Datenschutzrechtliche Spaltung in Europa? Teil 1

Andreas Günther

Die Kommission der Europäischen Gemeinschaften hat am 27. Juli 1990 im Rahmen eines ganzen EG-Datenschutzpaketes[1] den Vorschlag einer Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten vorgelegt, und in einem kleinen luxemburgischen Städtchen wurde am 19. Juni 1990 das Übereinkommen zur Durchführung des nach demselben Ort benannten Schengener Übereinkommens betreffend den schrittweisen Abbau der Kontrollen an den gemeinsamen Grenzen vom 14. Juni 1985[2] unterzeichnet. Grenzüberschreitender Datenschutz ist aktueller denn je. Vor dem Hintergrund der Tatsache, daß es in fünf von zwölf EG-Staaten immer noch kein allgemeines Datenschutzgesetz gibt, stellt sich die Frage: Erwartet uns eine datenschutzrechtliche Spaltung im EG-Raum?

Um dieser Frage nachzugehen, veranstalteten das Institut für Rechtsphilosophie und Rechtsinformatik der Ludwig-Maximilians-Universität München, der Lehrstuhl für Rechtstheorie der staatlichen Universität Mailand und das Italienische Kulturinstitut München am 1. März 1991 einen Workshop mit dem Thema „Das Nord-Süd-Gefälle im Europäischen Datenschutz nach dem Schengener Abkommen". Die Veranstaltung, die sich inzwischen schon traditionell mit hochaktuellen Themen im Schnittfeld von Informationstechnologie und Rechtswissenschaft beschäftigt – Vorjahresthemen waren Philosophie und Praxis Neuronaler Computer in der Rechtswissenschaft und Juristische Datenbanken auf optischen Speichermedien (CD-ROMs) –, fand wieder in den Räumen und unter besonderer Gastfreundschaft des Italienischen Kulturinstitutes statt. Neben den Referenten – in der Reihenfolge der Vorträge – Prof. Dr. Mario G. Losano (Università Statale di Milano), Prof. Dr. Hans-Ullrich Gallwas (Universität München), Dr. Giovanni M. Borrello (Società di Informatica delle Camere di Commercio Italiane S.p.A., kurz: CERVED, Mailand) und RA Dr. Jochen Schneider (München) nahmen an dem Workshop unter Leitung von Prof. Dr. Lothar Philipps (Universität München) unter anderem Prof. Dr. Michael Lehmann (Universität München) sowie der Bayerische Landesdatenschutzbeauftragte Sebastian Oberhauser teil. Der folgende Veranstaltungsbericht soll den Verlauf des Workshops – versehen mit einigen Anmerkungen des Verfassers – nachzeichnen. Die Reihenfolge der in sich selbständigen Vorträge wird aus inhaltlichen Gründen nicht beibehalten, vielmehr soll zunächst das deutsche Instrumentarium grenzüberschreitenden Datenschutzes dargestellt werden, bevor die italienische Sichtweise wiedergegeben wird. Die Referate und Beiträge der z.T. lebhaft geführten Diskussionen boten eine Momentaufnahme des datenschutzrechtlichen Entwicklungsstandes aus unterschiedlichen Perspektiven.

Das deutsche Instrumentarium des Datenschutzes

Notwendigkeit eines speziellen datenschutzrechtlichen Instrumentariums

Einen Überblick über das deutsche System des Datenschutzes gab Prof. Gallwas in seinem Referat. Ausgehend von dem Befund, daß das überkommene rechtliche Instrumentarium zum Schutz vor allgemeinen Rechtsverletzungen und zu deren Wiedergutmachung nicht den Besonderheiten moderner Datenverarbeitungstechnologie gerecht werde und demnach ein spezielles datenschutzrechtliches Instrumentarium notwendig sei, stellte er die Prämisse auf, daß dieses so angelegt sein müsse, daß datenschutzrechtliche Rechtsverletzungen von vorneherein verhindert würden. Datenschutz müsse als Vorfeldschutz präventiv Gefahrenpotentiale benennen und schon ihre Entstehung zu vermeiden trachten. Erforderlich seien aber im Hinblick auf die Lebenswirklichkeit nicht nur punktuell wirkende Verbote oder Gestattungen der Datenerhebung und -verarbeitung, sondern ein Regelungsmodell für datenschutzrechtliche Rechtsverhältnisse, das eine Feinabstimmung je nach Zuordnung und Art der Beziehung zwischen dem Datenverarbeiter und dem Betroffenen zuließe.

Zentrales Schutzinstrument: Verarbeitungs- und Verwendungsverbot mit Erlaubnis- bzw. Einwilligungsvorbehalt

Es lag Prof. Gallwas in seinen Ausführungen insbesondere daran, die datenschutzrechtlichen Grundprinzipien zu verdeutlichen: Zentrales Schutzinstrument ist das grundsätzliche Verarbeitungs- und Verwendungsverbot mit Erlaubnis- bzw. Einwilligungsvorbehalt.

---

1 Übersichtlich zusammengestellt in BR-Drs. 690/90 v. 4.10.1990.

2 Übereinkommen von 1985 (Schengen I) abgedruckt in Bek. d. BMI v. 29.1.1986, GMBl. 1986, S. 79ff; Übereinkommen 1990 (Schengen II): Bundesanzeiger [BMJ], Jg. 42 Nr. 217a v. 23.11.1990.

Dieser datenschutzrechtliche Gesetzesvorbehalt, der seit dem Bundesdatenschutzgesetz vom 27. Januar 1977 kraft Gesetzes bestand (§ 3 BDSG a. F.), wurde durch das Bundesverfassungsgericht im Volkszählungsurteil vom 15. Dezember 1983[3] verfassungsrechtlich zu einem Grundrechtsvorbehalt überhöht, inhaltlich teils ausgeweitet und teils stärker konturiert und steht seither nicht mehr zur Disposition des Gesetzgebers.[4] Die Novelle des Bundesdatenschutzgesetzes vom 20. Dezember 1990[5] hat das Datenschutzrecht nun in erster Linie an die Vorgaben des Völkszählungsurteils – insbesondere den Ersatz des unbestimmten Rechtsbegriffs der schutzwürdigen Belange des Betroffenen als eigentlichem Schutzgut des Bundesdatenschutzgesetzes a.F. durch die griffigere Denkfigur des informationellen Selbstbestimmungsrechts – angepaßt.

Recht auf informationelle Selbstbestimmung

Zum Dreh- und Angelpunkt des gesamten Datenschutzrechts als speziellem Persönlichkeitsschutzrecht ist damit das Recht auf informationelle Selbstbestimmung geworden, die Befugnis des einzelnen, grundsätzlich selber über Preisgabe und über Verwendung seiner persönlichen Daten zu bestimmen, als besonderer Ausprägung des allgemeinen Persönlichkeitsrechts (Art. 2 Abs. 1 i.Vm. Art. 1 Abs. 1 GG). Grundlage des Datenschutzrechts – nicht nur für den staatlichen Bereich, sondern auch für Datenerhebung und -verarbeitung durch Private, zu der sich das Bundesverfassungsgericht aber noch nicht explizit geäußert hat – ist die Abwägung zwischen dem Erhebungs-, Verarbeitungs- und Nutzungsinteresse einerseits (den Allgemeinwohlinteressen des Staates bzw. den Grundrechten der privaten Datenverarbeiter) und andererseits dem informationellen Selbstbestimmungsrecht, d.h. dem Interesse des Betroffenen daran, daß seine Daten nicht erhoben, nicht gespeichert, nicht genutzt und nicht übermittelt werden. Im Bereich der Datenverarbeitung durch öffentliche Stellen stellt sich diese Abwägung als Grundrechtsanwendung, für die private Datenverarbeitung als Grundrechtskollision, die nach dem Prinzip der praktischen Konkordanz zu lösen ist, dar. In den allgemeinen Datenschutzgesetzen des Bundes und der Länder sowie entsprechenden bereichsspezifischen Regelungen (z.B. im Polizeirecht) hat der Gesetzgeber zumindest für bestimmte Verarbeitungsphasen der dateibezogenen Datenverarbeitung diese Abwägung durch einen Numerus Clausus von Erlaubnistatbeständen, verbunden mit einer Reihe von Schutzvorkehrungen (z.B. Zweckbindung, Weitergabebeschränkungen, Publizitätsgrundsatz und Auskunftsrechte, Fremdaufsicht und Kontrolle durch Datenschutzbeauftragte), im Einzelfall vorweggenommen oder zumindest vorstrukturiert. Sofern der Gesetzgeber aber die Abwägung für Sonderlagen nicht selber vorgenommen hat, ist immer auf das verfassungsrechtlich vorgegebene persönlichkeitsrechtliche Abwägungsmodell zurückzugreifen.

Persönlichkeitsrechtliches Abwägungsmodell

Grundprinzip: Datenschutz ist die Regel, Datenverarbeitung die Ausnahme

Entscheidend sei aber laut Prof. Gallwas, daß der Datenverarbeiter durch das Grundprinzip „Datenschutz als Regel, Datenverarbeitung als Ausnahme" in jedem Fall besonderen Rechtfertigungszwängen unterworfen werde. Wer personenbezogene Daten verarbeite, habe es in tatsächlicher Hinsicht leicht, rechtlich seien ihm jedoch viele Hürden aufgerichtet. Möge er sich über diese Hürden auch zunächst hinwegsetzen, er geriete zunehmend unter so großen Rechtfertigungsdruck, daß sich bei jedem Datenverarbeiter früher oder später ein Interesse bilde, diesem zu entgehen. Dieses Interesse zu wecken und wach zu halten, sei das wirksamste Mittel zur Realisierung des Datenschutzes als allgemeinem Rechtsprinzip.

Bereichsspezifische Sonderregelungen im Polizei- und Ordnungsrecht

Dies gelte natürlich nicht nur für die Auffangvorschriften der allgemeinen Datenschutzgesetze, sondern grundsätzlich auch für bereichsspezifische Regelungen. In der sich an das Referat anschließenden Diskussion wurde ergänzend auf besondere Aspekte im Sicherheitsrecht hingewiesen. Angesprochen auf die in der seit dem 1. Oktober 1990 geltenden Neufassung des bayerischen Polizeiaufgabengesetzes[6] erstmals vorgesehenen Vorschriften über die Datenverarbeitung durch Polizeibehörden,[7] mußte der Bayerische Landesdatenschutzbeauftragte Oberhauser feststellen, daß die Art. 30ff. BayPAG (insb. Art. 39) im Hinblick auf die Zweckbindung datenschutzrechtlich gesehen immer noch

---

3 BVerfGE 65, 1ff.

4 Hierzu nachdenklich Fiedler, CR 1989, S. 131ff m.w.N.

5 BGBl. I 1990, S. 2954ff; die Novelle ist (bis auf die in § 10 Abs. 4 Satz 3 und 4 BDSG n.F. enthaltenen Sondervorschriften über Stichproben im Hinblick auf die Zulässigkeit der Übermittlung personenbezogener Daten im Rahmen automatisierter Abrufverfahren sowie über die Stapelverarbeitung, die erst ab dem 1. Januar 1993 gelten) am 1. Juni 1991 in Kraft getreten.

6 BayGVBl. 1990, S. 397ff.

7 Hierzu Honnacker/Bartelt, BayVBl. 1991, S. 10ff; vgl. im Hinblick auf den MEPolG Knemeyer, NVwZ 1988, S. 193ff.

relativ weit gefaßte Erhebungs-, Nutzungs- und Übermittlungsbefugnisse enthielten. Prof. Gallwas äußerte daraufhin die Ansicht, daß das Zweckbindungsgebot als besonderer Ausprägung des informationellen Selbstbestimmungsrechts zwar grundsätzlich auch für den bereichsspezifischen Datenschutz im Polizei- und Ordnungsrecht gelte, gleichzeitig jedoch das Effektivitätsprinzip im Hinblick auf die im Bereich der öffentlichen Sicherheit und Ordnung oft überwiegenden Interessen des Allgemeinwohls zu berücksichtigen sei. Der Charakter des Sicherheitsrechts als „sozialpolitischem Feuerwehrrecht" rechtfertige eine eher großzügige Handhabung der Datenerhebung, -nutzung und -übermittlung soweit entsprechende Kontrollen (z.B. die umfassende Protokollierung sämtlicher Abfragen zwecks stichprobenartiger Überprüfung der Berechtigung) gegen einen Mißbrauch der Daten für private Zwecke vorhanden seien. In Anlehnung an eine vom Bayerischen Verfassungsgerichtshof geprägten Formel betonte Prof. Gallwas, daß Datenschutz nicht Täterschutz werden dürfe.

„Datenschutz, nicht Täterschutz"

Der Transfer von Daten aus öffentlichen und privaten Datenbanken über Ländergrenzen hinweg – die deutsche Sicht

Aufbauend auf diesem Überblick über datenschutzrechtliche Grundprinzipien ging Dr. Schneider auf die beim Im- und Export von Daten in ausländische Staaten im einzelnen zu beachtenden Vorschriften des deutschen allgemeinen Datenschutzrechts ein. Dabei stellte er die alte Rechtslage derjenigen nach der Novelle des Bundesdatenschutzgesetzes gegenüber. Am Anfang seines Referates stand die Feststellung, daß ein europäischer Binnenmarkt auch ein einheitlicher europäischer Informationsmarkt sein muß[8], in dem grenzüberschreitende Informationsflüsse nur so wenig wie möglich behindert werden dürfen. Dem steht entgegen, daß bislang keine Harmonisierung der nationalen Datenschutzrechtssysteme herbeigeführt worden ist. Nach mehreren Anläufen auf EG-Ebene liegt zwar jetzt der z.T. auf deutschen Vorstellungen beruhende Vorschlag einer „Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vor[9]. Bislang richtet sich der grenzüberschreitende Verkehr mit personenbezogenen Daten aber – abgesehen von sehr allgemeinen völkerrechtlichen Vorgaben in Art. 12 einer Datenschutzkonvention des Europarates[10] und Teil 3 einer OECD-Empfehlung[11] sowie u.U. anwendbarem gemeinschaftlichem Primärrecht[12] – ausschließlich nach nationalem Recht.[13]

Einheitlicher europäischer Informationsmarkt

Bislang: Lediglich nationale Regelungen

Da grenzüberschreitender Datenfluß aber im deutschen Bundesdatenschutzgesetz nur am Rande ausdrücklich erwähnt ist (z.B. in § 2 Abs. 3 Nr. 2 sowie § 11 Satz 3 BDSG a.F.), müssen die auftauchenden Fragen z.T. durch Rückgriff auf die allgemeinen Regelungen beantwortet werden. Einschlägig sind insofern die Vorschriften für die „Übermittlung von Daten". Fast gleichlautende Legaldefinitionen des Begriffs „Übermittlung" enthalten sowohl das alte als auch das neue Bundesdatenschutzgesetz (§ 2 Abs. 2 Nr. 2 BDSG a.F. bzw. § 3 Abs. 5 Nr. 3 BDSG n.F.). Dr. Schneider begrüßte, daß § 3 Abs. 5 Nr. 3 Buchstabe b) BDSG n.F. gegenüber der mißverständlichen alten Regelung nun klargestellt hat, daß Übermittlung nur der tatsächliche Zugriff auf die Daten, nicht aber

Grenzüberschreitender Datentransfer im BDSG nur z.T. explizit geregelt

Übermittlung: „Bekanntgabe personenbezogener Daten an Dritte"

---

8 Hierzu zuletzt Steven, CR 1991, S. 48ff.

9 Siehe oben Fn. 1 und unten Fn. 29; der Vorschlag enthält in Art. 1 Abs. 2, Art. 4 Abs. 3 und Art. 24f auch ausdrückliche Regelungen im Hinblick auf grenzüberschreitenden Datentransfer.

10 Am 17. September 1980 verabschiedete der Ministerrat des Europarates ein Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (BGBl. II 1985, S. 538ff); die Konvention wurde am 28. Januar 1981 für die Unterzeichnung durch die Mitgliedsstaaten zugänglich gemacht und wird daher z.T. in Zusammenhang mit diesem Datum genannt; sie trat zwar am 1. Oktober 1985 nach der Ratifikation durch den fünften Signatarstaat in Kraft, harrt aber immer noch der Ratifikation durch mehr als ein Dutzend der inzwischen 25 Mitgliedsstaaten; ausführlich zur Europarats-Konvention Burkert, CR 1988, S. 751ff m.w.N.

11 Empfehlung des Rates der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung über Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten vom 23. September 1980 (die offizielle Übersetzung der deutschsprachigen Mitgliedsstaaten ist abgedruckt in Simitis/Dammann u.a., Dokumentation zum Bundesdatenschutzgesetz, D 12.1).

12 Zu den völker- und europarechtlichen Aspekten vgl. Bergmann, Nachr. f. Dok., Jg. 38 (1987), S. 293ff; Klaas, CR 1986, S. 680ff; Riegel, DSWR 1989, S. 36ff, 65ff; ders., ZRP 1990, S. 132ff; Ulbricht, CR 1990, S. 602ff; Vivant, IuR 1986, S. 159ff; jeweils m.w.N.

13 Rechtsvergleichender Überblick in A.C.M. Nugter, Transborder Flow of Personal Data within the EC (Kluwer Computer/Law Series no. 6), Deventer 1990.

Stelle ausgeübt werde. Im Hinblick darauf, daß eine Tätigkeit in einem anderen Rechtskreis i.d.R. auch immer mit einer anderen funktionalen Aufgabe als im Inland verbunden sei, käme man – unabhängig von der Rechtsform – im Hinblick auf ausländische Niederlassungen zu dem gewünschten Ergebnis, soweit es sich nicht nur um unselbständige Betriebsstätten handele.

Datenexport aus öffentlichem Bereich: Strenge Voraussetzungen

Im einzelnen gilt für die Zulässigkeit der Übermittlung personenbezogener Daten ins schon das Bereithalten der Daten zum Abruf ist. Fraglich ist in diesem Zusammenhang jedoch weiterhin, wann eine Bekanntgabe der Daten an Dritte anzunehmen ist, d.h. ob z.B. die Tochterfirma eines deutschen Unternehmens im Ausland eine „Person oder Stelle außerhalb der speichernden Stelle" i.S.d. § 2 Abs. 3 Nr. 2 BDSG a.F. bzw. § 3 Abs. 9 BDSG n.F. ist. Dr. Schneider plädierte dafür, Niederlassungen außerhalb des Geltungsbereichs des Bundesdatenschutzgesetzes i.d.R. als Dritten anzusehen. In der sich an das Referat anschließenden Diskussion zu diesem Punkt ging später Prof. Gallwas ergänzend auf den sog. funktionalen Stellenbegriff im Gegensatz zum organisatorischen Stellenbegriff ein: Während letzterer auf die Rechtsform der anderen „Stelle" als selbständiger juristischer Person, also allein auf die rechtliche Eigenständigkeit abstelle und somit zu zufälligen Ergebnissen führe, frage ersterer auch nach der funktionalen Eigenständigkeit, also danach, ob eine andere Funktion als die der speichernden Ausland folgendes: Im öffentlichen Bereich war Datenexport bislang nach § 11 BDSG a.F. nur dann zulässig, wenn dies zur Erfüllung der Aufgaben der übermittelnden Stelle erforderlich war oder soweit der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machte und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt wurden. Der Maßstab der „schutzwürdigen Belange des Betroffenen" ist im neuen Bundesdatenschutzgesetz nach dem Volkszählungsurteil verfassungsrechtlich durch das allgemeine Recht auf informationelle Selbstbestimmung zu erweitern[14]. § 16 Abs. 1 Nr. 2 BDSG n.F. spricht insofern jetzt von einem schutzwürdigen Interesse des Betroffenen an einem Ausschluß der Übermittlung. Ganz überwiegend wird davon ausgegangen, daß im öffentlichen Bereich streng auf das Äquivalenzprinzip abzustellen ist und eine Übermittlung i.d.R. zu unterbleiben hat, wenn im Empfängerland kein kodifiziertes Datenschutzrecht existiert, das den Anforderungen des Bundesdatenschutzgesetzes entspricht[15]. Die schon bislang restriktiv zu handhabende Regelung wird in § 17 BDSG n.F., der die Datenübermittlung an Stellen außerhalb des Geltungsbereichs des Gesetzes explizit regelt, noch verschärft. So trägt jetzt die übermittelnde Stelle die Verantwortung für die Zulässigkeit der Übermittlung (§ 17 Abs. 3), und eine Übermittlung hat schon dann zu unterbleiben, wenn Grund zu der Annahme besteht, daß durch sie gegen den Zweck eines deutschen Gesetzes verstoßen würde (§ 17 Abs. 2). Eine Übermittlung von Daten aus öffentlichen Stellen an Behörden in Staaten, in denen weder rechtlich noch praktisch ein entsprechender Schutz personenbezogener Daten gewährleistet wird, ist demnach nach dem Bundesdatenschutzgesetz prinzipiell unzulässig.[16]

Stellenbegriffe

Äquivalenzprinzip

Auch im privaten Bereich setzt das deutsche Datenschutzrecht nicht die ausdrückliche Lizenzierung von Datenexporten voraus, sondern folgt dem sog. materiellrechtlichen Modell. Bei der Datenverarbeitung durch nicht-öffentliche Stellen für eigene Zwecke unterliegt die Übermittlung ins Ausland aber schwächeren Restriktionen.[17] Sie war bislang in § 24 BDSG a.F. geregelt und grundsätzlich zulässig im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen oder soweit es zur Wahrung berechtigter Interessen der übermittelnden Stelle, eines Dritten oder der Allgemeinheit erforderlich war und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt wurden. In die Interessenabwägung im Rahmen der 3. Alternative mußte insbesondere auch der Schutz der übermittelten Daten beim Empfänger einfließen. War dieser nicht gewährleistet, so bedurfte es in jedem Fall der Einwilligung des Betroffenen. Umstritten war (und wird es wohl auch nach der Novelle bleiben, solange es Staaten ohne angemessene Datenschutzgesetzgebung gibt) die Frage, ob es zur Wahrung der schutzwürdigen Belange des Betroffenen

Privater Bereich: Schwächere Restriktionen

Wahrung schutzwürdiger Belange des Betroffen durch Vertragsvereinbarungen?

[14] Vgl. oben die Ausführungen von Prof. Gallwas.

[15] Ordemann/Schomerus, Bundesdatenschutzgesetz mit Erläuterungen, § 11 Anm. 3.

[16] Zu ggf. als lex specialis vorgehenden bereichsspezifischen Regelungen für die grenzüberschreitende Informationsverarbeitung der Sicherheitsbehörden ausführlich Riegel, CR 1987, S. 311ff, 446ff, 614ff m.w.N.

[17] Vgl. hierzu Baumeister, RDV 1990, S. 23ff; Bergmann, Nachr. f. Dok., Jg. 38 (1987), S. 293ff; Schapper, CR 1987, S. 86ff (90ff); jeweils m.w.N.

ausreicht, wenn der empfangenden Stelle durch vertragliche Vereinbarungen ein ausreichendes Datenschutzniveau auferlegt bzw. dieses durch sonstige Maßnahmen sichergestellt wird[18] oder ob in dem ausländischen Staat ein dem Bundesdatenschutzgesetz vergleichbares Datenschutzgesetz erlassen worden sein muß.[19] Im Gegensatz zur Regelung der Übermittlung ins Ausland durch öffentliche Stellen geht die wohl h.M. davon aus, daß es im privaten Bereich ausreicht, wenn sich der Empfänger vertraglich verpflichtet, die Daten im Ausland ebenso zu schützen, wie dies in der Bundesrepublik der Fall ist.

Novelle: Tendenz zu liberalerer Handhabung?

Die Novelle verwendet in § 28 BDSG n.F. zwar z.T. anderslautende Formulierungen als bisher, dies liegt aber auch darin begründet, daß die Voraussetzungen für die Zulässigkeit des Speicherns, Veränderns, Nutzens und Übermittelns personenbezogener Daten jetzt einheitlich in einer Vorschrift geregelt sind. Es sei abzuwarten, wie die neuen Formulierungen im einzelnen ausgelegt würden, Dr. Schneider sah jedoch durchaus die Möglichkeit einer Tendenz zu eher liberalerer Handhabung als bislang. Ähnlich stellt sich die Rechtslage im Hinblick auf die Zulässigkeit der grenzüberschreitenden Datenverarbeitung für gewerbliche Zwecke dar (bisher in § 32 Abs. 2 u. 3 BDSG a.F. geregelt, jetzt nicht mehr im Rahmen eines eigenen Abschnitts „Geschäftsmäßige Datenverarbeitung nicht-öffentlicher Stellen für fremde Zwecke", sondern als „Geschäftsmäßige Datenspeicherung zum Zwecke der Übermittlung" in § 29 Abs. 2 BDSG n.F.). Datenexport im privaten Bereich unterliegt demnach – folgt man der herrschenden liberalen Ansicht – im Großen und Ganzen keinen besonderen Erschwernissen, soweit zumindest durch vertragliche Verpflichtungen ein ausreichender Schutz der personenbezogenen Daten gewährleistet ist.

Import personenbezogener Daten

Der Import personenbezogener Daten in den Geltungsbereich des Bundesdatenschutzgesetzes ist hingegen auf den ersten Blick aufgrund des hohen Schutzniveaus in der Bundesrepublik aus Sicht des Betroffenen scheinbar unproblematisch, zumal das Bundesdatenschutzgesetz nicht auf Staatsangehörigkeit oder Aufenthaltsort des Betroffenen abstellt. Diesbezüglich ist aber zu beachten, daß die „Einfuhr" personenbezogener Daten bislang gesetzlich im Grunde nicht erfaßt war. Der Schutz des Bundesdatenschutzgesetzes a.F. setzte erst mit der erstmaligen Speicherung der Daten im Inland ein, allein die Übermittlung aus dem Ausland, die sich aus Sicht des Gesetzes als Erhebung der Daten darstellt, unterlag noch keinen Beschränkungen[20], es sei denn sie fand im Rahmen einer Auftragsdatenverarbeitung im Ausland statt, die sich nach den Übermittlungsvorschriften zu richteten hatte und insofern wie Inlandsverarbeitung behandelt wurde (vgl. § 2 Abs. 3 Nr. 2, § 8, § 22 Abs. 2 BDSG a.F.). Das bedeutete demnach, daß es keine Übermittlungsschranken für personenbezogene Daten aus dem Ausland gab, daß sich erst Speicherung, Übermittlung, Veränderung und Löschung dieser importierten Daten im Inland nach den Schutzvorschriften des Bundesdatenschutzgesetzes zu richten hatten. In der Novelle hat der Schutz nun eine Vorverlagerung erfahren, weil im Hinblick auf die Volkszählungsrechtsprechung auch die Erhebung personenbezogener Daten – für öffentliche Stellen ausdrücklich in § 13 BDSG n.F., im privaten Bereich nach Treu und Glauben (die Drittwirkung der Grundrechte als Einfallstor der informationellen Selbstbestimmung) – erfaßt und geregelt wird.

Novelle: Vorverlagerung des Datenschutzes

Resümierend stellte Dr. Schneider fest, daß in Deutschland im öffentlichen Bereich relativ strenge Voraussetzungen, im privaten Bereich hingegen schwächere Restriktionen für grenzüberschreitenden Datentransfer bestehen.

---

18 Gallwas/Schneider u.a., Datenschutzrecht, § 24 Rn. 84; Ordemann/Schomerus, aaO., § 24 Anm. 5.

19 Simitis/Dammann u.a., Kommentar zum Bundesdatenschutzgesetz, § 24 Rn. 46.

20 § 9 II BDSG a.F., der sich als einzige Vorschrift mit der Erhebung von Daten im öffentlichen Bereich befaßte, traf aber keine ausdrücklichen Regelungen hinsichtlich deren Zulässigkeit.