Alexander Roßnagel

Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive

1. Der Wert der Daten und des Datenschutzes

Auf dem Weg in die Informationsgesellschaft gewinnen Informationen immer mehr an Wert. Dies gilt auch und erst recht für personenbezogene Daten. Für sie werden – je nach Sensitivität der Daten – beachtliche Summen geboten (s. zum wirtschaftlichen Wert personenbezogener Daten z. B. Brönneke/Bobrowski 2000; Weichert 2000; ders., DuD 2001, 264 ff.; ders., NJW 2001, 1463 ff.). Sie sind die Grundlagen für moderne – personalisierte – Methoden des Marketing und der Kundenbindung, ohne die viele Unternehmen meinen, nicht mehr existieren zu können. Personenbezogene Daten zu Kaufkraft, Kaufgewohnheiten und Kreditwürdigkeit werden zu aussagekräftigen Profilen gebündelt. Anhand von Bewertungsmodellen wird auf der Grundlage dieser Daten darüber entschieden, welcher Nutzen von dem Kunden für das Unternehmen noch zu erwarten ist und auf dieser Grundlage über Kontoführung, Kredite, Energieversorgung, Telekommunikation, Versicherungen und ähnliche Dienstleistungen sowie ihre Preise entschieden. Die Nachfrage nach personenbezogenen Daten nimmt ständig zu. Und umgekehrt wird diese Nachfrage immer öfter die Grundlage von Geschäftsmodellen, die solche Daten verkaufen oder vermieten.

Zugleich werden auf dem Weg zur Informationsgesellschaft immer mehr Unternehmen in ihrem Erfolg abhängig vom Vertrauen ihrer Kunden. Dies gilt nicht nur für die Unternehmen, die – wie etwa Banken – schon immer sensitive Dienstleistungen verkauft haben. Dies gilt zunehmend auch für reine Produktverkäufer, weil sie nicht mehr nur Produkte verkaufen, sondern um die Produkte herum auch vielfältige Dienstleistungen. Diese Vertrauensabhängigkeit verschärft sich noch für die Internetwirtschaft, weil in ihr keine persönlichen Beziehungen geknüpft und damit keine Vertrauensanker durch unmittelbare Kommunikation geschaffen werden können (Fuhrmann 2001). Vertrauen entwickelt sich immer mehr zu einem entscheidenden Faktor für wirtschaftlichen Erfolg und nachvollziehbare Maßnahmen zum Datenschutz werden zu einem wichtigen Vertrauensfaktor.

Datenschutz ist daher auch ein Wirtschaftsfaktor (ausführlich Büllesbach, RDV 1997, 239 ff.). Auch wenn es sich nicht unmittelbar auf Umsatz und Gewinn umrechnen lässt, ist es etwa für Versicherungen nicht ohne Folgen, dass sie hinsichtlich eines korrekten Umgangs mit personenbezogenen Daten nur das Vertrauen von 30% der Bundesbürger genießen und damit zum Beispiel deutlich hinter dem Verfassungsschutz (41%) rangieren. Was auf den ersten Blick nur als Imagefrage erscheint, kann sich in Zukunft zur Existenzfrage ausweiten. Wenn Versicherungen nicht zugetraut wird, Datenschutz auf Dauer zu garantieren, werden sich die Verbraucher nach anderen Sicherheiten umsehen oder umorientieren. Wer mit anvertrauten Daten nicht sorgsam um-

gehen kann, wird in der Informationsgesellschaft des 21. Jahrhunderts einen schweren Stand haben (s. zum Verhältnis von Datenschutz und Vertrauen die empirischen Ergebnisse in Opaschowski 2002).

Wenn die Verarbeitung personenbezogener Daten und die Gewährleistung informationeller Selbstbestimmung zu einem Wettbewerbsfaktor in der modernen Wirtschaft geworden sind, liegt es nahe, diese Entwicklung für den Datenschutz zu nutzen und den Wettbewerb für den Datenschutz fruchtbar zu machen (s. hierzu auch die Vorschläge in den Gutachten im Auftrag des Bundesinnenministeriums Roßnagel/Pfitzmann/Garstka 2001, 42, 45, 132 ff.; s. auch Weichert, DuD 2001, 265 ff.; ders., NJW 2001, 1465).

2. Neue Ziele des Datenschutzes

Aber nicht nur die Bedeutung der Daten und des Datenschutzes für den Wettbewerb legt diesen Schluss nahe, sondern auch die Struktur der neuen Ziele des Datenschutzes. Neue Herausforderungen – wie die Globalisierung der Datenverarbeitung und die dynamische Entwicklung der Technik – fordern angemessene instrumentelle Zielsetzungen. Gegenüber diesen Herausforderungen muss Datenschutz durch Technik erreicht werden.[1] Datenschutz hat nur dann eine Chance, wenn die Entwicklung von Verfahren und die Gestaltung von Hard- und Software am Ziel des Datenschutzes ausgerichtet und Datenschutz so weit wie möglich in Produkte, Dienste und Verfahren integriert wird (Roßnagel, DuD 1999, 253 ff.). Durch Technik müssen alle normativen Ziele unterstützt werden – nicht nur die Abschottung und Kontrollfähigkeit der Datenverarbeitung, sondern auch die Prinzipien der Transparenz, der Vermeidung des Personenbezugs, der Erforderlichkeit, der Zweckbegrenzung und Zweckbindung, der Verantwortlichkeit und der Selbstbestimmung sowie die Wahrnehmung von Betroffenenrechten. Durch die Realisierung von Systemdatenschutz (ausführlich z. B. Büllesbach/Garstka 1997; Dix 2002) soll sichergestellt werden, dass die Datenverarbeitungsverfahren diese Ziele einhalten und einen Verstoß gegen sie möglichst gar nicht zulassen. Techniken des Selbstdatenschutzes sollen den Einzelnen in die Lage versetzen, seine informationelle Selbstbestimmung selbst zu schützen und durchzusetzen. Verantwortliche Stellen sollen das Ziel der Datensparsamkeit vor allem dadurch umsetzen, dass sie die Möglichkeit anonymen und pseudonymen Handelns anbieten und dadurch den Personenbezug der zu verarbeitenden Daten vermeiden (ausführlich Roßnagel 2002b; zu Regelungsvorschlägen s. Roßnagel/Pfitzmann/Garstka 2001, 103 ff., 150 ff.).

Diese neuen Ziele lassen sich aber kaum durch administrativen Datenschutz, durch Ge- und Verbote, erreichen. Staatlicher Zwang mobilisiert Widerstand und die Suche nach Umgehungsmöglichkeiten. Die genannten neuen Ziele sind aber letztlich nur umzusetzen, wenn die verantwortlichen Stellen ein eigenes Interesse daran haben. Ihr Wissen und ihr Engagement ist hierfür unverzichtbar. Daher muss ein modernes Datenschutzrecht Rahmenbedin-

gungen schaffen, die Anreize bieten und Eigeninteresse mobilisieren, diese Ziele zu realisieren. Ergänzend zu bestehenden Datenschutzregelungen muss es versuchen, Verbesserungen des Datenschutzes und der Datensicherheit ohne Zwang durch die Kräfte des Wettbewerbs zu erzielen. Es gilt, legitimen Eigennutz zur Verwirklichung von Gemeinwohlzielen zu nutzen (Roßnagel 2002c; Weichert, NJW 2001, 1465).

Dabei kann es angesichts einer akzelerierend fortentwickelten Technik, immer neuen Geschäftsmodellen in der Verwertung personenbezogener Daten, kaum vorhersagbaren Anwendungsfeldern der netzgestützten und der ubiquitären Datenverarbeitung nicht darum gehen, isolierte Antworten auf einzelne Sachprobleme zu finden. Benötigt werden vielmehr Strukturlösungen. Erforderlich ist, in den verantwortlichen Stellen lernfähige Systeme zu etablieren, die auf ständig sich ändernde Herausforderungen immer wieder neue Antworten zu geben vermögen. Das Datenschutzrecht muss für die verantwortlichen Stellen Anreize bieten, Problembewusstsein auszubilden, Risiko- und Lösungswissen zu generieren und immer wieder Lernprozesse zur Verbesserung von Datenschutz und Datensicherheit zu initiieren.

3. Keine Eigentumsrechte an Daten

Wenn nun überlegt wird, wie ein Wettbewerb um Datenschutz zu konzipieren ist, liegt es nahe, den betroffenen Personen ein Eigentum an »ihren« Daten zuzubilligen und Wettbewerb dadurch zu initiieren, dass die betroffenen Personen »ihre« Daten an Nachfrager »verkaufen« können. Ein solcher »Property Rights-Ansatz« wird für den Datenschutz tatsächlich propagiert (bspw. Ladeur, DuD 2000, 18; zu diesem zwar kritisch, aber dennoch Datenüberlassungsverträge propagierend Weichert, DuD 2001, 268; ders., NJW 2001, 1467).

Eine solche Konzeption verkennt jedoch zutiefst die Grundstruktur personenbezogener Daten und der informationellen Selbstbestimmung. Sie taugt nicht für eine gesellschaftliche Ordnung im Umgang mit personenbezogenen Daten, die den Freiheitsrechten aller Beteiligten gerecht wird. Informationelle Selbstbestimmung kann nicht so verstanden werden, dass sie eine Herrschaft der betroffenen Person über »ihre« personenbezogenen Daten gewährleistet und ihr eine eigentumsähnliche Ausschluss- und Verfügungsmacht sichert. Ein solches Verständnis würde zum einen den objektivrechtlichen Gehalt der informationellen Selbstbestimmung als Funktionsvoraussetzung für eine Gesellschaft verkennen, die auf individueller Selbstbestimmung und freier demokratischer Willensbildung ruht[2]. Sie würde zum anderen aber auch verkennen, dass personenbezogene Daten mehrrelational sind. Als Modelle der Wirklichkeit haben sie immer einen Autor und ein Objekt. Sie haben eine Beziehung zum Objekt, aber auch zum Autor. Sie können nicht allein dem Objekt zugeordnet werden.[3] Für ein mehrrelationales Wirklichkeitsmodell ist grundsätzlich keine Eigentumsäquivalenz gegeben. Datenschutzrecht regelt daher keine Eigentumsordnung, sondern eine Informations- und Kommu-

nikationsordnung, die bestimmt, wer in welcher Relation befugt ist, mit den Modellen über bestimmte Personen in einer bestimmten Weise umzugehen (s. hierzu auch Trute 2002, Rn. 19; Simitis 1987, 1475, 1489, insb. 1492; Hoffmann-Riem 1997, 779; ders. 1998, 11; ders., AöR 1998, 520; Trute, VVDStRL 57 (1998), 260; Pitschas, DuD 1998, 146 ff.; Schulz, Verwaltung 1999, 150). Datenschutz schützt daher nicht die betroffene Person als »Dateneigentümer«, sondern unterstützt sie als aktiven Interessen- und Entscheidungsträger im Rahmen dieser Informations- und Kommunikationsordnung.

Informationelle Selbstbestimmung ist daher nicht in der Weise zu gewährleisten, dass ausschließlich die betroffene Person selbst über »ihre« Daten verfügt und sie demjenigen »verkauft«, der ihr den höchsten oder einen ihr ausreichenden Preis bietet. Die personenbezogenen Daten sind nicht nur Daten der betroffenen Person, sondern ebenso der Stelle, die die Daten erhoben oder verarbeitet hat. So sind Daten über eine medizinische Behandlung zugleich auch Daten über die Leistung des Arztes, die dieser benötigt, um seinen Leistungsanspruch zu begründen und abzurechnen, um seine ärztliche Dokumentationspflicht zu erfüllen und im Streitfall eine ordnungsgemäße Behandlung nachweisen zu können. Eine ausschließliche Verfügungsbefugnis als Grundlage für eine Konzeption des Datenschutzes als Eigentumsordnung kann es daher nicht geben (Roßnagel/Pfitzmann/Garstka 2001, 37 f.).

4. Marktwirtschaft und Privatautonomie

Vielmehr ist die Grundvoraussetzung, um marktwirtschaftlichen Wettbewerb im Datenschutz zu realisieren, dessen Grundprinzip, die Privatautonomie, auch im Datenschutzrecht konsequent umzusetzen. In diesem Sinn muss die informationelle Selbstbestimmung nicht nur im Verfassungsrecht, sondern auch im einfachen Datenschutzrecht als die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (BVerfGE 65,1), zur Grundregel werden: Die Entscheidungsprärogative der betroffenen Person wird am besten gewahrt, wenn die Einwilligung zum vorrangigen Legitimationsgrund der Datenverarbeitung wird (Roßnagel/Pfitzmann/Garstka 2001, 72 ff.).

Im nichtöffentlichen Bereich[4] müssen daher die Erlaubnistatbestände zur zwangsweisen Datenverarbeitung durch das »Opt-in-Prinzip«[5] ersetzt werden. Hier kann grundsätzlich nur der freie Wille der betroffenen Person die Grundlage für die Verarbeitung personenbezogener Daten sein. Dies gilt auch für die Änderung des Verarbeitungszwecks oder die Übermittlung von Daten und damit insbesondere für die Zwecke der Markt- und Meinungsforschung, der Werbung und des Marketing (s. z.B. bereits § 89 Abs. 7 Satz 1 TKG; § 14 Abs. 2 MDStV), den Handel mit Adressen oder das Veröffentlichen von Verzeichnissen. In einer Marktwirtschaft vermag allein das unternehmerische Interesse einer Partei nicht zu rechtfertigen, die Entscheidungsprärogative der anderen Partei zu übergehen oder gar zu missachten.

Die Anerkennung der Entscheidungsbefugnis des betroffenen Vertragspartners führt auf das Grundmodell des Vertragsrechts zurück: Die Rechte einer Partei gegenüber der anderen können nicht über das hinausgehen, was diese ihr konkret zugestanden hat (zum Zusammenhang mit dem Recht der Willenserklärungen Weichert, DuD 2001, 264 ff.; Bizer, DuD 2001, 276 f., ders. DuD 1998, 552). Es bleibt den verantwortlichen Stellen – ganz im Sinn der Marktwirtschaft – überlassen, für ihr Anliegen – unter Darlegung ihrer Datenschutzmaßnahmen – zu werben und die betroffene Person zu gewinnen, ihnen die Verarbeitung ihrer Daten zu erlauben oder gar mit ihnen vertraglich zu vereinbaren (so sind wohl die Datenüberlassungsverträge im Sinn von Weichert, DuD 2001, 268; ders., NJW 2001, 1467 zu verstehen). In der Wirtschaft gelten in vielen Bereichen Opt-in-Lösungen bereits als »professionell«. So heißt es zum Beispiel für die Gewinnung von Daten jenseits von vertraglich erforderlichen Daten etwa für Werbung und Marketing: »Kunden- und wettbewerbsorientiert handelnde Datenschutzverantwortliche werden generell auf die Anwendung transparenter Opt-in-Prozeduren hinwirken« (Kranz 2002, Rn. 10).

Die durch das »Opt-in-Prinzip« geforderte Datenschutzkommunikation zwischen verantwortlichen Stellen und betroffenen Personen ist eine Chance der Vertrauenswerbung. Datenschutz wird zu einem immer wichtigeren Qualitätsmerkmal für Vertrauensbeziehungen. Erst ein wirksamer – und kommunizierter – Datenschutz ermöglicht es, die hoffnungsvollen Prognosen des E-Commerce zu erreichen und – nebenbei bemerkt – ebenso eine Verwal-tungsmodernisierung unter Mitwirkung der Bürger durchzuführen. Wird der Kunde um seine Einwilligung zur Datenverarbeitung gebeten und wird ihm erläutert, wofür er diese Einwilligung geben kann, wird dies die Vertrauensbeziehung zwischen verantwortlicher Stelle und betroffener Person erheblich stärken.

»Opt-in« kann in zwei Formen erfolgen, die den sonstigen Handlungsformen der Marktwirtschaft entsprechen. Einmal kann die betroffene Person ihre Einwilligung ausdrücklich erklären. Allerdings ist zu beachten, dass zwischen der verantwortlichen Stelle und der betroffenen Person oft ein erhebliches faktisches Machtgefälle besteht, durch das die Einwilligung zum Einfallstor »diktierter« Verarbeitungsbedingungen werden kann. Daher kommt es darauf an, die Freiwilligkeit durch gesetzliche Rahmenregelungen abzusichern, vor Übereilung zu schützen und eine prüffähige Rechtsgrundlage zu gewährleisten (s. zu den hierfür notwendigen Maßnahmen Roßnagel/Pfitzmann/Garstka 2001, 92 ff.). Insbesondere wird es wichtig sein, für Formulareinwilligungen verbindlich echte Wahlmöglichkeiten des Einwilligenden einzufordern. Zum anderen erfolgt »Opt-in« durch den Abschluss eines Vertrags oder das Eingehen eines vertragsähnlichen Vertrauensverhältnisses. In diesem Fall wird durch das von der betroffenen Person freiwillig gesuchte Verhältnis diejenige Datenverarbeitung legitimiert, die zur Erfüllung des Verhältnisses erforderlich ist.

Eine zwangsweise Datenverarbeitung gegen den Willen der betroffenen Person sollte im nichtöffentlichen Bereich nur noch dort möglich sein, wo das »Opt-in-Prinzip« nicht funktionieren kann, wo es also der verantwortlichen

Stelle nicht möglich ist, für ihre Verarbeitung der personenbezogenen Daten zu werben, zu überzeugen und die Einwilligung der betroffenen Person zu erreichen. Zur Umschreibung dieser Ausnahmefälle ist jedoch der bisher die Datenverarbeitung steuernde Begriff des »berechtigten Interesses« zu weit. Er macht marktwirtschaftlichen Datenschutz unmöglich. Ausnahmen sollten vielmehr nur erlaubt sein, wenn dies zum Schutz oder zur Verfolgung eigener Rechte oder Rechte Dritter notwendig ist, oder wenn es erforderlich ist, um eine Gefahr für Leben, Gesundheit oder sonstige bedeutende Rechtsgüter der betroffenen Person zu beseitigen und die betroffene Person ihre Zustimmung nicht geben kann, oder wenn die Datenverarbeitung erforderlich ist, um Verpflichtungen zu erfüllen, die durch Rechtsvorschriften der verantwortlichen Stelle auferlegt wurden.[6]

Durch eine normative Aufwertung der Einwilligung wird auch ein erwünschter Nebeneffekt für die notwendige Vereinfachung des Datenschutzrechts bewirkt. Wird die Zulässigkeit der Datenverarbeitung grundsätzlich an die Einwilligung der betroffenen Person geknüpft, ist auch eine Entlastung des Datenschutzrechts und eine Einschränkung seiner Normenflut und Überdifferenzierung möglich. Der Gesetzgeber muss dann nicht mehr für alle Fälle die Konfliktlösung selbst festlegen, sondern kann sie vielfach der autonomen Konfliktlösung der Parteien überlassen.

5. Markttransparenz

Sowohl informationelle Selbstbestimmung als auch Wettbewerb erfordern Transparenz. Eine informierte Einwilligung setzt eine ausreichende Unterrichtung über die Bedingungen der Datenverarbeitung voraus. Damit die betroffene Person wissen kann, »wer was wann und bei welcher Gelegenheit über sie weiß« (BVerfGE 65, 1 (43), sollten personenbezogene Daten grundsätzlich bei ihr erhoben werden. Ist dies nicht möglich, muss sie sobald wie möglich unterrichtet werden (Roßnagel/Pfitzmann/Garstka 2001, 82 ff.).

Ein besonders wirksames Mittel des Wettbewerbs sind allgemein zugängliche Datenschutzerklärungen der verantwortlichen Stellen. Sie sind als »Privacy Statements« zumindest für den Online-Bereich internationaler Standard. In diesen können die verantwortlichen Stellen ihre Datenverarbeitungs- und Datenschutzpraxis darstellen[7] und vor allem über die Struktur und Zwecksetzung ihrer Datenverarbeitung unterrichten. In individuellen Unterrichtungen können sie auf diese verweisen. Interessierte Kunden können mit ihrer Hilfe die Bedingungen der Datenverarbeitung vergleichen (Weichert, DuD 2001, 268 f.).

Wer ein Buch kaufen will, will nicht zuvor drei eng beschriebene Seiten in ziselierter Juristensprache lesen. Noch weniger wird er dazu bereit sein, wenn er nur eine Webseite besuchen will. Von den Möglichkeiten, sich über Datenverarbeitungsgrundsätze und praktizierten Datenschutz zu informieren, wird daher selten Gebrauch gemacht. Dennoch ist es wichtig, die Möglichkeit hier-

zu zu bieten. Allerdings führt die nicht wahrgenommene Information noch nicht zu Wettbewerb. Um diesen anzuregen, ist eine Automatisierung der Transparenz notwendig. Für den Nutzer wäre es sehr hilfreich, wenn die Informationen über die Datenverarbeitung im Hintergrund verarbeitet würden, ohne dass er ihnen im Regelfall besondere Aufmerksamkeit schenken muss.

Dies ist möglich. Wird die Datenschutzerklärung auf der Website veröffentlicht, kann für die Datenschutzkommunikation zwischen datenverarbeitender Stelle und betroffener Person der weltweite Datenschutzstandard »Plattform for Privacy Preferences (P3P)«[8] des World Wide Web Consortiums genutzt werden. Publiziert die verantwortliche Stelle eine Datenschutzerklärung im WWW, die dem P3P-Standard entspricht, kann der Nutzer seine Datenschutzpräferenzen im Hintergrund automatisiert mit der veröffentlichten Datenverarbeitungspraxis der verantwortlichen Stelle abgleichen. Seine P3P-Software kann ihm dann »grünes Licht« signalisieren oder ihn vor unzumutbaren Bedingungen warnen. Er kann dann im Sinn der Grundregel des »Notice and Choice« entscheiden, ob er die Bedingungen akzeptiert oder die Verbindung zu der verantwortlichen Stelle abbricht (s. zur technischen Unterstützung von Transparenz näher Hansen 2002, Rn. 96). Eine Kommunikation über Datenschutzbedingungen ermöglicht die im April 2002 verabschiedete Fassung von P3P noch nicht. Als Mittel des Wettbewerbs würde P3P noch effektiver wirken, wenn es in den künftigen Versionen zu einem echten Kommunikationsstandard fortentwickelt würde (eine differenziertere Aushandlung bietet z.B. SSONET, Pfitzmann/Schill/ Westfeld/Wolf 2000). Im Idealfall sollte der P3P-Standard zum Beispiel Verhandlungen darüber ermöglichen, wie die personenbezogenen Daten verwendet werden, ob und in welchem Umfang überhaupt personenbezogene Daten nötig sind und welche Pseudonyme verwendet werden.

Transparenz kann auch die Grundlage für das marktwirtschaftliche Angebot von Datenschutzdienstleistungen sein. In USA beispielsweise bieten sich neu entstandene Unternehmen, Infomediaries (Begriff von Hagel/Singer 1999; s. auch Cranor 1999, 19 ff.), als Datentreuhänder an. Ihre Geschäftsidee beruht darauf, dass sie über die entsprechende Technologie und über Vertrauen beider Seiten verfügen, um einerseits personenbezogene Daten der Nutzer sicher verwalten zu helfen und andererseits Regeln des Datenaustauschs zwischen Nutzern und Web-Diensten durchzusetzen. Den Nutzern versprechen die Infomediaries Schutz vor unbemerkter und unfairer Datenweitergabe, Transparenz der Datenübermittlung und Kontrolle über ihre Daten. Sie analysieren Web-Angebote für Kunden auf ihre Datenschutzpolitik hin – dies kann mit P3P automatisiert erfolgen – und ordnen diese in Rating-Skalen ein.[9] Durch Bündelung von Nutzerinteressen können Infomediaries eine höhere Marktmacht entwickeln und dadurch bessere Bedingungen und Erlöse erzielen als vereinzelte Nutzer, um so mehr, wenn diese schlecht informiert und mangelhaft mit Technik ausgestattet sind. Den Web-Diensten versprechen Infomediaries mehr und korrekte Daten. Sie finanzieren ihre Aktivitäten, indem sie die Daten als

pseudonyme Nutzerprofile oder anonymisiert als statistisches Forschungsmaterial verkaufen. Zum Teil beteiligen sie die Nutzer sogar am Verkauf der Daten (für Deutschland z.B. www.cocus.de; hierzu Köhntopp/Pfitzmann 2000, 316 ff.).

Infomediaries unterstützen allerdings nicht nur den Datenschutz, sondern bergen für diesen auch erhebliche Risiken. So erzeugen sie wachsende Ströme personenbezogener Daten und kehren damit die Zielrichtung datensparsamer Technikentwicklung um. Die Vermittlung personenbezogener Daten bildet immerhin ihren Geschäftszweck. Außerdem bauen sie zentrale Großlager personenbezogener Daten auf, die durch Hacker, durch korrumpierte Insider, durch löchrige Geschäftspraktiken oder staatliche Beschlagnahme gefährdet sein können.

Rechtliche Transparenzanforderungen sind nicht in der Weise zu verstehen, dass der betroffenen Person künftig viele Prüfpflichten auferlegt werden, um ihre Rechte geltend zu machen. Auch für eine nachlässige und uninteressierte Person muss ein Mindestmaß an Datenschutz – vor allem durch Systemdatenschutz – gewährleistet sein. Auch muss sie sich auf eine gewisse Kontrolle durch Aufsichtsbehörden oder Verbände verlassen können. Allerdings setzen Mitwirkung und Selbstdatenschutz ein gewisses Mindestmaß an Kenntnis und Interesse hinsichtlich der Datenverarbeitung voraus. Die Transparenzanforderungen sollen diese ermöglichen. Dabei ist zu beachten, dass die Transparenzmaßnahmen Anknüpfungspunkte für technische Verfahren (P3P) oder Dienstleistungen (Infomediaries) sind, die – im Wettbewerb – für die betroffene Person Kontrollen durchführen und ihre Interessen durchsetzen.

6. Datenschutzaudit als Vertrauensanker

Der Markt benötigt verlässliche Informationen. Die Aussagen zu Datenschutzanstrengungen in Datenschutzerklärungen können in ihrer Werbewirkung verstärkt werden, wenn sie in nachprüfbarer Weise ausgezeichnet werden. Dies soll mit einem Datenschutzaudit ermöglicht werden. Es belohnt verantwortliche Stellen, die ihren Datenschutz verbessern, mit der abgesicherten Möglichkeit, im Wettbewerb um das Vertrauen Dritter ein Auditzeichen zu führen, das die von einem zugelassenen Datenschutzgutachter überprüften Datenschutzanstrengungen bestätigt (Roßnagel 2000; Roßnagel/Pfitzmann/Garstka 2001, 132 ff.; zum Behördenaudit s. Golembiewski 2002).

Diese Auszeichnung soll sowohl die »Anspruchsgruppen« – wie Kunden, Vertragspartner, Mitarbeiter, Banken, Versicherungen, Anteilseigner, Behörden, Presse, Parteien und die interessierte Öffentlichkeit – als auch die Konkurrenten beeindrucken. Sie soll als Diskriminierungsmerkmal am Markt dienen. Durch die Prämierung werden marktgerechte Anreize geschaffen, nachprüfbare Ergebnisse zur Verbesserung von Datenschutz und Datensicherheit zu präsentieren. Nehmen wichtige Akteure einer Branche am Datenschutzaudit teil, entsteht ein Wettbewerbsdruck für alle Konkurrenten, dies ebenfalls zu tun und ihren Datenschutz nachprüfbar zu verbessern.

Zielsetzung des Datenschutzaudits ist die freiwillige Überprüfung des Datenschutzmanagementsystems (s. zur Zusammenfassung bestehender Datenschutzpflichten zu einem Datenschutzmanagement näher Roßnagel/Pfitzmann/Garstka 2001, 130 ff.) hinsichtlich seiner Eignung, flexibel auf die rasanten Veränderungen der Informations- und Kommunikationstechniken zu reagieren und die sich dadurch immer wieder neu stellenden Herausforderungen für den Datenschutz zu meistern. Daher zielt das Datenschutzaudit nicht auf eine einmalige Evaluierung, sondern auf die Fähigkeit, immer wieder neue Lösungen zu generieren, und daher auf die kontinuierliche Verbesserung des Datenschutzmanagementsystems.

Die Prüfung verwendet zwei Maßstäbe: einen objektiven, für alle gleichen Maßstab, nämlich die Erfüllung der Anforderungen des Datenschutzrechts, und einen subjektiven, nämlich eine Verbesserung der Anstrengungen zum Datenschutz, die über den objektiven Maßstab hinausgeht und die sich nach den individuellen Möglichkeiten der verantwortlichen Stelle bestimmt. Von der selbstverständlichen Verpflichtung zur Einhaltung der geltenden Rechtsvorschriften abgesehen, bestimmen die verantwortlichen Stellen die inhaltlichen Anforderungen des Datenschutzaudits in Form von Selbstverpflichtungen selbst. Gefordert werden sollte nur, dass diese Anstrengungen auf eine kontinuierliche Verbesserung des Datenschutzes und der Datensicherheit gerichtet sein und den wirtschaftlich vertretbaren Einsatz der besten verfügbaren Technik vorsehen müssen. Mit diesen beiden subjektiven Kriterien soll die Zielgerechtigkeit der Selbstverpflichtungen gewährleistet und die Vergleichbarkeit der zusätzlichen Anstrengungen aller Teilnehmer ermöglicht werden. Welche Anforderungen sich daraus für die verantwortliche Stelle ergeben, bestimmt diese in eigener Verantwortung (näher Roßnagel 2000, 84 ff.). Es bietet sich an, Empfehlungen für Selbstverpflichtungen im Rahmen branchenbezogener Selbstregulierung zu erarbeiten (Arbeitskreises Datenschutzaudit Multimedia, DuD 1999, 285).

Das Datenschutzaudit sollte für die verantwortlichen Stellen mit möglichst wenig zusätzlichem Verwaltungsaufwand verbunden sein. Zugleich muss aber auch die erforderliche Zielgerechtigkeit des Verfahrens und der Kriterien, die notwendige Transparenz und Vergleichbarkeit der Prüfergebnisse sowie die Rechtssicherheit für die Werberegeln gewährleistet sein. Für die Wahl des geeigneten Verfahrens kommt es vor allem darauf an, welche verantwortlichen Stellen als Zielgruppe angesehen werden. Von ihnen muss erwartet werden, dass sie das Angebot eines Datenschutzaudits annehmen und mit ihrem Vorbild andere Stellen nachziehen. Wie auch beim Umweltschutzaudit ist diese Zielgruppe eher in den etablierten und größeren Unternehmen zu sehen als in Internet-Start-Up-Unternehmen. Sie haben sowohl das Interesse als auch die Kapazität, ein Audit durchzuführen. Außerdem haben sie die erforderliche wirtschaftliche Bedeutung, um für andere verantwortliche Stellen als Vorbild zu wirken. Da diese verantwortlichen Stellen in der Regel bereits an Qualitäts- und Umweltschutzaudits nach internationalen Normen[10] teilnehmen, wird die Einführung des Datenschutzaudits erleichtert und sein

Verwaltungsaufwand reduziert, wenn es an die in den Unternehmen bereits bestehenden Managementsysteme angepasst wird (Verfahrens- und Regelungsvorschlag bei Roßnagel/Pfitzmann/Garstka 2001, 135, 140 ff.).

Nimmt die verantwortliche Stelle erfolgreich am Datenschutzaudit teil, ist sie berechtigt, ein Datenschutzzeichen für Werbezwecke zu nutzen. Dieses Logo kann sie für die Kommunikation mit der Öffentlichkeit, insbesondere für Vertrauenswerbung nutzen. Ein gesetzlich geschütztes Zeichen für die überprüfte Selbstverpflichtung zur Einhaltung aller rechtlichen Datenschutzanforderungen und zu weitergehenden Anstrengungen zur kontinuierlichen Verbesserung des Datenschutzes und der Datensicherheit bietet tatsächlich eine Grundlage, dem Unternehmen Vertrauen entgegenzubringen.

Um die Verbreitung des Datenschutzaudits zu unterstützen, sollten verantwortliche Stellen, die an diesem teilnehmen, bevorzugt berücksichtigt werden, wenn es um Aufträge zur Verarbeitung personenbezogener Daten geht. Zumindest für öffentliche Stellen sollte diese Berücksichtigung zur Pflicht erhoben werden.[11] Als Erleichterungen für die Teilnehmer am Datenschutzaudit sollte vorgesehen werden, dass sie ihr Prüfergebnis an Stelle des Organisationsplans und des Datenschutz- und Datensicherheitskonzepts im Rahmen eines verbindlichen Datenschutzmanagements verwenden können.

7. Produktzertifizierung als Qualitätssiegel

Recht und Technik müssen zur Gewährleistung des Datenschutzes eine Allianz eingehen. Durch entsprechende rechtliche Rahmenbedingungen muss zu erreichen versucht werden, dass Datenschutz so weit wie möglich in Produkte, Dienste und Verfahren integriert wird (Roßnagel 2001). Datenschutz durch Technik ist oft die einzig mögliche Antwort auf Probleme der Globalisierung der Datenflüsse, der dynamischen Technikentwicklung und der Zunahme der Datenverarbeitung bis hin zu ihrer Allgegenwärtigkeit (s. zu den Datenschutzproblemen der Ubiquitons Computing Mattern/Langheinrich 2001). Je mehr der Datenschutz dem Einflussbereich des nationalen Gesetzgebers entschwindet, desto mehr muss Datenschutz weltweit wirksam werden. Dies ist mangels einer wirksamen Weltrechtsordnung nur dann möglich, wenn er in die Technik eingelassen ist. Dieser Weg bietet zwei Vorteile: Datenschutztechniken sind – im Gegensatz zu Datenschutzrecht – weltweit wirksam und Technikunternehmen sind – im Gegensatz zu Gesetzgebern – sehr schnell lernende Systeme. Beide Vorteile lassen sich nutzen, wenn es gelingt, für Datenschutztechnik einen Markt zu entwickeln. Wenn sich Datenschutztechnik verkauft, wird sie sich ebenso dynamisch entwickeln wie neue technische Herausforderungen für den Datenschutz (Roßnagel, DuD 1999, 253 ff.).

Für den Markt muss aber bekannt sein, welche Produkte datenschutzgerecht oder datenschutzförderlich sind. Damit deren spezifische Datenschutz- und Datensicherheitseigenschaften zu einem Wettbewerbsvorteil werden, sollte das künftige Datenschutzrecht eine Produkzzertifizierung anbieten

(zum Zusammenhang zwischen Produkttransparenz und Verbraucherschutz s. Weichert, DuD 2001, 268 f.). Deren »Gütesiegel« muss ein verlässliches Unterscheidungsmerkmal für die Marktnachfrage bieten.

Während das Datenschutzaudit das Datenschutzmanagement einer verantwortlichen Stelle in einem Systemaudit evaluiert, bezieht sich die Zertifizierung von Hard- und Software sowie von automatisierten Verfahren ausschließlich auf ein Produkt. Die Produktzertifizierung zielt daher nicht auf die wiederholte Überprüfung und Bewertung von Anstrengungen zur Verbesserung des Datenschutzes, sondern um die einmalige Bewertung der Datenschutz- und Datensicherheitseigenschaften einer bestimmten Version eines Produkts[12].

Datenschutzaudit und Produktzertifizierung sollten auch deshalb klar unterschieden werden, weil sie unterschiedliche Interessenten betreffen. Die Produktzertifizierung erfolgt auf Antrag des Herstellers oder Anbieters. Es macht wenig Sinn, wenn die vielen tausend Anwender eines Datenverarbeitungssystems oder -programms dieses viel tausendfach zertifizieren lassen.[13] Vielmehr sollte allein der jeweilige Hersteller oder Anbieter für das System oder Programm eine einzige Zertifizierung erhalten, auf die sich dann alle Anwender verlassen können. Die verantwortlichen Stellen sollten – soweit vorhanden – zertifizierte Datenverarbeitungssysteme und -programme in ihrer Datenverarbeitung einsetzen. Verwenden sie zertifizierte Produkte, sollte eine Vermutung bestehen, dass mit ihrer richtigen Verwendung die jeweils relevanten Anforderungen des Datenschutzes erfüllt sind.

Anforderungen an die Produkte sollten sich vor allem aus den Kriterien ergeben, die von den Herstellern bei der Prüfung für die Entwicklung und Herstellung zu beachten sein sollten (Roßnagel/Pfitzmann/Garstka 2001, 143 ff.). Diese sollten anwendungsspezifisch vom Hersteller zusammen mit dem Prüfer etwa in Form von »Protection Profiles« entsprechend den »Common Criteria« präzisiert werden. Soweit dies möglich ist, sollten Vertreter der Anwender und Nutzer an der Erstellung der »Profiles« beteiligt werden. Zumindest sollte ihnen Gelegenheit hierzu gegeben werden. Wird das Zertifikat zur Werbung für das Produkt verwendet, ist auf das »Profile« hinzuweisen. Es ist der Öffentlichkeit zugänglich zu machen, insbesondere dadurch, dass ein einfacher Zugriff im Rahmen elektronischer Medien ermöglicht wird.

Die Prüfung der Produkte sollte – wie beim Datenschutzaudit – von privaten Gutachtern durchgeführt werden, deren Zuverlässigkeit, Unabhängigkeit und Fachkunde durch Zulassung und Kontrolle gewährleistet sein muss. Die Zulassung der Gutachter könnte zum Beispiel nach § 36 GewO erfolgen oder wie in Schleswig-Holstein dem Landesdatenschutzbeauftragten übertragen werden.

Das Siegel sollte nicht vom Gutachter, sondern von einer dritten Stelle vergeben werden, die die Korrektheit des Gutachtens und der Arbeit des Gutachters überprüft. Hierfür kämen – wie dies in Schleswig-Holstein praktiziert wird – der Landesdatenschutzbeauftragte oder eine andere Stelle wie etwa die Industrie- und Handelskammern in Frage. Im zweiten Fall wäre dem Datenschutzbeauftragten Gelegenheit zu Einwendungen zu geben.

Anzustreben ist eine Produktzertifizierung, die nicht erst nach dem Markteintritt eines Produkts beginnt, sondern bereits entwicklungsbegleitend erfolgt. Schon die Entwicklungsabteilungen der Hersteller wären so gehalten, datenschutzfördernde Techniken in die Produktgestaltung aufzunehmen. Verbesserungen der Produkte, die erst nachträglich versuchen, Datenschutz zu integrieren, wären nicht mehr notwendig. Darüber hinaus könnten Hersteller von Beginn an mit dem Zertifikat werben.

Da das Datenschutzrecht auf die Verbreitung datenschutzgerechter Produkte angewiesen ist, muss es auch deren Absatz fördern. Daher sollte für verantwortliche Stellen des öffentlichen Bereichs die Verpflichtung vorgesehen werden, bei der Gestaltung von Prozessen zur Verarbeitung personenbezogener Daten vorrangig datenschutzfördernde Produkte zu verwenden (zur Zulässigkeit Petri, DuD 2001, 150). Hierdurch würde die Vorbildfunktion des Staats in der Weise angesprochen, dass er mit gutem Beispiel vorangehen sollte, wenn es darum geht, Belange des Datenschutzes bei der Beschaffung zu berücksichtigen. Die Verwendung datenschutzgerechter oder datenschutzfördernder Produkte durch staatliche Stellen kann bei Bürgern und Unternehmen einen Nachahmungseffekt bewirken, wenn sie sehen, dass es möglich und umsetzbar ist, datenschutzgerechte Produkte zu verwenden. Die gezielte Nachfrage durch die öffentliche Hand kann darüber hinaus den Bekanntheitsgrad und den Marktanteil datenschutzgerechter Produkte fördern und damit ihre Markteinführung und Diffusion ermöglichen oder beschleunigen.

8. Wettbewerb und Selbstregulierung

Für den Datenschutz wird Selbstregulierung eine steigende Bedeutung gewinnen (zu Modellen und Chancen der Selbstregulierung s. Roßnagel 2002 c). Selbstregulierung ermöglicht es der Wirtschaft, relativ schnell passgerechte branchen- oder unternehmensbezogene Regelungen zu entwickeln. Sie kann insbesondere eine globalisierte Datenverarbeitung vereinfachen, wenn ihre Regelungen weltweite Anwendung finden[14]. Selbstregulierung bietet die Chance, für die gefundenen normativen Vorgaben leichter die Akzeptanz bei den direkten Regelungsadressaten zu finden und erleichtert die Durchsetzung des Datenschutzrechts[15]. Ein weiterer Vorteil der Selbstregulierung kann die Mobilisierung von Sachverstand und die Gewinnung von Informationen sein, die nur von den Beteiligten selbst eingebracht und eingearbeitet werden können[16].

Trotz vieler Risiken (Roßnagel 2002b, Rn. 60 ff. mwN.) ist Selbstregulierung notwendig und unvermeidbar. Selbstgesetzte Verhaltensregeln begründen neue Rahmenbedingungen für den Wettbewerb, die sich zwiespältig auswirken können. Einerseits setzt Selbstregulierung oft voraus, dass alle oder mindestens die wichtigsten Angehörigen des betroffenen Markts diese anwenden[17]. In solchen Situationen sichern die Unternehmen das von allen Mitbewerbern gewünschte Verhalten durch gegenseitige Verpflichtungserklärungen

ab. Andererseits ermöglicht Selbstregulierung, die für Wirtschaft und den Wettbewerb passenden Regelungen zu finden. In der Regel beschreiben diese den kleinsten gemeinsamen Nenner, damit alle Mitglieder eines Verbands die Verhaltensregeln auch einhalten können. Auf deren Grundlage bleibt dann ein Wettbewerb um mehr Vertrauen durch Datenschutz ebenso möglich wie auf der Basis einer gesetzlichen Regelung. Horizontale Vereinbarungen zwischen Unternehmen können wettbewerbsbeschränkende Wirkung haben und sind daher grundsätzlich nach § 1 GWB unzulässig (Roßnagel 2002c, Rn. 148 f.). Ob dies auch für staatlich initiierte Absprachen zur Umsetzung von Allgemeininteressen gilt, ist umstritten. Überwiegend wird vertreten, dass das Kartellverbot nach § 1 GWB nicht zur Anwendung kommt, wenn der vom Staat inspirierte Inhalt der Abrede aufgrund einer speziellen gesetzlichen Ermächtigung in einem Gesetz festgelegt würde (z. B. Kloepfer, JZ 1980, 788; Baudenbacher, JZ 1988, 694; Brohm, DÖV 1992, 1027). Das Gleiche soll nach dieser Meinung auch bei staatlich inspirierten horizontalen Abreden gelten, die staatliche Regelungen der Wirtschaftslenkung ersetzen. Da staatliche wirtschaftslenkende Maßnahmen aus dem Kartellrecht ausgenommen sind, fallen nach dieser Meinung auch entsprechende Abreden zwischen den Unternehmen nicht unter das Kartellrecht. Über sie kann der Staat als Inspirator der Abrede kein Unrechtsurteil aussprechen. Das Kartellrecht habe keine Kontrollfunktion gegenüber staatlicher Wirtschaftslenkung, sondern lediglich gegenüber privaten »wirtschaftslenkenden« Maßnahmen .[18]

In dieser Situation erscheinen drei Regelungen angebracht: Zum einen ist – auch zur Sicherstellung der Gesetzeskonformität der selbstgesetzten Verhaltensregeln – deren Anerkennung durch die datenschutzrechtliche Kontrollstelle vorzusehen (ausführlich Roßnagel/Pfitzmann/Garstka 2001, 159 ff.). Dabei sollte die Kontrollstelle sicherstellen, dass ein Offenhalten des Datenschutzwettbewerbs gewährleistet ist. Zum anderen sollte aber im GWB klargestellt werden, dass privatrechtliche Absprachen, die zur Umsetzung von Verhaltensregeln erforderlich sind, nicht am Wettbewerbsrecht scheitern. Drittens sollte vorgesehen werden, dass solche horizontalen Verträge der zuständigen Kontrollstelle und der Kartellbehörde anzuzeigen sind. Die Kartellbehörde kann dann eventuell erforderliche Maßnahmen ergreifen. Sie wird hierzu sinnvoller Weise die Stellungnahme der zuständigen Kontrollstelle einholen.

9. Schutz gegen unlauteren Wettbewerb

Datenschutz durch Wettbewerb setzt auch eine Kontrolle und Sicherstellung des Wettbewerbs voraus. Insbesondere muss verhindert werden, dass mit Datenschutz unlauterer Wettbewerb betrieben wird. Wie im allgemeinen Lauterkeitsrecht sollte auch in diesem Bereich eine Kontrolle durch gesellschaftliche Akteure – im Sinn einer wirtschaftlichen Selbstkontrolle – in der Form ermöglicht werden, dass Wettbewerber und anerkannte Verbände die

Unterlassung datenschutzrechtswidriger Praktiken geltend machen können.

Zum einen sollte hierfür sichergestellt werden, dass Wettbewerber den Verstoß gegen Datenschutzpflichten im Rahmen einer privatrechtlichen Konkurrentenklage als unlauteren Wettbewerbsvorteil geltend machen können. Ob Datenschutzverstöße nach geltendem Recht die beiden Generalklauseln der §§ 1 und 3 UWG erfüllen können, blieb bisher umstritten.[19] Durch eine kleine Ergänzung des § 3 UWG sollte klargestellt, dass dies möglich ist, wenn der Datenschutzverstoß durch eine Handlung im geschäftlichen Verkehr begangen wurde (Roßnagel/Pfitzmann/Garstka 2001, 204).

Neben einer privatrechtlichen sollte auch eine an § 13 UWG angelehnte öffentlich-rechtliche Konkurrentenklage möglich sein (zur Einfügung dieser Forderung in die Struktur des VWG und zu einem Formulierungsvorschlag in Roßnagel/Pfitzmann/Garstka 2001, 204 f.). Mit dieser sollen Wettbewerber die verwaltungsgerichtliche Überprüfung der Rechtmäßigkeit behördlicher Maßnahmen oder Unterlassungen beantragen können. Voraussetzung für die Klage ist, dass der Kläger geltend macht, dass die behördliche Maßnahme oder das behördliche Unterlassen geeignet ist, den Wettbewerb zu seinem Nachteil zu beeinträchtigen. Diese Beeinträchtigung muss dadurch erfolgen, dass der andere Wettbewerber gegen abschließend bestimmte datenschutzrechtliche Pflichten verstößt. Der Kläger muss zu dem anderen Gewerbetreibenden in einem Wettbewerbsverhältnis stehen, also Waren oder gewerbliche Leistungen gleicher oder verwandter Art für denselben Markt herstellen oder auf demselben Markt vertreiben. Eine Beeinträchtigung des Wettbewerbs kann zum Beispiel entstehen, wenn ein Wettbewerber, der datenschutzrechtliche Pflichten missachtet, etwa keinen Datenschutzbeauftragten bestellt, Unterrichtungen unterlässt oder keine Einwilligungen einholt, in der Lage ist, preiswerter anzubieten als der Kläger, der die datenschutzrechtlichen Pflichten erfüllt.[20]

Zum anderen sollte sichergestellt werden, dass anerkannte Verbände und Vereine nach § 3 Abs. 1 Unterlassungsklagengesetz oder § 13 Abs. 2 UWG Datenschutzverstöße mit einer Unterlassungsklage verfolgen können. Diese Möglichkeit besteht bereits, wenn der Anspruch eine Handlung betrifft, durch die wesentliche Belange der Verbraucher berührt werden. Diese Regelung müsste dahingehend konkretisiert werden, dass dies auch bei wesentlichen Verletzungen von Vorschriften zum Schutz der informationellen Selbstbestimmung gilt. Dem Gedanken der gesellschaftlichen Selbstregulierung entspricht es auch, wenn Verstöße gegen die selbstgesetzten Verhaltensregeln durch anerkannte Verbraucher- und Datenschutzverbände verfolgt werden können (s. zum Zusammenhang zwischen Selbstregulierung der Wirtschaft und Selbstkontrolle der Akteure aus der Wirtschaft Roßnagel/Pfitzmann/Garstka 2001, 203f.). Selbstgesetzte Verhaltensregeln können nicht werbewirksam öffentlich für verbindlich erklärt und danach ohne jede wettbewerbsrechtliche Sanktion ignoriert werden[21].

Verbraucherverbände werden nach § 4 Unterlassungsklagengesetz vom Bundesverwaltungsamt anerkannt, wenn es sich um rechtsfähige Vereine mit

mehr als 75 Mitgliedern handelt, »die Interessen der Verbraucher durch Aufklärung und Beratung wahrnehmen«. Datenschutzverbände könnten nach den gleichen Kriterien anerkannt werden, hierfür wäre in § 4 Unterlassungsklagengesetz nur eine kleine Ergänzung vorzusehen: Nach dem Wort »Verbraucher« wäre »und der von der Datenverarbeitung Betroffenen« einzufügen.

10. Datenschutz durch Wettbewerb und Wettbewerb durch Datenschutz

Datenschutz und Marktwirtschaft könnten sich gegenseitig unterstützen. Datenschutz könnte durch das Mittel des Wettbewerbs leichter durchgesetzt werden, indem statt der Angst vor staatlichem Zwang das Eigeninteresse der verantwortlichen Stelle Datenschutzmaßnahmen motiviert. Die Aussicht, in der Konkurrenz um das Vertrauen der »Anspruchsgruppen«, nicht nur der Kunden, Vorteile zu erringen, mobilisiert die Eigeninitiative der Wettbewerber, ihren Datenschutz – möglichst nachprüfbar – zu verbessern. Umgekehrt bietet Datenschutz für den Wettbewerb eine Möglichkeit, sich vom Konkurrenten zu unterscheiden. Datenschutz ist ein Thema, über das mit den Anspruchsgruppen positiv kommuniziert werden kann und das ermöglicht, ein Image der Vertrauenswürdigkeit aufzubauen. Datenschutz verliert durch seine Verbindung mit dem Wettbewerbsgedanken sein Bild als bürokratisches Hindernis und gewinnt neue Konturen als Wettbewerbsvorteil, als Beratungsgegenstand, als Dienstleistung, als Produktidee und als Aspekt der Selbstbestimmung.

1 Podlech, DÖV 1970, 475; ders., DVR 1976, 25; ders. 1982, 451; Roßnagel/Wedde/Hammer/Pordesch 1990, 259 ff.; Roßnagel 1993, 241 ff.; ders. 2001, 13 ff.; Simitis 1996, 35 ff.; Hoffmann-Riem, AöR 1998, 537; Vogt/Tauss 1998, Nr. 6; Bizer 1999, 28 ff; aus technischer Sicht Pfitzmann, DuD 1999, 405 ff.

2 BVerfGE 65, 1 (43 f) »Der Einzelne hat nicht ein Recht im Sinne einer absoluten, uneinschränkbaren Herrschaft über ›seine‹ Daten; er ist vielmehr eine sich innerhalb der sozialen Gemeinschaft entfaltende, auf Kommunikation angewiesene Persönlichkeit. Information, auch soweit sie personenbezogen ist, stellt ein Abbild sozialer Realität dar, das nicht ausschließlich dem Betreiber allein zugeordnet werden kann.«

3 In der Regel bilden die Modelle eine soziale Beziehung ab, sie betreffen dann beide Partner der Beziehung und unterliegen nicht dem alleinigen Verfügungsrecht nur einer Person – s. z.B. Zöllner, RDV 1985, 12.

4 Für den öffentlichen Bereich kann dieses Prinzip wegen der Gesetzesbindung der Verwaltung nicht in gleichem Maß zum Tragen kommen – s. näher Roßnagel/Pfitzmann/Garstka 2001, 73 ff.

5 Eine Ausnahme sollte für die Datenverarbeitung vorgesehen werden, durch die wegen der Offenkundigkeit oder der Art der Verarbeitung schutzwürdige Interessen der betroffenen Person offensichtlich nicht beeinträchtigt werden – s. Roßnagel/Pfitzmann/Garstka 2001, 62.

6 Für die Bereiche der Warndienste, Detekteien und Auskunfteien, der Medien und der Forschung sollten ihren Arbeitsbedingungen angepasste Erlaubnistatbestände und Verarbeitungsregeln ermöglicht werden, wenn diese Bereiche sich selbst Verhaltensregeln erarbeiten, die von den zuständigen Kontrollstellen anerkannt werden können – s. Roßnagel/Pfitzmann/Garstka 2001, 77 ff.

7 Die Verhaltensregeln für den Datenschutz können Ergebnis der Selbstregulierung von Unternehmen und Verbänden sein, die durch die Anerkennung einer Datenschutzkontrollstelle Rechtsverbindlichkeit erlangen können – s. hierzu Roßnagel/Pfitzmann/Garstka 2001, 153 ff.

[8] www.w3c.org/P3P/; Cranor, P3P, Roadshow, www.w3.org/P3P/p3p-roadshow-0800.ppt; dies., DuD 2000, 479; Cavoukian/ Gurski/Mulligan/Schwartz, DuD 2000, 475; Grimm/Roßnagel 2000a, 293 ff.; dies. 2000b, 157; Wenning/Köhntopp, DuD 2001, 139 ff.; Greß, DuD 2001, 144 ff.; Lohse/Janetzko, CR 2001, 55

[9] Solche Dienstleistungen bietet z.B. www.enonimous.com an. Sie verwalten Kundendaten, schalten sich unbemerkt in die Internetkommunikation ein und geben die Daten nur weiter, wenn dies den Bedingungen des Kunden entspricht (z.B. www.digitalme.com; www.privaseek.com; www.privacybank.com; zu weiteren Beispielen s. www.koehntopp.de/marit/ publikationen/idmanage)

[10] Z.B. ISO 9.001 zum Qualitätsmanagement und ISO 14.001 zum Umweltschutzmanagement; EG-Verordnung Nr. 761/2001 »über freiwillige Beteiligung von Organisationen an einem Gemeinschaftssystem für das Umweltmanagement und die Umweltbetriebsprüfung« (EMAS) vom 19.3.2001, EG ABl. L 114 vom 24.4.2001, 1.

[11] Eine ähnliche Regelung wurde im Entwurf für ein Umweltgesetzbuch in §51 vorgeschlagen – s. Entwurf der Unabhängigen Sachverständigenkommission zum Umweltgesetzbuch 1998, 547.

[12] Eine solche Produktzertifizierung ist in Schleswig-Holstein nach § 4 Abs. 2 LDSG vorgesehen und in einer Verordnung umgesetzt, die allerdings den falschen Titel führt: Landesverordnung über ein Datenschutzaudit vom 3.4.2001, GVBl. I, 51, www.datenschutzzentrum.de/guetesiegel/ – s. näher Bäumler, DuD 2001, 252; ders., RDV 2001, 169 ff; Diek 2002.

[13] In der Regel verfügen die Anwender auch nicht über die für eine Zertifizierung des Produkts notwendige Detailinformation, wie über Quelltexte und verwendete Hilfsmittel, Entwurfsdokumentation und ähnliches.

[14] Zur Bedeutung für global agierende Unternehmen s. Büllesbach, RDV 2000, 1 ff. und Büllesbach/Höss-Löw, DuD 2001, 135 ff. Auch nach den Safe Harbor Principles wird ein Verstoß gegen die freiwillig übernommenen Prinzipien als unlautere und irreführende Handlung sanktioniert – s. Grundsätze des »sicheren Hafens« zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 10; Entscheidung der Kommission vom 26.7.2000, Art. 1 Abs. 2 b) und Erwägungsgrund 5, EG-ABl. L 215 vom 25.8.2000, 7.

[15] Zur Erhöhung der Akzeptanzchancen und zusätzlichen Gewinnen an »funktionaler« Legitimität s. z.B. Ritter, AöR 1979, 411; Ukrow 2000, 14.

[16] Z.B. Swire 1997, der darauf hinweist, dass dies insbesondere für die Kosten-Effektivität der Regelungen gilt; s. auch Fuhrmann 2001, 143. Selbstregulierung kann schließlich zu einer Entlastung des Staats führen und dazu beitragen, seine Überforderung zu verringern (s. hierzu am Beispiel des Umweltschutzes z.B. Faber 2011, 80).

[17] Für den Bereich des Umweltschutzes z.B. Oldiges, WiR 1973, 13 f.; Baudenbacher, JZ 1988, 692; Brohm, DÖV 1992, 1026; Schmidt-Preuß, VVDStRL 56 (1997), 215.

[18] Z.B. Baudenbacher, JZ 1988, 694f., Brohm, DÖV 1992, 1028) Allerdings fordert eine andere Meinung eine Genehmigung durch den Bundeswirtschaftsminister nach § 8 GWB, s. z.B. Kloepfer, JZ 1980, 784 ff.; Scherer, DÖV 1991, 5; Schmidt-Preuß, VVDStRL 56 (1997), 216f.

[19] Ein Wettbewerbsverstoß im Sinn des § 1 UWG durch Rechtsbruch wird in der Regel nur angenommen, wenn die verletzten Normen wertbezogen sind und dem Schutz wichtiger Rechtsgüter und Interessen dienen. Dies wird für das Datenschutzrecht in der Rechtsprechung zum Teil angenommen – s. z.B. BGH, NJW 1992, 2419; OLG Köln, WRP 1982, 540; OLG Koblenz, DuD 1999, 358; LG Mannheim, NJW 1996, 1835; LG Hamburg, CR 1997, 21; LG München I, CR 1998, 83; LG Stuttgart, DuD 1999, 295; OLG Köln, RDV 2001, 103 ff. – zum Teil verneint – s. z.B. OLG Frankfurt, DuD 1997, 47 – und zum Teil offengelassen – s. z.B. OLG Köln, MMR 2000, 106, das letztlich aber doch den Wettbewerbsverstoß bejaht. s. aus der Literatur z.B. Hoeren/ Lütkemeier 1999, 111 f.

[20] S. zu dieser öffentlich-rechtlichen Konkurrentenklage den parallelen Vorschlag in § 46 des Entwurfs zu einem UGB und seine Begründung die Unabhängigen Sachverständigenkommission zum Umweltgesetzbuch, 1998, 540.

[21] Auch nach den Safe Harbor Principles wird ein Verstoß gegen die freiwillig übernommenen Prinzipien als unlautere und irreführende Handlung sanktioniert – s. Grundsätze des »sicheren Hafens« zum Datenschutz, vorgelegt vom amerikanischen Handelsministerium am 21.7.2000, EG-ABl. L 215 vom 25.8.2000, 10; Entscheidung der Kommission vom 26.7.2000, Art. 1 Abs. 2 b) und Erwägungsgrund 5, EG-ABl. L 215 vom 25.8.2000, 7.

Literatur:

Arbeitskreis »Datenschutz-Audit Multimedia« (DuD 1999): Prinzipien und Leitlinien zum Datenschutz-Audit bei Multimedia-Diensten, DuD 1999, 285.

Baudenbacher, C. (JZ 1988): Kartellrechtliche und verfassungsrechtliche Aspekte gesetzesersetzender Vereinbarungen zwischen Staat und Wirtschaft – Ein Beitrag zu den staatlich inspirierten Selbstbeschränkungsabkommen, JZ 1988, S. 692.

Bäumler, H. (Hrsg.) (2000): E-Privacy, Braunschweig 2000.

Bäumler, H. (DuD 2001): Datenschutzaudit und Gütesiegel in Schleswig-Holstein, DuD 2001, S. 252.

Bäumler, H. (RDV 2001): Datenschutzaudit und IT-Gütesiegel im Praxistest, RDV 2001, S. 167.

Bäumler, H./v. Mutius, A. (Hrsg.) (2002): Datenschutz als Wettbewerbsvorteil, Vieweg 2000.

Bizer, J. (DuD 1998): Zweckbindung durch Willenserklärung, DuD 1998, 552.

Bizer, J. (DuD 2001): Ziele und Elemente der Modernisierung des Datenschutzrechts, DuD 2001, S. 274.

Brönneke, T./Bobrowski, M. (2000): Das als Kernanliegen des Verbraucherschutzes im E-Commerce, in: Bäumler 2000, S. 141.

Brohm, W. (DÖV 1992): Rechtsgrundsätze für normersetzende Absprachen – Zur Substitution von Rechtverordnungen, Satzungen und Gesetzen durch kooperatives Verwaltungshandeln, DÖV 1992, 1026.

Büllesbach, A./Garstka, H. (1997): Systemdatenschutz und persönliche Verantwortung, in: Müller, G./Pfitzmann, A. (Hrsg.), Mehrseitige Sicherheit in der Kommunikationstechnik, Bonn 1997, S. 383.

Büllesbach, A. (RDV 1997): Datenschutz und Datensicherheit als Qualitäts- und Wettbewerbsfaktor, RDV 1997, S. 239.

Büllesbach, A./Höss-Löw, P. (DuD 2001): Vertragslösung, Safe Harbor oder Privacy Code of Conduct, DuD 2001, S. 135.

Büllesbach, A. (RDV 2000): Datenschutz in einem globalen Unternehmen, RDV 2000, 1.

Cavoukian, A./Gurski, M./Mulligan, D./Schwartz, A. (DuD 2000): P3P und Datenschutz, DuD 2000, S. 475.

Cranor L. F.(1999): Agents of Choice: Tools that Facilitate Notice and Choice about Web Site Data Practices, Proc. of the 21st Int. Conference on Privacy and Personal Data Protection, 1999, S. 19.

Cranor, L. F. (DuD 2000): Platform for Privacy Preferences – P3P, DuD 2000, 479.

Diek, A. C. (2002): Gütesiegel nach dem schleswig-holsteinischen Landesdatenschutzgesetz, in Bäumler/v. Mutius (Hrsg.) (2002), S. 157.

Dix, A. (2002): Konzepte des Systemschutzes, in: Roßnagel (Hrsg.) (2002a), Kap. 3.5.

Faber, A. (2001) Gesellschaftliche Selbstregulierungssysteme im Umweltrecht – unter besonderer Berücksichtigung der Selbstverpflichtungen, Köln 2001.

Fuhrmann, H. (2001): Vertrauen im Electronic Commerce – rechtliche Gestaltungsmöglichkeiten unter besonderer Berücksichtigung verbindlicher

Rechtsgeschäfte und des Datenschutzes, Baden-Baden 2001.
Golembiewski, C. (2002): Das Datenschutzaudit in Schleswig-Holstein, in: Bäumler/v. Mutius (Hrsg.) (2002), S. 107.
Greß, S. (DuD 2001): Datenschutzprojekt P3P, DuD 2001, S. 144.
Grimm, R./Roßnagel, A. (2000a): Weltweiter Datenschutzstandard?, in: Kubicek, H./Bracyk, H.-J./Klumpp, D./Roßnagel, A. (Hrsg.), Global@Home, Jahrbuch Telekommunikation und Gesellschaft 2000, Heidelberg 2000, 293.
Grimm, R./Roßnagel, A. (2000b): Can P3P Help to Protect Privacy Worldwide?, in: ACM (Ed.) Multimedia Security, Proceedings of the International Workshop, November 2000, 157.dies. 2000b, S. 157;
Hansen, M. (2002): Privacy Enhancing Technologies, in: Roßnagel (2002), Kap. 3.3.
Hoffmann-Riem, W. (1997): Datenschutz als Schutz eines diffusen Interesses in der Risikogesellschaft, in: Krämer, L./Micklitz, H.-W./Tonner, K. (Hrsg.), Recht und diffuse Interessen in der Europäischen Rechtsordnung, Baden-Baden 1997, S. 777.
Hofmann-Riem, W. (1998): Informationelle Selbstbestimmung als Grundrecht kommunikativer Entfaltung, in: Bäumler, H. (Hrsg.), Der neue Datenschutz, Neuwied 1998, S. 11.
Hofmann-Riem, W. (AöR 1998): Informationelle Selbstbestimmung in der Informationsgesellschaft – Auf dem Weg zu einem neuen Konzept des Datenschutzes –, AöR 1998, 514.
Kloepfer, M. (JZ 1980): Umweltschutz als Kartellprivileg?, JZ 1980, 788.
Köhntopp, M./Pfitzmann, A. (2000): Datenschutz Next Generation, in: Bäumler (Hrsg.) 2000, S. 316.
Kranz, H. J. (2002): Datenschutz im Reise- und Tourismusgewerbe, in: Roßnagel (Hrsg.) 2002, Kap. 7.4.
Ladeur, K.-H. (DuD 2000): Datenschutz – vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken, Zur »objektiv-rechtlichen Dimension« des Datenschutzes, DuD 2000, S. 12.
Lohse, C./Janetzko, D. (CR 2001): Technische und juristische Regulationsmodelle des Datenschutzes am Beispiel von P3P, CR 2001, 55.
Hagel, J./Singer, M. (1999): Net Worth. The Emerging Role of the Infomediary in the Race for Costumer Information, Harvard Business School Press 1999.
Hoeren. T./Lütkemeier, S. (1999): Unlauterer Wettbewerb durch Datenschutzverstöße, in: Sokol, B. (Hrsg.), Neue Instrumente im Datenschutz, Düsseldorf 1999, S. 107.
Mattern. F./Langheinrich, M. (2001): Allgegenwärtigkeit des Computers – Datenschutz in einer Welt intelligenter Alltagsdinge, in: Müller, G./ Reichenbach, M. (Hrsg.), Sicherheitskonzepte für das Internet, Berlin 2001. 7.
Oldiges, M. (WiR 1973): Staatlich inspirierte Selbstbeschränkungsabkommen der Privatwirtschaft, WiR 1973, S. 13f.;
Opaschowski, H. (2002): Gesellschaftliche Grundlagen, in: Roßnagel (2002), Kap. 2.1.
Petri, T. B. (DuD 2001): Vorrangiger Einsatz auditierter Produkte, DuD 2001, 150.
Pfitzmann, A. (DuD 1999): Datenschutz durch Technik, DuD 1999, S. 405.

Pfitzmann, A./Schill, A./Westfeld, A./Wolf, G. (2000), Mehrseitige Sicherheit in offenen Netzen, Braunschweig 2000.
Pitschas, R. (DuD 1998): Informationelle Selbstbestimmung zwischen digitaler Ökonomie und Internet, DuD 1998, S. 139.
Podlech, A. (DÖV 1970): Verfassungsrechtliche Probleme öffentlicher Datenbanken, DÖV 1970, S. 473.
Podlech, A. (DVR 1976): Aufgaben und Problematik des Datenschutzes, DVR 1976, S. 23.
Podlech, A. (1982): Individualdatenschutz – Systemdatenschutz, in: Brückner/Dalichau (Hrsg.), Beiträge zum Sozialrecht, Festgabe für Grüner, Percha 1982, S. 451.
Ritter, H. (AöR 1979): Der kooperative Staat, AöR 1979, S. 411
Roßnagel, A. (1993): Rechtswissenschaftliche Technikfolgenforschung, Umrisse einer Forschungsdisziplin, Baden-Baden 1993.
Roßnagel A. (DuD 1999): Datenschutz in globalen Netzen, DuD 1999, S. 253.
Roßnagel, A. (2000): Datenschutzaudit Konzeption, Durchführung, gesetzliche Regelung, Braunschweig 2000.
Roßnagel, A. (Hrsg.) (2001): Allianz von Medienrecht und Informationstechnik: Herausforderungen und Hoffnungen, in: Roßnagel, A. (Hrsg.), Allianz von Medienrecht und Informationstechnik? Ordnung in digitalen Medien durch Gestaltung der Technik am Beispiel von Urheberschutz, Datenschutz, Jugendschutz und Vielfaltschutz, Schriftenreihe des Instituts für Europäisches Medienrecht (EMR) 24, Baden-Baden 2001, S. 17.
Roßnagel, A. (Hrsg.) (2002a): Handbuch des Datenschutzrechts, München 2002, i.E.
Roßnagel, A. (2002b): Konzepte des Selbstdatenschutzes, in: Roßnagel (Hrsg.) (2002), Kap. 3.4.
Roßnagel, A. (2002c): Konzepte der Selbstregulierung, in: Roßnagel (Hrsg.) (2002), Kap. 3.6.
Roßnagel, A. (2002d): Marktwirtschaftlicher Datenschutz im Datenschutzrecht der Zukunft, in: Bäumler/v. Mutius (Hrsg.) (2002), S. 115.
Roßnagel, A./Pfitzmann, A./Garstka, H. (2001): Modernisierung des Datenschutzrechts, Berlin, 2001.
Roßnagel, A./Wedde, P./Hammer, V./Pordesch, U. (1990): Digitalisierung der Grundrechte? Zur Verfassungsverträglichkeit der Informations- und Kommunikationstechnik, Opladen 1990.
Scherer, J. (DÖV 1991): Rechtsprobleme normersetzender »Absprachen« zwischen Staat und Wirtschaft am Beispiel des Umweltrechts, DÖV 1991, S. 5.
Schmidt-Preuß. M. (1997): Verwaltung und Verwaltungsrecht zwischen gesellschaftlicher Selbstregulierung und staatlicher Steuerung, VVDStRL 56 (1997), S. 215.
Schulz, W. (Verwaltung 1999): Verfassungsrechtlicher »Datenschutzauftrag« in der Informationsgesellschaft, Die Verwaltung 1999, S. 137.
Simitis, S. (1996): Virtuelle Präsenz und Spurenlosigkeit, in: Hassemer, W./Möller, K. P. (Hrsg.), 25 Jahre Datenschutz, Baden-Baden 1996, S. 28.

Simitis, S. (1987): Programmierter Gedächtnisverlust oder reflektiertes Bewahren, in: Fürst u.a. (Hrsg.), FS für Zeidler, Bd. 2, 1987, S. 1475.
Simitis, S. (DuD 2001): Auf dem Weg zu einem neuen Datenschutzkonzept, DuD 2000, S. 714.
Swire, P. P. (1997): Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information, in: U.S. Department of Commerce (Ed.), Privacy and Self-Regulation in the Information Age, Washington 1997, www.ntia.doc.gov/reports/ privacy/selfreg1.htm
Trute, H.-H. (1998): Öffentlich-rechtliche Rahmenbedingungen einer Informationsordnung, VVDStRL 57 (1998), S. 216.
Trute, H.-H (2002): Verfassungsrechtliche Grundlagen, in: Roßnagel (2002), Kap. 2.5.
Ukrow, J. (2000): Die Selbstkontrolle im Medienbereich in Europa, München 2000.
Unabhängige Sachverständigenkommission zum Umweltgesetzbuch (1998): Umweltgesetzbuch, Entwurf der Unabhängigen Sachverständigenkommission (UGB-KomE) zum Umweltgesetzbuch beim Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, hrsg. v. Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, Berlin 1998.
Vogt, U./Tauss, J. (1998): Entwurf für ein Eckwerte-Papier der SPD-Bundestagsfraktion: Modernes Datenschutzrecht für die (globale) Wissens- und Informationsgesellschaft, Bonn Oktober 1998.
Weichert, T. (2000): Zur Ökonomisierung des Rechts auf informationelle Selbstbestimmung, in: Bäumler (Hrsg.) 2000, S. 158.
Weichert, T. (DuD 2001): Datenschutz als Verbraucherschutz, DuD 2001, 264.
Weichert, T. (NJW 2001): Die Ökonomisierung des Rechts auf informationelle Selbstbestimmung, NJW 2001, S. 1463.
Wenning, R./Köhntopp, M. (DuD 2001): P3P im europäischen Rahmen, DuD 2001, S. 139.
Zöllner, W. (RDV 1985): Die gesetzgeberische Trennung des Datenschutzes für öffentliche und private Datenverarbeitung, RDV 1985, S. 3.