

Joachim Jacob/Helmut Heil

»Datenschutz im Spannungsfeld von staatlicher Kontrolle und Selbstregulierung«

1. Selbstregulierung im Spektrum der Antworten auf datenschutzrechtliche Gegenwartsfragen

Wirtschaftliche Globalisierung und Netzoffenheit in weltweiten Dimensionen bilden deutliche Markierungspunkte für die Grenzen nationalstaatlicher Einflussmöglichkeiten und die eingeschränkte Macht hoheitlicher Handlungsformen. Das Netz kennt keine Grenzkontrollen, im Netz herrscht keine Rechtssicherheit (Roßnagel 1997, S. 28). Angesichts der wachsenden Gefahren eines Zurückbleibens des Rechts hinter den umwälzenden Herausforderungen der Informationsgesellschaft kann es kaum verwundern, dass in der Reformdebatte um die Weiterentwicklung des Datenschutzes nicht nur gesetzlichen Maßnahmen, sondern auch Mechanismen der Selbstregulierung ein zunehmend höherer Stellenwert eingeräumt wird (vgl. Bull 1998, S. 313 und Tauss/Özdemir 2000, S. 144). Und nicht nur unter dem Blickwinkel innerstaatlicher Reformdiskussionen, sondern auch im Zusammenhang mit der erwünschten Akzeptanz europäischer Rechtsvorstellungen im Nicht-EU-Ausland wird beispielsweise in selbstregulierenden »Codes of Conduct« eine Möglichkeit gesehen, international bestehende Verständigungsprobleme über Eignung und Erforderlichkeit staatlicher Regulierungsmaßnahmen zu überbrücken (Kranz, 1998, S. 217 und 2001, S. 161). Zu den Brückenbauern auf diesem Gebiet zählt in vorderster Reihe Alfred Büllsbach, der die Diskussion um datenschutzrechtliche Codes of Conduct für international operierende Konzerne seit Jahren mit hohem Engagement und nachhaltig vorantreibt (siehe etwa Büllsbach, in: Büllsbach (Hrsg.), 17 sowie 2000, S. 3 f. und 2001, S. 137 f.)

2. Ernüchternde (Zwischen-)Bilanz außereuropäischer Vorbilder

2.1 Die Vereinigten Staaten von Amerika

Insbesondere die transatlantische Datenschutzdiskussion zwischen der Europäischen Union und den USA ist geprägt von dem Gegensatz zwischen einer Präferenz für die Regelungsverantwortung delegierende Selbstregulierung und für eigenverantwortliche Gestaltung der erforderlichen Prozesse auf amerikanischer Seite und einer deutlich stärker auf formellen Rechts- und insbesondere Gesetzesvorschriften beruhenden europäischen Regelungsorientierung (Heil 1999 b, S. 458 f.). Der dem Safe-Harbor-Arrangement (Entscheidung der Europäischen Kommission vom 26.7.2000, ABl. Nr. L 215 vom 28.8.2000, 7 ff.; s.a. Heil 1999 b, S. 461, 2000, S. 444) zugrunde liegende Kompromiss greift denn auch auf selbstregulierende Elemente zurück, für die die

europäische Datenschutzrichtlinie 95/46/EG (ABl. Nr. L 281 vom 23.11.1995, 31 ff.) im Rahmen der Bestimmung der Angemessenheit des Schutzniveaus in einem Drittstaat nach Art. 25 Abs. 2 grundsätzlich offen ist (vgl. Artikel 29-Datenschutzgruppe, Dok. GD XV D/5057/97 (WP 7¹)). Denn ein Schutzkonzept entspricht auch dann dem Regelungszweck, wenn es nicht auf gesetzliche Vorschriften, sondern auf ein auf freiwilliger Selbstverpflichtung beruhendes Reglement gestützt wird, solange es nur aufgrund seiner inhaltlichen Beschaffenheit einen gleichwertigen Schutzeffekt verspricht (Dammann 2000 S. 25).

Mit Blick auf die USA gibt es jedoch gute Gründe, die Vorkehrungen besonders kritisch zu prüfen, die die praktische Durchführung der auf selfregulation beruhenden Regelungsbereiche gewährleisten sollen. Denn ausweislich der ersten zusammenfassenden Darstellung des Datenschutzrechts der Vereinigten Staaten aus dem Jahre 1996 (Schwartz/Reidenberg 1996, S. 215 ff., 387 ff., 379 ff.) wird der gemeinsamen Strategie von amerikanischen Regierungskreisen und Wirtschaft, gesetzlichen Regelungsbedarf zu verneinen und ausschließlich auf Selbstregulierung zu setzen, ein deutliches Zeugnis erteilt: Branchen- und Unternehmensrichtlinien sind in den USA weitgehend inexistent, und wenn vorhanden, sind sie vielfach den für die Datenverarbeitung Verantwortlichen unbekannt und ohne wirksamen Sanktionsmechanismus. Abgesehen von Ausnahmen mangelt es an Transparenz für die Betroffenen ebenso wie an durchsetzbaren Individualrechten oder einem wirksamen Schutz gegen zweckwidrige Datenverarbeitungen. Auch neuere Untersuchungen bestätigen die beschränkte juristische Wirksamkeit der Selbstregulierung nach amerikanischem Vorbild, indem sie die zentralen Probleme der selfregulation, die dem soft law immanente Unverbindlichkeit und die damit zusammenhängenden Kontroll- und Vollzugsdefizite, offen legen (Wuermeling 2000, S. 187 ff.²; Grimm/Roßnagel 2000, S. 448 ff.³; Schwartz 2000, S. 349; 1999 S. 1609; Reidenberg 2001, S. 717). Es überrascht daher wenig, dass die Verhandlungen mit der US-Regierung über das Safe Harbor Principle »Enforcement« einen Schwerpunkt bei den langwierigen Beratungen bildeten, wobei gerade in diesem Punkt ein »Restrisiko« am größten sein dürfte (Stellungnahme 4/2000 (Dok. CAO7/434/00 = WP 32) der Art. 29-Gruppe, 7 f.).

2.2 Japan, Singapur, Hongkong

Asiatische Selbstregulierungskonzepte finden sich in Japan, Singapur und Hongkong. Im Jahre 2000 wurden in Hongkong sog. Codes of Practice on Human Resource Management verabschiedet (Privacy Commissioner Hong Kong 2000, S. 9 f. und 68 ff.). In der aktuellen Diskussion befindet sich ein Draft Code of Practice on Monitoring and Personal Data Privacy at Work (Privacy Commissioner Hong Kong 2002; zu Singapur s. EPIC/PI 2000, S. 13 f. und Privacy Law and Business Int'l Newsletter, Vol. 53, April 2000, 7). In Japan mit seiner »verwirrenden Vielfalt von Guidelines« (Überblick bei Roßnagel/Scholz 2000, S. 458) findet man solche für elektronisches Direktmarketing im Rahmen

des Business-to-Consumer E-Commerce. Bei ihrer Ausarbeitung vom Ministerium für internationalen Handel und Industrie (MITI) gefördert, gelten sie für die Mitglieder des japanischen Direktmarketingverbands. Doch auch aus Japan ist hinsichtlich der Befolgsrate selbstregulierender Vorgaben Kritik zu hören, da auch dort – ähnlich dem Beispiel USA – die entsprechenden Schwachstellen im Bereich der Durchsetzungsmöglichkeiten liegen: Weder ist eine allgemeine Beachtung der Guidelines sichergestellt, noch erstreckt sich ihre Geltung auf die Angestellten der den Guidelines verpflichteten Unternehmen, die ihnen infolgedessen – da Sanktionen nicht zu befürchten sind – keine besondere Aufmerksamkeit schenken (Roßnagel/Scholz 2000, S. 458 Fn. 61).

Von Ernüchterung ist denn auch die Bilanz gekennzeichnet, die die vom Electronic Privacy Information Center (EPIC) in Washington und von Privacy International (PI) in London gemeinsam verantwortete Studie »Privacy and Human Rights 1999« zieht. Die Studie zeigt mit ungeschminkter Deutlichkeit, dass die bisherigen Anstrengungen zum Datenschutz durch Selbstregulierung enttäuschend ausfallen, wobei insbesondere »Adequacy« und »Enforcement« die Hauptprobleme bilden; in vielen Ländern böten selbstregulierende Elemente nur geringen Schutz und mangelnde Durchsetzungsmöglichkeiten (EPIC/PI 1999, S. 13 f.).

3. Europäisches Parlament und Europarat

Mit dem Ziel, das noch entwicklungsfähige Vertrauen der Benutzer in den elektronischen Geschäftsverkehr durch ansprechende Lösungen für den Schutz der Privatsphäre zu intensivieren, beschlossen im Jahre 1999 das Europäische Parlament und der Ministerrat einen Aktionsplan zur Förderung der sicheren Nutzung des Internet. Dieser wird angesichts seiner knappen Mittelausstattung i.H.v. 25 Millionen Euro jedoch nur Anstöße bieten können. Das bis Ende 2002 laufende Programm sieht als einen von vier Schwerpunkten die Förderung der Selbstkontrolle durch Verhaltenskodizes vor (FAZ vom 27.7.2000, S. 8).

Für den Bereich des Europarats verabschiedete das Ministerkomitee am 23.2.1999 die Empfehlung zum Schutz personenbezogener Daten im Internet (R (99) 5), die im Anhang »Leitlinien für den Schutz der Privatsphäre im Internet« enthält. Die sog. »Internet Guidelines« stellen das erste derartige Regelwerk auf internationaler Ebene dar. Die Empfehlung verlangt von den Providern frühzeitige und umfassende Aufklärung über die mit ihren Diensten möglicherweise verbundenen Risiken und appelliert an die Nutzer, alle erreichbaren technischen Vorkehrungen zum Aufbau eines hohen Eigenschutzes zu treffen. Die Guidelines setzen dabei vor allem auf die Eigeninitiative von Providern und Nutzern, die möglichst weit im Vorfeld staatlicher Regulierung ansetzen sollte. Sie könnten als Modelle für verhaltensregelnde Codes of Conduct im nichtöffentlichen Bereich dienen.

4. Förderung von Verhaltensregeln nach der EG-Datenschutzrichtlinie

Das allein aus Art. 27 bestehende und »Verhaltensregeln« betitelte Kapitel V der EG-Datenschutzrichtlinie bietet einen interessanten Ansatz zur Sicherung eines bereichsspezifischen und technisch relevanten Datenschutzes für die Mitgliedstaaten der EU und des EWR. Die Vorschrift will der gegen die Selbstregulierung hauptsächlich vorzubringenden Kritik der Unverbindlichkeit, präzisiert durch die jederzeitige Abänderbarkeit und die mangelnde Durchsetzungsfähigkeit, durch die Einführung eines Konsultationsverfahrens zwischen staatlichen bzw. europäischen Stellen und den Verfassern von Verhaltensregeln begegnen.

Art. 27 Abs. 1 der Richtlinie verpflichtet Mitgliedstaaten und Kommission zur Förderung der Ausarbeitung von Verhaltensregeln. Dabei liegt das Ziel ausdrücklich darin, die bereichsspezifische Relevanz der aufgrund der Richtlinie erlassenen einzelstaatlichen Vorschriften zu erhöhen. Allerdings ist es den Mitgliedstaaten verwehrt, ihre innerstaatlichen Vorschriften durch Verhaltensregeln zu ersetzen, da diese lediglich der Unterstützung der nationalen Gesetzgebung zu dienen bestimmt sind (Dammann/Simitis 1997, Art. 27 Anm. 3; Ehmann/Helfrich 1999 Art. 27 Rdn. 8; Brühann 1999, Art. 27 Rdn. 8). Folglich können datenschutzrechtliche Verhaltensregeln – im Gegensatz zum Verbandsrecht, das etwa in Form von Satzungen abdingbares Recht durch verbandsrechtliche Sondervorschriften ersetzt – das Gesetz nicht substituieren oder inhaltlich abändern, sondern lediglich ausfüllen und vervollständigen.

In Art. 27 Abs. 2 ist ein Verfahren zum Erlass von Verhaltensregeln auf mitgliedstaatlicher Ebene geregelt, das eine Kooperation zwischen Berufsverbänden und staatlichen Stellen vorsieht. Der ausschließlich empfehlende Charakter der Verhaltensregeln und ihre reine Hilfsfunktion machen eine vorherige Genehmigung im Sinne eines »Unbedenklichkeitsattests« (Dammann/Simitis, 1997, Art. 27 Anm. 5), sowie die Überwachung ihrer Einhaltung durch eine Kontrollinstanz erforderlich. Daher sind sie den Aufsichtsbehörden zur Prüfung ihrer Übereinstimmung mit den Vorgaben des jeweiligen innerstaatlichen Rechts vorzulegen. Am Ende des dialogorientierten Verfahrens steht eine Entscheidung der Aufsichtsbehörde, die im Falle eines positiven Ausgangs die vorgelegten Regelungen bestätigend annimmt (im einzelnen Dammann/Simitis 1997, Art. 27 Anm. 8 f.; Brühann 1999, Art. 27 Rdn. 9 ff.).

Bestimmungen für Verhaltensregelungen auf der Ebene der Gemeinschaft enthält Art. 27 Abs. 3. Ihnen wird im Hinblick auf den Binnenmarkt zunehmende Bedeutung prognostiziert, da sie die Harmonisierung erheblich voran bringen können (Dammann/Simitis 1997, Art. 27 Anm. 10). Zuständig für Prüfung und Stellungnahme ist die Art. 29-Datenschutzgruppe (dazu Heil 1999 a, 472). Als Vorbereitung auf die praktische Ausführung dieses Auftrags hat die Gruppe eine diesbezügliche Arbeitsunterlage verabschiedet (Dok. GD XV D/5004/98 (WP13)). Danach bestimmt sie, ob ihr unterbreitete Verhaltensregeln mit den Datenschutzrichtlinien und gegebenenfalls den zu deren

Umsetzung erlassenen einzelstaatlichen Vorschriften in Einklang stehen und ob sie ausreichende Qualität und Kohärenz aufweisen sowie genügenden zusätzlichen Nutzen für die Richtlinien und andere geltende Datenschutzrechtsvorschriften liefern. Insbesondere stellt die Gruppe fest, ob der Entwurf der Verhaltensregeln ausreichend auf die spezifischen Fragen und Probleme des Datenschutzes in der jeweiligen Organisation oder auf dem spezifischen Sektor ausgerichtet ist und ob er für diese Fragen und Probleme ausreichend klare Lösungen bietet.

Drei Organisationen haben der Arbeitsgruppe bislang ihre Entwürfe für gemeinschaftliche Verhaltensregeln zur Annahme unterbreitet: FEDMA (Federation of European Direct Marketing Associations), IATA (International Air Transport Association) und AESC (Association of Executive Search Consultants). Die Art. 29-Gruppe hat entsprechende Untergruppen gebildet, die jeweils einen Verhaltenskodex prüfen.

5. EU-Mitgliedstaatliche Erfahrungen

Die generelle Linie der Richtlinie, die wichtigsten Elemente der verschiedenen nationalen Datenschutzgesetze zu kombinieren und zu einem Gesamtsystem zusammenzuführen, zeigt sich auch in Art. 27. Hinsichtlich der Förderung von Verhaltensregeln stützt sich die Vorschrift auf niederländische, britische und irische Vorbilder einer kontrollierten Selbstregulierung (Dammann/Simitis 1997, Einl. Anm. 11, Art. 27 Anm. 1; Kuitenbrouwer 1997, S. 109), die bislang vorwiegend auf den Gebieten des Handels- und Kreditauskunfts wesens, des Direktmarketing und der Gesundheitsfürsorge bestehen.

Selbstregulierende Verhaltensregeln zum Datenschutz lassen sich zuerst für die Niederlande nachweisen (Kaspersen 2000, S. 117 f.; Simitis, BDSG, § 1 Rdn. 118). Die im Datenschutzgesetz aus dem Jahre 1988 enthaltenen Vorschriften über Verhaltensregeln werden im novellierten Gesetz fortgeschrieben. Es regelt auf der Grundlage der im Gesetz selbst festgelegten Prinzipien in Art. 25 die Ausarbeitung von Verarbeitungsbedingungen durch hinreichend repräsentative Organisationen bis hin zur feststellenden Entscheidung der Aufsichtsbehörde darüber, wie die letztlich allein verbindliche, im Amtsblatt zu publizierende Regelung auszusehen hat.

Das irische Datenschutzgesetz von 1988 – noch im April 2002 befand sich ein Novellierungsentwurf zur Umsetzung der Richtlinie 95/46/EG in der parlamentarischen Beratung – eröffnet in Sect. 13 interessierten Wirtschaftsverbänden sowie anderen Organisationen die Möglichkeit zur Erarbeitung von Codes of Practice. Im Falle der Genehmigung durch die Aufsichtsbehörde ist der Code of Practice dem Parlament zur abschließenden Entscheidung vorzulegen, woraufhin er rechtliche Bindungswirkung für alle Organisationen in dem betreffenden (Geschäfts-) Bereich entfaltet.

Dagegen weist der britische Data Protection Act aus dem Jahre 1998 dem Information Commissioner als Aufsichtsbehörde die Initiative zur Vorbe-

reitung von Codes of Practice zu. Nach Sect. 52 par. 3 i.V.m. Sect. 51 par. 3 sind Wirtschaftsverbände, Betroffene oder diese repräsentierende Organisationen im Rahmen eines Konsultationsverfahrens mit einzubeziehen und die Entwürfe beiden Häusern des Parlaments zur Verabschiedung vorzulegen.

Im Zuge der Umsetzung von Art. 27 der EG-Datenschutzrichtlinie gesellen sich zu den »klassischen« Ländern Niederlande, Irland und Vereinigtes Königreich weitere Mitgliedstaaten der Union. Ihnen steht ein beachtlicher Gestaltungsspielraum zur Verfügung, da Art. 27 bei der Förderung von Verhaltensregeln auf eine abschließende Verfahrensregelung verzichtet und sich stattdessen auf die Mitwirkung der zuständigen Stellen konzentriert. Die Mitgliedstaaten können festlegen, welche Organisationen oder Stellen überhaupt Verhaltensregeln erlassen dürfen oder müssen, welche Verfahrensgrundsätze dabei im einzelnen einzuhalten sind, ob und in welchen Verfahren selbstregulierenden Bestimmungen verbindlicher Charakter beigelegt werden kann, in welcher Weise sich die Betroffenen darauf beziehen können und welche Mechanismen zur Bearbeitung von Problemfällen bzw. zur Durchsetzung bestehen müssen (Dammann/Simitis, 1997 Art. 27 Anm. 3). Entsprechende Vorschriften über Verhaltensregelungen finden sich in den neuen Datenschutzgesetzen von Belgien (Art. 44 Abs. 2 und 3), Finnland (Sect. 42), Italien (Art. 31 Abs. 1 Buchst. h), Portugal (Art. 32), Schweden (Sect. 12) und Spanien (Art. 32).

6. Selbstregulierende Elemente im neuen Bundesdatenschutzgesetz 2001

Mit der Novellierung des BDSG (Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze vom 18.5.2001, BGBl. I S. 904) wird in Deutschland zunächst im Zusammenhang mit der Drittstaatenübermittlung gem. § 4c Abs. 2 Satz 1, 2.Hs. – neben Vertragsklauseln – verbindlichen Unternehmensregelungen die Möglichkeit einer Garantiefunktion eingeräumt, wenn im Land des Datenimporteurs ansonsten kein dem Adäquanzprinzip geschuldetes Datenschutzniveau gewährleistet ist. Das Gesetz stellt sich damit der häufig anzutreffenden Situation, dass Teilunternehmen von international operierenden Unternehmen in Ländern ohne angemessenem Datenschutzniveau angesiedelt sind und das Verhältnis der Teilunternehmen untereinander in der Regel nicht von Vertragsklauseln bestimmt wird. Als Reaktion hierauf gehen internationale Konzerne mehr und mehr dazu über, für alle Teilunternehmen unabhängig vom Standort verbindliche Verhaltenskodizes auf den Gebieten des Datenschutzes und der Datensicherheit zu erlassen (Gackenholtz 2000, S. 731 f.; Bizer 2001 a, S. 168). Ein derartiger Verhaltenskodex kann als Arbeitsanweisung oder als Verhaltensregel eigener Art konzipiert und umgesetzt werden. Dadurch können die Schutzwirkungen für betroffene Kunden oder Mitarbeiter gewährleistet werden (Heil in: Abel 2002, § 4c BDSG Anm. 2.1.6). Alfred Büllesbach (2000, S. 4 und 2001, S. 137 f.⁴) hat im Hinblick auf Privacy Codes of Conduct für einen global operierenden Konzern

die Diskussion angestoßen und ein interessantes und diskussionswürdiges Konzept vorgelegt.

Im Rahmen der Umsetzung von Art. 27 der EG-Datenschutzrichtlinie sollen nach § 38a BDSG Verhaltensregeln von Berufs- und Branchenverbänden als interne Regelungen zur ordnungsgemäßen Durchführung datenschutzrechtlicher Vorschriften beitragen. Derartige Verhaltensregeln böten einen Rahmen, in dem sich Verbände oder sonstige Repräsentanten von Datennutzern und Betroffenen über ihre jeweiligen Interessen verständigen und faire Verarbeitungsbedingungen aushandeln könnten. Hierfür kämen etwa die Bereiche des Direktmarketing oder der Versicherungen in Betracht (Walz 2000, S. 461). Den in § 38a Abs. 1 BDSG genannten Verbänden und Vereinigungen wird die Möglichkeit eingeräumt, von ihnen erarbeitete Verhaltensregeln der Aufsichtsbehörde zu unterbreiten. Gem. Abs. 2 der Vorschrift ist die Aufsichtsbehörde zur Überprüfung der vorgelegten Entwürfe anhand des geltenden Datenschutzrechts verpflichtet.

Die in der Literatur mit Zustimmung (Bull, 1998, S. 313) aufgenommene Regelung des § 38a BDSG wird von der novellierten Gemeinsamen Geschäftsordnung der Bundesministerien (GGO) flankiert (Bundeskabinett 2000 S. 7 ff.). Deren § 43 Abs. 1 Nr. 3 legt i. V. m. dem in Anlage 7 enthaltene Prüfkatalog fest, dass bei der Erstellung von Gesetzentwürfen nunmehr auch die Gestaltungsmöglichkeiten selbstregulierender Normgebung im Rahmen der erforderlichen Abwägungen in Betracht zu ziehen sind.

7. Zukunftsweisende Konzeption regulierter Selbstregulierung

Das Thema Selbstregulierung wird die Reformdiskussion um den Datenschutz begleiten und wie diese selbst noch für geraume Zeit die Aufmerksamkeit auf sich ziehen. Folgerichtig widmet das im Auftrag des Bundesministeriums des Innern erstellte Gutachten »Modernisierung des Datenschutzrechts« für die zweite Reformphase des Datenschutzes (hierzu Gerhold/Heil 2001, S. 381 f.) der Selbstregulierung die entsprechende Aufmerksamkeit (Roßnagel/Pfitzmann/Garstka 2001, S. 153 ff.): Für eine erste Evaluierung aus Datenschutzsicht ergeben sich unter dem Eindruck außereuropäischer Beispiele, vor dem Hintergrund von Erfahrungen europäischer Nachbarn und mit Blick auf die Äußerungen des Gutachtens für die zweite Stufe der Datenschutzreform in Deutschland erste Postulate für selbstregulierende Normsetzungen.

Nach Klarheit verlangt einmal das begriffliche Gedankengebäude (so auch Bennett 2000 a, 1), in dem Verhaltensregeln, Codes of Conduct, Codes of Practice, Privacy Commitments, Privacy Standards, Privacy Codes etc. – bisweilen in kumulativer Aufzählung oder auch als Synonym für das jeweils andere – verwendet werden (Bizer 2001 a, S. 168). Neben der definitorischen Aufgabe⁵ und der prioritären Auseinandersetzung mit inhaltlichen Fragen liegen die wesentlichen Herausforderungen in der Zuweisung ihres Stellenwertes im

Normengefüge und in der rechtlichen Absicherung der Verhaltensregeln.

Angesichts der Realitäten der Informationsgesellschaft ist es wünschwert und letztlich unumgänglich, nach neuen Konzepten des Datenschutzes Ausschau zu halten. Allerdings muss Konsens darüber herrschen, dass selbstregulierende Elemente keine Alternative zur gesetzlichen Absicherung der Grundkomponenten des Datenschutzes sein können (Simitis 1999, S. 212; Schwartz 2000, 347 und 1999, S. 1696). Bei der Arbeitsteilung zwischen gesellschaftlichem Schutz und staatlicher Intervention (Gusy 2000, S. 58) muss ein staatlich mitverantworteter Rahmen private Selbstregulierung begleiten. Dies ist mit dem Konzept der »regulierten Selbstregulierung« am treffendsten beschrieben (Hoffmann-Riem 1998, S. 537; Roßnagel/Pfitzmann/Garstka 2001, S. 158 f.)⁶ Entscheidend für die Wirksamkeit einer Selbstregulierung sind das materielle Niveau ihrer Regeln, die Wirksamkeit ihrer Kontrolle und ihre Transparenz (Bizer, DuD 2001 b, 277). Letztlich wird Selbstregulierung nur dann glaubwürdig und von Erfolg gekrönt sein, wenn Verstößen durch ein präventiv wirkendes Haftungsrecht begegnet wird (Bizer, DuD 2001 b, 277). Auch in bezug auf den Datenschutz ist es möglich, dass der Staat einige der ihm historisch zugewachsenen Aufgaben der gesellschaftlichen Selbstregulierung überlässt (Roßnagel 1997, S. 30; Jacob 2000, S. 24). Von zentraler Bedeutung ist dabei jedoch, dass er sich die Vorgabe der Spielregeln und die Kontrolle ihrer Einhaltung vorbehält.

Zusammenfassung

Resümierend lassen sich fünf Thesen ableiten⁷:

1. Die Rechtswirklichkeit der Informationsgesellschaft erfordert eine Öffnung des Datenschutzes für neue Denkansätze und Konzeptionen.
2. Der Staat kann im Datenschutzrecht einen Teilbereich seiner Aufgaben der gesellschaftlichen Selbstregulierung überlassen.
3. Selbstregulierende Elemente können keine Alternative zur gesetzlichen Absicherung der Grundkomponenten des Datenschutzes sein.
4. Bei der datenschutzrechtlichen Selbstregulierung muss sich der Staat die Vorgabe der Spielregeln und die Kontrolle ihrer Einhaltung vorbehalten.
5. Die hierfür am besten geeignete Methode verkörpert das Prinzip der regulierten Selbstregulierung.

¹ Davon zu unterscheiden ist die Selbstregulierung i.S.d. Förderung von Verhaltensregeln gem. Kap. V (Art. 27) der Richtlinie, denen im Gemeinschaftsgebiet lediglich eine unterstützende Funktion eingeräumt wird, s. dazu unten 4.

² Mit einer Zusammenstellung wichtiger US-amerikanischer Verbände und ihrer Codes of Conduct, Codes of Ethics, Guidelines etc.

³ Zur Selbstregulierung durch Privacy Statements u.a.m. sowie zu den in den USA pro und contra vorgebrachten Argumenten zur Selbstregulierung mit zahlr. Nachw. auf S. 451 f.;

⁴ Zum Inhalt von Privacy Codes of Conduct für einen global operierenden Konzern.

⁵ Erste Definitionen finden sich bei Dammann/Simitis 1997, Art. 27 Anm. 1 und Bing 2000, 76.

- ⁶ Damann/Simitis 1997, Einleitung, Anm. 11 und Kaspersen 2000, 122 sprechen von »kontrollierter Selbstregulierung« bzw. »controlled self-regulation«; Lutterbeck 2000, 103, plädiert für ein »mixed system out of self-regulation and regulation by statutes.«
- ⁷ Hierzu und zum Vorstehenden Heil 2001, S.129 ff.; insbes. S. 133 f.; zusammenfassend Gerhold/Heil 2001, S. 382.

Literatur

- Abel, H. (1993): Praxishandbuch Datenschutz, Augsburg 1993 ff.
- Bennett (2000): Privacy Self-Regulation in a Global Economy: A Race to the Top, the Bottom or Somewhere Else?, Paper Prepared for Plenary Session III of the International Conference of Privacy and Data Protection Commissioners, Venice, September 28 – 30, 2000.
- Bing, J. (2000): Regulation and Self-Regulation in Data Networks: The Role or Rule of Law in the Information Society, in: Wiebe (2000), S. 75 ff.
- Bizer, J. (2001 a): Selbstregulierung des Datenschutzes, DuD 25 (2001), 168.
- Bizer, J. (2001 b): Ziele und Elemente der Modernisierung des Datenschutzrechts, DuD 25 (2001), 274 ff.
- Brühann, U. (1999): Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, in: Grabitz/Hilf, Kommentar zur Europäischen Union, Teil II: Sekundärrecht, EG-Verbraucher- und Datenschutzrecht (Hrsg. Wolf), A 30, München 1999.
- Büllesbach, A. (2000): Datenschutz in einem globalen Unternehmen, RDV 2000, 1 ff.
- Büllesbach A. (1999): Datenverkehr ohne Datenschutz? – Eine globale Herausforderung, Köln 1999.
- Büllesbach A. (Hrsg.) (1999 a): Innovation und technikgestaltender Datenschutz – gesellschaftliche und wirtschaftliche Anforderungen, in: Büllesbach (1999), S. 1 ff.
- Büllesbach, A. / Höss-Löw, P. (2001): Vertragslösung, Safe Harbor oder Privacy Code of Conduct, DuD 25 (2001) 135 ff.
- Bull, H.-P. (1998): Neue Konzepte, neue Instrumente? – Zur Datenschutzdiskussion des Bremer Juristentages, ZRP 1998, 310 ff.
- Bundeskabinett (2000): Beschluss des Bundeskabinetts vom 26. Juli 2000, in: Bundesministerium des Innern (Hrsg.), Moderner Staat – Moderne Verwaltung, Berlin 2000.
- Dammann, U. (2000): Safe Harbor – neue Elemente im internationalen Datenschutz, in: Simon/Weiss (Hrsg.) (2000), S. 19 ff.
- Dammann, U./Simitis, S. (1997): EG-Datenschutzrichtlinie, Kommentar, Baden-Baden 1997.
- Ehmann, E./Helfrich, M. (1999): Die EG-Datenschutzrichtlinie, Kurzkomentar, Köln 1999.
- EPIC/PI (1999): Electronic Privacy Information Center (EPIC) / Privacy International (PI), Privacy and Human Rights 1999 – An International Survey of Privacy Laws and Developments, Washington/D.C., USA, 1999
- Gackenholtz (2000): Datenübermittlung ins Ausland unter besonderer

- Berücksichtigung internationaler Konzerne, DuD 24 (2000), S. 727 ff.
- Gerhold, D. / Heil, H. (2001): Das neue Bundesdatenschutzgesetz 2001, DuD 25 (2001), S. 377 ff.
- Grimm, R. / Rossnagel, A. (2000): Datenschutz für das Internet in den USA, DuD 24 (2000), S. 446 ff.
- Gusy, Chr. (2000): Informationelle Selbstbestimmung und Datenschutz: Fortführung oder Neuanfang? , KritV 83 (2000), S. 52 ff.
- Heil, H. (1999 a): Die Artikel 29-Datenschutzgruppe, DuD 23 (1999), S. 471 ff.
- Heil, H. (1999 b): Europäische Herausforderung – Transatlantische Debatte/ Zur Datenschutzdiskussion zwischen der EU und den USA, DuD 23 (1999), S. 458 ff.
- Heil, H. (2000): Safe Harbor: Ein Zwischenstandsbericht, DuD 24 (2000), S. 444 f.
- Heil, H. (2001): Datenschutz durch Selbstregulierung – Der europäische Ansatz, DuD 25 (2001), S. 129 ff.
- Hoffmann – Riem, W. (1998): Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes, AöR 123 (1998), S. 513 ff.
- Jacob, J. (2000): Datenschutz in Netzen: Es gibt keinen Grund zur Resignation! – Perspektiven zwischen Regulierung und Selbstregulierung, in: Wiebe (2000), S. 17 ff.
- Kaspersen, H. (2000): Self-regulation and the Internet, in: Wiebe (2000), S. 117 ff.
- Kranz, H.-L. (1998), Datenschutz im internationalen Luftverkehr, DuD 22 (1998), S. 215 ff.
- Kranz, H.-L. (2001): Kundendatenschutz und Selbstregulierung im Luftverkehr, DuD 25 (2001), S. 161 ff.
- Kuitenbrouwer (1997): Self-Regulation: Some Dutch Experiences, in: U.S. Department of Commerce (Ed.), Privacy and Self-Regulation in the Information Age, Washington/D.C., USA, 1997, S. 109 ff.
- Lutterbeck, B. (2000): Regulation and Self-Regulation in Open Networks – Four Theses on Internet Governance, in: Wiebe (2000), S. 103 ff.
- Privacy Commissioner Hong Kong (2000): Office of the Privacy Commissioner for Personal Data, Annual Report 1999 – 2000, Hong Kong 2000.
- Privacy Commissioner Hong Kong (2002): Office of the Privacy Commissioner for Personal Data, Draft Code of Practice on Monitoring and Personal Data Privacy at Work, Consultation Document, Deadline for Submission of Comments 7 June 2002, Hong Kong 2002.
- Reidenberg, J. R. (2001): E-Commerce And Trans-Atlantic Privacy, Houston L.R. 44 (2001), S. 713 ff.
- Roßnagel, A. (1997): Globale Datennetze: Ohnmacht des Staates – Selbstschutz der Bürger, ZRP 1997, S. 26 ff.
- Roßnagel, A./Pfitzmann, A./Garstka, H. (2001): Modernisierung des Datenschutzrechts, Gutachten im Auftrag des Bundesministeriums des Innern, Berlin 2001.

- Roßnagel, A./Scholz, P. (2000): Datenschutz in Japan, DuD 24 (2000), S. 454 ff.
- Schwartz, P. (1999): Privacy and Democracy in Cyberspace, Vanderbilt L.R. 52 (1999), S. 1609 ff.
- Schwartz, P. (2000): Privacy, Participation, and Cyberspace: An American Perspective, in: Simon/Weiss (Hrsg.) (2000), S. 337 ff.
- Schwartz, P./Reidenberg, J. R: (1996): Data Privacy Law, Charlottesville/Virginia, USA, 1996.
- Simitis, S.: Der Transfer von Daten in Drittländer – ein Streit ohne Ende? in: Büllsbach (1999), S. 177 ff.
- Simitis, S. / Dammann, U. / Geiger, H. / Mallmann, O. / Walz, S.: Kommentar zum Bundesdatenschutzgesetz, 4. Aufl., Baden-Baden 1992 ff.
- Simon, D. / Weiss, M. (Hrsg.) (2000): Zur Autonomie des Individuums – Liber Amicorum Spiros Simitis, Baden-Baden 2000.
- Tauss, J. / Özdemir, C. (2000): Umfassende Modernisierung des Datenschutzes in zwei Stufen, RDV 2000, S. 143 ff.
- Walz, S. (2000): Selbstkontrolle versus Fremdkontrolle – Konzeptwechsel im deutschen Datenschutzrecht? in: Simon/Weiss (Hrsg.) (2000), S. 455 ff.
- Wiebe, A. (2000): Regulierung in Datennetzen, Darmstadt 2000.
- Wuermeling, U. (2000): Handelshemmnis Datenschutz – Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Köln etc. 2000.