezember 1985.

[33] BGH, jur-pc 89, 258 = NJW 1989, 2818ff; grundlegend hierzu Kollhosser, NJW 1988, S. 2409ff.

[34] DSB 2/90, S. 1ff.

Voraussetzungen geschaffen sind. Einig war man sich auf dem Workshop aber auch darin, daß Datenschutz den internationalen Datenverkehr in Zukunft nicht übermäßig behindern dürfe. In besonders sensiblen Rechtsgebieten seien ggf. bereichsspezifische Sonderregelungen zu schaffen, im übrigen sei immer das allgemeine persönlichkeitsrechtliche Abwägungsmodell im Auge zu behalten.
Die Hindernisse, die sich aus dem Nord-Süd-Gefälle im Datenschutz für den grenzüberschreitenden Datenverkehr ergeben, haben inzwischen ebenfalls die zuständigen EG-Gremien im Hinblick auf eine Beeinträchtigung des gesamten Binnenmarktkonzeptes erkannt. Die EG-Kommission ist derzeit daher auch offensichtlich entschlossen, in Zukunft keinesfalls mehr einen „Fleckenteppich" unterschiedlich strenger nationaler Vorschriften in diesem Bereich zuzulassen. Ob dies zu einer Fixierung lediglich eines Minimalstandards, der hinter z.T. schon erreichtem nationalem Datenschutz zurückbleibt oder aber zu einem auch in der Praxis hohen Schutzniveau innerhalb einer europäischen Datenverkehrsordnung führt, muß sich nach der nun allgemein in Gang gesetzten Debatte über die Vorschläge der Kommission zeigen. Zumindest mittelfristig besteht die berechtigte Hoffnung, daß ein „Europa der zwei Geschwindigkeiten" im Hinblick auf den Schutz personenbezogener Daten überwunden wird.

## Handelsregister und gewerbliche Datenbank

BGH, 12.7.89 (IVa ARZ (VZ) 9/88)

### Leitsätze

1. Das Recht auf Einsicht in das Handelsregister ist weit gefaßt und umfaßt auch die Durchsicht großer Teile oder des ganzen Registers sowie die Dokumentation durch selbstgefertigte Abschriften gegebenenfalls unter Zuhilfenahme technischer Reproduktionsgeräte.
2. § 9 HGB gibt aber kein Recht auf Gestattung der Mikroverfilmung des gesamten Bestandes des Handelsregisters, um sie als eigene Datei in Konkurrenz zum Handelsregister gewerblich zu verwerten. Die Gestattung eines solchen Vorhabens steht im Ermessen der Justizverwaltung.

Das BGH-Urteil zur Mikroverfilmung des Handelsregisters wird mittlerweile von den Urteilen zustimmend zitiert, deren Leitsätze sich im folgenden finden.

## OLG Karlsruhe, 24.7.1990, VA 3/90

Leitsatz
Ein ausdrücklich als Einsichtsersuchen nach HGB § 9 an das Registergericht gerichteter Antrag, Kopien von Handelsregisterauszügen betreffend 170 Firmen zu übersenden, ist auch dann vom Registergericht und nicht vom Amtsgerichtspräsidenten zu bescheiden, wenn der Verdacht besteht, der Antragsteller wolle damit unter Verstoß gegen die vom BGH (12. Dezember 1989, IVa ARZ (VZ) 9/88, BGHZ 108, 32) aufgestellten Grundsätze das Handelsregister in einer Weise benutzen, die mit einer Einsicht nach HGB § 9 nichts mehr gemein hat.

## OLG Hamm, 17.1.1991 (15 W 482/90)

Leitsätze der Redaktion
1. Nach § 9 HGB steht die Einsicht in das Handelsregister jedermann zu. Dieses Einsichtsrecht ist nicht vom Nachweis irgendeines Interesses abhängig. Es steht dem Einsichtnehmenden frei, zu welchen Zwecken er die Handelsregisterauszüge verwerten will.
2. Der Antrag, Handelsregisterauszüge von zehn Firmen zu erhalten, kann nicht so ausgelegt werden, daß er auf die Erlaubnis zur Erfassung der gesamten Daten des Handelsregisters gerichtet ist.
3. Die Gesamterfassung sämtlicher Daten des Handelsregisters ist grundsätzlich nicht verbotenen.