Innenausschuss
A-Drs 16(4)560 F neu

Prof. Dr. Hans Peter Bull
Bundesbeauftragter für den Datenschutz a.D.
Landesminister a.D.
Universität Hamburg, Seminar für Verwaltungslehre

Hamburg, im März 2009

Stellungnahme

**zu dem Gesetzentwurf der Bundesregierung
zur Regelung des Datenschutzaudits und zur Änderung datenschutzrechtlicher Vorschriften (BT-Drs. 16/12011)[1]**

– Beitrag zur Sachverständigenanhörung des Innenausschusses am 23. März 2009 –

I. Der Entwurf eines Datenschutzauditgesetzes

1. Der anzuwendende Maßstab

Der Gesetzentwurf des BMI verfolgt das Ziel, „einen über das gesetzlich vorgeschriebene Datenschutzniveau hinausgehenden Datenschutz“ zu fördern. Dieses Ziel scheint auf den ersten Blick begrüßenswert. Solange aber schon die gesetzlichen Vorschriften von einem relevanten Teil der Adressaten nicht eingehalten werden und es für die Betroffenen nicht erkennbar ist, ob die Einhaltung kontrolliert wird, wäre es schon ein großer Schritt zur tatsächlichen „Verbesserung“ des Datenschutzes und der Datensicherheit (vgl. § 9a BDSG!), wenn in einem geordneten, vertrauenswürdigen Verfahren festgestellt würde, dass ein bestimmtes Verfahren der Informationsverarbeitung bzw. -nutzung den gesetzlichen Vorschriften entspricht oder dass ein bestimmtes informationstechnisches Produkt datenschutzgerecht eingesetzt werden kann.

Ich verweise hierzu auf die Ausführungen der Stelle, die als einzige bisher über Erfahrungen mit einem Datenschutzaudit verfügt, nämlich des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein. In der Stellungnahme vom 13.10.2008 macht das ULD auf die Unterschiede zwischen der Zertifizierung „auf dem Gebiet des ökologischen Landbaus“, die als Vorbild für das DSAG gedient hat, und der Auditierung informationstechnischer Produkte aufmerksam, und stellt dar, dass solche Produkte aus unterschiedlichen Gründen datenschutzrechtlich unzureichend sein können. Für die gesetzeskonforme Ausführung von Datenverarbeitungsprozessen gilt erst recht, dass es den Betroffenen auf die **tatsächliche** Beachtung der Datenschutzvorschriften ankommt. Weil diese Prozesse in vielfältiger Weise gestaltet werden können, ergibt sich die

[1] Die folgende Stellungnahme bezieht sich implizit auch auf die im Anhörungsbeschluss bezeichneten Anträge von Abgeordneten der FDP (Drs. 16/1169) und der Fraktion „BÜNDNIS 90/DIE GRÜNEN“ (Drs. 16/1499 und 16/10216).

Datenschutzkonformität nicht „von selbst“ und nicht eindeutig allein aus den gesetzlichen Vorschriften.

Es ist daher durchaus sinnvoll, die Vergabe eines Gütesiegels **nicht** an die Voraussetzung zu knüpfen, dass die gesetzlichen Anforderungen **übererfüllt** werden. Wenn dem entgegengehalten wird, dass die Einhaltung des Gesetzes selbstverständlich sei und nicht „amtlich“ bestätigt zu werden brauche, so wird verkannt, dass dies eben bei der Datenverarbeitung nicht so ist. Jedenfalls in den Bereichen, die datenschutzrechtlich durch weit gefasste, unterschiedlich auslegbare Generalklauseln geregelt sind, kann die Auditierung und Zertifizierung den betroffenen Personen ein gewisses Maß an Sicherheit vermitteln, dass ihre Angaben gesetzeskonform verarbeitet und verwertet werden.

Das Gütesiegel kann aber nicht allein dafür verliehen werden, dass der Hersteller sein Produkt oder der Anwender sein Verfahren beschreibt und versichert, sich an diesen Rahmen halten zu wollen. Das **Vertrauen** der Betroffenen kann nur gewonnen werden, wenn die Hersteller bzw. die verantwortlichen Stellen sich einer unabhängigen **Kontrolle** unterwerfen, die **vor der Erteilung des Qualitätssiegels** durchgeführt wird. Die prüfende Stelle muss sich davon überzeugen, dass die korrekte Ausführung der jeweiligen (gesetzeskonformen) Konzepte etc. durch Organisations- und Verfahrensvorschriften sichergestellt ist. Unter dieser Voraussetzung trägt die Auditierung auch zur „Verbesserung“ des Datenschutzes i.S. von § 9a BDSG bei.

Die FDP-Fraktion stellt in ihrem Antrag Drs. 16/1169 v. 6. 4.2006 fest, es fehlten „anerkannte Kriterien, mit denen die datenschutzrechtliche Qualität von Produkten, Dienstleistungen und Datenverarbeitungsverfahren für den Einsatz in Wirtschaft und Verwaltung gemessen werden kann“. Das wesentliche Kriterium der „datenschutzrechtlichen Qualität“ von Produkten, Diensten und Verfahren kann aber nur sein, ob sie die **gesetzlichen Anforderungen** erfüllen. Dabei kann gewiss zwischen verschiedenen *Dimensionen* der Qualitätsprüfung (Umfang der Datenspeicherung, Datensicherheit, Transparenz u.ä.) unterschieden werden, etwa so wie das schleswig-holsteinische Landesrecht es tut, indem es „besondere Eigenschaften des IT-Produktes“ hervorhebt, insbesondere die Eignung zur Datenvermeidung und Datensparsamkeit, Datensicherheit und Revisionsfähigkeit der Datenverarbeitung sowie die Gewährleistung der Rechte der Betroffenen (Landesverordnung über ein Datenschutzaudit v. 3. 11.2008, § 2 Abs. 2 S. 1 Nr. 4). Eine graduelle Abstufung nach „Qualitätsklassen“ ist aber – anders als vielleicht bei den Produkten des ökologischen Landbaus – kaum möglich und dürfte – wenn überhaupt – nur geringe Bedeutung für den Wettbewerb der Unternehmen haben.

2. Einzelkritik des Entwurfs

Weil der Gesetzentwurf des BMI eine Übererfüllung der rechtlichen Vorgaben voraussetzt, muss er eine Methode entwickeln, strengere Vorschriften als das geltende (materielle) Gesetz zu formulieren, ohne diesen zusätzlichen Anforderungen Gesetzeskraft zu verleihen. Dazu soll ein achtzehn Mitglieder umfassender **Datenschutzauditausschuss** mit einer eigenen Geschäftsstelle geschaffen werden, der seinerseits der Rechtsaufsicht des BMI unterliegt. Er soll „Richtlinien“ zur Verbesserung des Datenschutzes und der Datensicherheit beschließen, deren „Erfüllung“ Voraussetzung des Auditsiegels sein soll.

Diese Regelung wird nicht zu dem gewünschten Erfolg führen, sondern eine neue Stufe übermäßiger **„Bürokratisierung“ –** d.h. **Überregulierung –** des Datenschutzes einleiten. Es ist schon fragwürdig, ob ein unabhängiger Ausschuss aus Vertretern von Verwaltungsbehörden, Unternehmen und Verbänden **legitimiert** wäre, derartige Richtlinien zu entwickeln. In der Sache wäre es jedenfalls angemessener und auch erfolgversprechender, wenn die Beteiligten selbst – im Wettbewerb miteinander – die wünschenswerten Verbesserungen entwickelten und die Ergebnisse dann **einzeln** von einer unabhängigen Stelle geprüft würden. Aus der Prüfungspraxis mögen sich dann im Laufe der Zeit neue, höhere Standards ergeben, die vom Gesetzgeber bei Gelegenheit der nächsten Novelle verallgemeinert werden könnten.

Auch die **Ausgestaltung der Kontrollen** ist in dem Entwurf des BMI nicht gelungen. Der Entwurf schafft allenfalls den gesetzlichen Rahmen für die Entstehung eines neuen, bisher nur in Ansätzen vorhandenen Gewerbezweiges; bei der Entwicklung dieses Gewerbes sollen aber zahlreiche gesetzliche und behördliche Vorgaben beachtet werden. Die vorgesehenen Regelungen über die Zulassung und Beaufsichtigung der „Kontrollstellen“ und den Datenschutzauditausschuss sind wesentlich umfangreicher und detaillierter als die über die Voraussetzungen und das Verfahren der Prüfung selbst. Es ist zwar zu begrüßen, dass die Zulassung der Kontrollstellen von strengen Voraussetzungen abhängig gemacht wird (vgl. insbes. § 5), aber diese Vorschriften sind viel zu umständlich. So fragt es sich, warum außer der Zulassung durch denn Bundesbeauftragten noch eine zusätzliche „Akkreditierung“ erforderlich sein soll (§ 4 Abs. 1 S. 1 Nr. 2). Bei den Anforderungen an das Personal ist die Unabhängigkeit besonders betont (§ 5 Abs. 2), und die fachliche Vorbildung ist spezifiziert (§ 5 Abs. 3). Doch ist damit nicht ausgeschlossen (und es kann gar nicht ausgeschlossen werden), dass die Kontrollen tendenziell zu „wohlwollend“ durchgeführt werden; der Wert der strengen Klauseln ist also begrenzt.

Die zuständigen Behörden, insbesondere der Bundesbeauftragte (§ 2 Abs. 2) werden jedenfalls intensiv damit beschäftigt sein, die Kontrollstellen zuzulassen und zu überwachen (§ 7 Abs. 1 S. 1 und § 8), Informationen auszutauschen (§ 7 Abs. 1 S. 2 - 4) und zu überprüfen, ob Auditsiegel zu Unrecht erteilt worden sind (§ 7 Abs. 2 i.V.m. § 6 Abs. 3 S. 2). Es ist zweifelhaft, ob dieser große Aufwand notwendig ist.

Ein Kardinalfehler des Entwurfs besteht darin, dass das Gütesiegel **ohne vorherige Prüfung** erteilt werden soll, allein auf die Versicherung des Unternehmens hin, dass es sich nach § 3 des Entwurfs kontrollieren lasse – also erst im Anschluss an die Anzeige beim Bundesbeauftragten (§ 3 S. 4 i.V.m. § 9 Abs. 1 S. 1). Die vorgeschriebene Kontrollfrequenz (§ 3 S. 3 - 5) ist großzügig bemessen. Ob das Publikum unter diesen Umständen auf die behauptete Datenschutzqualität vertrauen wird, ist fraglich.

Kritisch zu beurteilen ist schließlich die Zuständigkeitsregelung, die entgegen der Regel des Art. 83 GG dem Bund (BfDI und BMI) wesentliche Elemente der administrativen Durchführung des Gesetzes zuschreibt. Zwar ist es richtig, dass die Auditierung mit Wirkung über die Ländergrenzen hinaus geschehen sollte. Dazu bedarf es aber keiner Zuständigkeitskonzentration beim Bund, sondern nur der gesetzlichen Klarstellung, dass das Gütesiegel bundesweit gilt. So wie Führerscheine und Kfz-Zulassungen von Landesbehörden mit Wirkung für das ganze Bundesgebiet

(und darüber hinaus international!) gelten, bestehen auch keine Bedenken gegen die überregionale Anerkennung der Auditierung und ggf. Zertifizierung.

3. Alternative

Als Alternative zu dem überkomplizierten BMI-Entwurf bietet es sich an, auf das Prinzip der „**geprüften Sicherheit**“ umzustellen, das Gütesiegel also erst aufgrund einer Prüfung durch eine zuständige Stelle zu erteilen. (Der Begriff „Auditsiegel“ sollte vermieden werden, da er zu sehr Fachbegriff ist und daher vielen Menschen unverständlich sein wird.)

Damit könnte an die Praxis angeknüpft werden, die sich in Schleswig-Holstein schon seit längerem bewährt hat. Unter der Aufsicht des ULD prüfen fachlich ausgewiesene und als solche anerkannte Gutachter informationstechnische Produkte darauf hin, ob sie den Rechtsvorschriften über den Datenschutz und die Datensicherheit entsprechen. Das ULD „zertifiziert“ auf dieser Grundlage die Produkte; damit wird ihre Kennzeichnung durch ein Gütesiegel erlaubt (§ 1 Abs. 1 und 3 der zitierten Datenschutzauditverordnung). Das ULD arbeitet auf diesem Gebiet auch mit ausländischen Partnern zusammen und bereitet mit Förderung durch die EU die Markteinführung eines europäischen Datenschutz-Gütesiegels vor (vgl. den Tätigkeitsbericht des ULD 2008, LT-Drs. 16/1839, S. 155 ff.).

Auch die Freie Hansestadt Bremen hat ein Prüf- und Bewertungsverfahren (Datenschutzaudit) eingerichtet; es steht allerdings nur öffentlichen Stellen zur Verfügung (Bremische Datenschutzauditverordnung v. 5.10.2004). Durchgeführt wird dieses Verfahren durch einen Auditor, der vom Landesbeauftragten für den Datenschutz zugelassen wird.

II. Die BDSG-Änderungen zur Einschränkung von Werbung, Marktforschung und Meinungsforschung

1. Abschaffung des „Listenprivilegs“ (§ 28 Abs. 3 S. 1 Nr. 3 BDSG)

Nach geltendem Recht dürfen bestimmte personenbezogene Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung ohne Einwilligung des Betroffenen verwendet (übermittelt oder genutzt) werden, wenn sie „listenmäßig oder sonst zusammengefasst“ sind und „kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat“ (§ 28 Abs. 3 Satz 1 Nr. 3 BDSG). Die Sinnhaftigkeit dieses „Listenprivilegs“ ist einigermaßen fragwürdig; es handelt sich um ein spezielles Privileg für den Adressenhandel, das mit den sonstigen Prinzipien des Datenschutzrechts kaum vereinbar ist. Zudem wird die Vorschrift bisher offenbar von den interessierten Unternehmen sehr weit ausgelegt, und es wird vermutlich nur selten geprüft, ob der Betroffene ein schutzwürdiges Interesse am Ausschluss der Verwendung hat.

Allerdings ist dies nicht verwunderlich, weil nämlich dieses Interesse allenfalls in Ausnahmefällen bestehen kann; durch die Übermittlung und Nutzung der „privilegierten“ Daten wird in aller Regel kein Risiko für die Betroffenen begründet. In dem Normalfall, dass ein Unternehmen Namen und Anschriften von Kunden an ein anderes Unternehmen weitergibt, das dann gezielte Werbeschreiben an die

Betroffenen versendet, entsteht keinerlei Nachteil und meist nicht einmal eine Gefahr für irgendwelche Rechtsgüter (Beispiel für eine denkbare Ausnahme: Sicherheitsgründe).

Gezielte Werbung kann andererseits für Absender wie Empfänger nützlich sein. Für einige Branchen und insbesondere für kleine Unternehmen, die neu auf den Markt drängen, ist es sogar dringend wünschenswert oder sogar zwingend nötig, dass sie potentielle Kunden gezielt ansprechen können. Dieses Interesse sollte vom Gesetzgeber anerkannt werden. Das Datenschutzrecht sollte sinnvolle wirtschaftliche Betätigung, die anderen nicht schadet, möglichst nicht behindern.

In der letzten Zeit sind in großer Zahl zu Werbezwecken übermittelte Daten für andere Zwecke – insbesondere unzulässige Werbeanrufe und unberechtigte Abbuchungen von einem Konto des Betroffenen – *missbraucht* worden. Der Adressenhandel und die Call-Center-Branche sind dadurch insgesamt in Misskredit geraten, auch soweit sie sich gesetzestreu verhalten. Als Reaktion auf diese Fälle rechtswidrigen Umgangs mit personenbezogenen Daten ist vorgeschlagen worden, Übermittlungen zu Werbe- und Marketingzwecken generell einzuschränken, vielleicht sogar ganz zu verbieten. Aber es wäre eine fragwürdige Methode, Missbrauch dadurch zu bekämpfen, dass man den Bereich *nicht* missbräuchlichen Verhaltens einschränkt.

Vertretbar und konsequent im Sinne der Einheitlichkeit des Datenschutzes ist es allerdings, im Fall der Werbedaten die Übermittlung und Nutzung personenbezogener Daten an die strengere Voraussetzung zu knüpfen, dass die Betroffenen **einwilligen.** Damit wird ein ohnehin sonst geltendes Prinzip zur Geltung gebracht, das in der Regel einen angemessenen Interessenausgleich ermöglicht. Auf diese Weise kann zudem bei den Betroffenen wieder um das **Vertrauen** geworben werden, das durch die Missbrauchsfälle verloren gegangen ist. Die Unternehmen, die auf die Vermittlung von Anschriften angewiesen sind oder diese Vermittlung betreiben, werden sich bemühen müssen, die Einwilligungserklärungen den entsprechenden Bedürfnissen anzupassen. (Dabei ist besonders auf die Einhaltung von § 4a BDSG – Informationspflicht, besondere Gestaltung der Formulare – zu achten!)

Der Entwurf geht einen vertretbaren Mittelweg zwischen Einwilligungslösung (§ 28 Abs. 3 Satz 1) und einem modifizierten (beschränkten) Listenprivileg. Die Ausnahmen vom Einwilligungsvorbehalt sind im wesentlichen angemessen. Vor allem die Nutzung für eigene Werbung sowie Markt- oder Meinungsforschung (Nr. 1) und für Zwecke der Spendenwerbung (Nr. 3) ist unbedenklich. Zu Nr. 2 könnte man fragen, ob nicht Geschäftsadressen generell freigegeben werden sollten; sie sind ja gerade dazu bestimmt, Kontakte mit anderen zu vermitteln. Eine weitere Erleichterung für die werbende Wirtschaft ist in § 28 Abs. 3 Satz (Erlaubnis der Beipackwerbung) enthalten.

Nicht mehr erlaubt ist jedoch die Verarbeitung allgemein zugänglicher Daten (bisher § 28 Abs. 1 Satz 1 Nr. 3 BDSG; diese Bestimmung ist in den neuen Text offenbar bewusst nicht übernommen worden). Das mag auf den ersten Blick irritieren, hat aber seinen Grund darin, dass auch die Angaben in gedruckten Verzeichnissen nicht ohne weiteres dazu bestimmt sind, von jedermann genutzt zu werden. Die „Öffentlichkeit“ von Mitgliederlisten u.ä. ist also mehr oder weniger beschränkt. Erst

recht erscheint diese Überlegung plausibel, wenn man an die Öffentlichkeit des Internets denkt. Das Internet ist vielfach auch Kommunikationsinstrument für Teilgruppen, die den Kontakt mit Dritten nicht anstreben.

Insgesamt lässt sich feststellen: Der Übergang vom „Listenprivileg“ als allgemeinem Privileg für die werbende Wirtschaft zum Einwilligungsprinzip ist systemgerecht und wird in dem Entwurf des BMI hinreichend abgefedert. Die Unternehmen werden sich auf diese Einschränkungen einstellen können, insbesondere indem sie die Einwilligungserklärungen so formulieren, dass sie den legitimen Bedürfnissen der Datennutzer gerecht werden.

2. Die Form der Einwilligung

a) Nach dem Entwurf des BMI soll die Einwilligung in die Datenverwendung zur Werbung etc. nur gültig sein, wenn durch eine **besonders strenge Form** jeder Zweifel daran ausgeschlossen ist, dass der Betroffene bewusst gerade in diese Verwendung einwilligt. Der Text dieser Klausel (§ 28 Abs. 3a Satz 2 BDSG-E) lautet:

> „Eine zusammen mit anderen Erklärungen erteilte Einwilligung ist nur wirksam, wenn der Betroffene durch Ankreuzen, durch eine gesonderte Unterschrift oder durch ein anderes, ausschließlich auf die Einwilligung in die Verarbeitung oder Nutzung der Daten für Zwecke des Adresshandels, der Werbung oder der Markt- oder Meinungsforschung bezogenes Tun zweifelsfrei zum Ausdruck bringt, dass er die Einwilligung bewusst erteilt.“

Eine solche Formvorschrift findet sich sonst im gesamten Datenschutzrecht nirgends. Als allgemeine Regelung bestimmt § 4a Satz 3 BDSG für die Einwilligung in alle anderen Formen der Datenerhebung, -verarbeitung und -nutzung die *Schriftform*, „soweit nicht wegen besonderer Umstände eine andere Form angemessen ist“; wenn die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden soll, so ist sie „besonders hervorzuheben“. Dass sie freiwillig erfolgt, ist Gültigkeitsvoraussetzung und muss daher im Streitfall bewiesen werden (dies auch zur Stellungnahme des Bundesrates Nr. 13), begründet aber im Rahmen von § 4a BDSG kein zusätzliches Formerfordernis. Dasselbe gilt für die in § 4a Satz 2 BDSG vorgeschriebene *Information* des Einwilligenden über den Zweck der Erhebung, Verarbeitung oder Nutzung und – eventuell – über die Folgen der Verweigerung der Einwilligung.

Nach der geplanten Regelung sollen ausgerechnet für die im Normalfall vollkommen harmlose Übermittlung von Adressen zu Werbezwecken (und zur Markt- oder Meinungsforschung, die ebenso wenig Risiken für die Betroffenen begründen) besondere formale Hürden aufgebaut werden. Wenn ein Kreditinstitut sich die Einwilligung erteilen lässt, Daten an Auskunfteien, an die Schufa oder an eine zentrale Warndatei (z.B. der Versicherungswirtschaft) weiterzugeben – also Daten, die ein Bild von der Zahlungsfähigkeit und Kreditwürdigkeit des Kunden vermitteln – , werden keine gleich strengen Anforderungen gestellt. Darin liegt ein **Wertungswiderspruch**, der nur schwer verständlich ist und den der Gesetzgeber vermeiden sollte.

Das mit der Klausel verfolgte Ziel, „unfreiwillige“ Einwilligungen auszuschließen, kann überdies auf diese Weise gar nicht erreicht werden. Es kann nämlich durchaus sein,

dass Betroffene auch solche Erklärungen „blind“ unterschreiben, ohne sich Gedanken über die Folgen zu machen. Ein solches Verhalten kann auch vollkommen rational sein: Wenn jemand die Praxis der Adressennutzung kennt und daher weiß, dass die Erklärung ihm nicht schadet, oder wenn er es in Kauf nimmt, mit gezielter Werbung eingedeckt zu werden, handelt er genauso als „mündiger“ Verbraucher wie ein anderer, der eine solche Erklärung zunächst sorgfältig durchliest und dann in vollem Bewusstsein der Folgen sein Kreuz anbringt. Der Staat braucht niemanden davor zu bewahren, dass er geringfügige Belästigungen hinnimmt.

b) Mit der bezeichneten Klausel würde sich der Gesetzgeber in **Widerspruch zur Rechtsprechung des Bundesgerichtshofs** (BGH) setzen. Dieser hat in seinem Urteil vom 16. Juli 2008 in Sachen Verbraucherzentrale Bundesverband gegen Payback Rabattverein[2] eine anders gestaltete Einwilligungserklärung als „bewussten und autonomen Willensakt“ anerkannt, obwohl „ein unsorgfältiger Verbraucher“ sie möglicherweise überliest. Diese Klausel war so aufgebaut, dass neben der eigentlichen Einwilligungserklärung[3] – die vom BGH nur in Bezug auf SMS- und E-Mail-Werbung für ungültig erklärt wurde – ein vorgedrucktes Kästchen angebracht war, neben dem die Worte standen: „Hier ankreuzen, falls die Einwilligung **nicht** erteilt wird“.[4] Auf diese Einwilligung oder Nichteinwilligung folgte schließlich die Unterschrift, die alle vorangehenden Teile der „Payback-Anmeldung“ abdeckte. Der BGH hat dazu erklärt, es sei „nicht auf einen oberflächlichen, sondern auf einen durchschnittlich informierten und verständigen Verbraucher abzustellen, der einer vorformulierten Einwilligungserklärung die der Situation angemessene Aufmerksamkeit entgegenbringt“.[5] Auch im Rahmen von § 4a Abs. 1 BDSG sei „dem Betroffenen jedenfalls ein Mindestmaß an Aufmerksamkeit zuzumuten“.[6] Dem trägt nach Ansicht des BGH die von dem Payback Rabattverein benutzte Klausel hinreichend Rechnung. Sie ist inzwischen der Entscheidung des BGH in Bezug auf SMS und E-Mail-Werbung angepasst worden und wird im übrigen (Ankreuzen der Nichteinwilligung) weiter verwendet. Es besteht kein Anlass, diese Rechtsprechung durch Gesetz zu ändern.

Nach einer von der Firma Loyalty Partner in Auftrag gegebenen Untersuchung der „Innofact AG“ achten 80 Prozent der Befragten beim Abschluss eines Vertrags auf die Datenschutzbestimmungen. Mehr als ein Drittel der Verbraucher geben an, sie genau durchzulesen. Rund 70 Prozent der Befragten vertrauen den Anbietern von Kundenkarten, was einen sorgfältigen Umgang mit ihren Daten angeht.[7]

---

[2] Az. VIII ZR 348/06, NJW 2008, 3055 = GRUR 2008, 1010..

[3] „Mit meiner Unterschrift erkläre ich mich einverstanden, dass die von mir oben angegebenen Daten sowie die Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Datum des Vorgangs) für an mich gerichtete **Werbung** (z.B. Informationen über Sonderangebote, Rabattaktionen) per Post und mittels ggf. von mit beantragter Services (SMS oder E-Mail-Newsletter) sowie zu Zwecken der **Marktforschung** ausschließlich von der Loyalty Partner GmbH und den Partnerunternehmen gemäß **Nummer 2 der beiliegenden Hinweise zum Datenschutz** gespeichert und genutzt werden.“ (Hervorhebungen im Original). Nach dem BGH-Urteil ist die Bezugnahme auf SMS- und E-Mail-Werbung aus dieser Klausel herausgenommen worden.

[4] Es ist strittig, ob diese Gestaltung eine besondere Form von „opt-in“ darstellt (so die Auffassung der Payback-Betreiber) oder ob sie besser als „opt-out“ bezeichnet werden sollte. Nach der Gesetzessystematik ist ein „opt-out“ nur im Falle des *Widerspruchs* gegen die Datenerhebung oder -verarbeitung gegeben (§ 28 Abs. 4 BDSG). Wegen der Unklarheiten empfiehlt es sich, die Begriffe „opt-in“ und „opt-out“ zu vermeiden und das Gemeinte genauer auszudrücken.

[5] In dem Urteil folgen Hinweise auf frühere Entscheidungen: BGHZ 156, 250, 252f. – Marktführerschaft – und BGH, GRUR 2005, 438 = WRP 2005, 480 – Epson-Tinte.

[6] Abs. 24 des Urteils.

[7] Information der Firma Loyality Partner an den Verfasser.

c) Die nunmehr vorgeschlagene Regelung soll im Grunde davon **abschrecken**, die Einwilligung zu erteilen, und schützt daher vor allem diejenigen, die sich vor **unbekannten Risiken** fürchten. Das könnte sinnvoll sein, wenn man wirklich mit ernsthaften Risiken für Rechte und Interessen der Betroffenen rechnen müsste. Davon kann trotz der „Skandale" der letzten Zeit nicht die Rede sein. Die Tatsache, dass mit legal erworbenen Daten rechtswidrig umgegangen worden ist, rechtfertigt nicht die Änderung der Erlaubnistatbestände, sondern allenfalls Verbesserungen des einzuhaltenden Verfahrens.

Vielfach wird die Sorge geäußert, die Daten von Kunden könnten zur Erstellung von „**Persönlichkeitsprofilen**" benutzt werden, die dann ihrerseits an Dritte weitergegeben und für obskure Zwecke – bis hin zu geheimdienstlichen Ermittlungen – verwendet würden. Damit wird unterstellt, dass die Zweckentfremdung von Daten in großem Ausmaß üblich sei. Die Autoren, die sich so äußern, verkennen schon die Interessenlage der beteiligten Unternehmen. Diese wollen werben, neue Produkte in den Markt einführen oder Meinungen über Produkte und Leistungen erforschen. Ihnen kann nicht daran liegen, die früheren oder potentiellen künftigen Kunden zu überwachen oder ihnen zu schaden. Staatliche Stellen, die nach bestimmten Personen suchen, mögen zwar im Einzelfall versuchen, vorhandene Kundendaten zu „rastern"; sofern die dafür geltenden strafprozessualen oder polizeilichrechtlichen Voraussetzungen gegeben sind, wäre das jedoch eine legale, wenn auch von Kunden wie Unternehmen nicht gewollte Maßnahme zur Vorbereitung gezielter Ermittlungen gegen Einzelne und daher ebenfalls keine Massen-„Überwachung".

Die große Menge der Kunden, denen an Rabatten, Lotteriegewinnen und ähnlichen Vergünstigungen gelegen ist, braucht sich insofern nicht zu sorgen. Es ist aus Gründen des Datenschutzes also nicht angezeigt, die Kunden von der Einwilligung in die Datennutzung abzuschrecken. Von einer bewussten Abschreckungsstrategie sollte der Gesetzgeber auch deshalb Abstand nehmen, weil die Erschließung neuer und die Pflege alter Märkte gerade gegenwärtig – in einer Zeit wirtschaftlicher Krisen – wünschenswert ist und der Adresshandel dazu beitragen kann.

Aus den genannten Gründen halte ich es für geboten, § 28 Abs. 3a Satz 2 der Entwurfsfassung zu streichen. Die geltende Vorschrift des § 4a BDSG reicht aus, die Betroffenen vor „Übertölpelung" zu schützen.

3. Das Verbot der Koppelung von Einwilligung und Vertragsschluss

Durch § 28 Abs. 3b BDSG-E soll es verboten werden, den Abschluss eines Vertrags von einer Einwilligung des Betroffenen in die Datenverwendung abhängig zu machen, „wenn dem Betroffenen ein anderer Zugang zu gleichwertigen vertraglichen Leistungen ohne die Einwilligung nicht oder nicht in zumutbarer Weise möglich ist". Dieses **Koppelungsverbot** ist gerechtfertigt, weil es dazu dienen kann, die Freiwilligkeit der Einwilligung zu sichern. Entgegen dem Petitum des Bundesrates (Nr. 15) sollte dieses Verbot aber nicht ohne die zitierte Voraussetzung gelten. Wenn der Verbraucher ohne weiteres auf ein anderes Angebot ausweichen kann, ist seine Freiwilligkeit ausreichend gesichert. Auf die „Marktbeherrschung" eines Unternehmens kommt es dabei nicht an; dieser Begriff taucht im Gesetz nicht auf. Das Abstellen auf die **Zumutbarkeit** erweitert den Anwendungsbereich in angemessener Weise. Die Unternehmen können aber, wie in der

Gesetzesbegründung richtig ausgeführt ist (S. 26 zu Nr. 5, unterer Absatz) die Betroffenen „z.B. durch Gewährung von Vorteilen für eine Einwilligung gewinnen“.

Wenn der Bundesrat darauf hinweist, dass sich ein eingeschränktes Koppelungsverbot bereits aus § 4a Abs. 1 Satz 1 BDSG ergibt und durch die neue Vorschrift Auslegungsschwierigkeiten befürchtet, so plädiert er im Grunde für eine Streichung dieser Vorschrift. Das hielte ich gerade im Interesse der Gesetzesklarheit nicht für angebracht.

4. Stärkung des Widerspruchsrechts oder Bekräftigung des Widerrufsrechts?

Der Bundesrat schlägt eine Änderung des § 35 Abs. 5 BDSG vor, durch die das Widerspruchsrecht des Betroffenen gestärkt werden soll (Stellungnahme Nr. 17). Dieser Forderung sollte der Gesetzgeber nicht folgen. Wenn die Datenverwendung für Zwecke der Werbung etc. grundsätzlich von einer Einwilligung abhängig gemacht wird, besteht für ein allgemeines Widerspruchsrecht schon kein Bedarf mehr (anders für ein **Widerrufsrecht**; dieses ist in § 28 Abs. 3a Satz 1 BDDSG-E für die in anderer Form als schriftlich erteilte Einwilligung vorgesehen; der entsprechende Satzteil sollte dadurch stärker betont werden, dass er in einen eigenen Satz umgewandelt wird: „Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden“).

§ 35 Abs. 5 ist bereits in der geltenden Fassung schwer verständlich und in der Sache fragwürdig. Die Vorschrift soll den Betroffenen nicht vor der Verarbeitung „seiner“ Daten an sich schützen, sondern davor, dass diese gerade *in dateimäßiger Form* geschieht (vgl. den ersten Satz: „nicht für eine automatisierte Verarbeitung oder Verarbeitung in nicht automatisierten Dateien“ und am Ende dieses Satzes: „Interesse ... an *dieser* Erhebung“ etc.). Die Verarbeitung in anderer Form (z.B. die gezielte Einzelmitteilung einer kompromittierenden Information) kann gleiche oder sogar schwerere Beeinträchtigungen mit sich bringen. Andererseits ist die automatisierte oder zumindest dateimäßige Verarbeitung seit vielen Jahren die Regel, und es ist schwer vorstellbar, welche Interessen eines einzelnen Betroffenen am Ausschluss dieser Verarbeitungsformen über die allgemeinen Datenschutzbedenken hinaus hier gemeint sein könnten, die nicht bereits in die grundsätzlichen Überlegungen des Gesetzgebers eingegangen sind, also in den allgemeinen Regelungen des BDSG ihren Ausdruck gefunden haben. § 35 ist eine allgemeine Vorschrift über subjektive Rechte der Betroffenen; inhaltliche Spezialvorschrift für Werbung, Markt- und Meinungsforschung ist § 28.

Wenn gleichwohl ein Bedürfnis für eine Erweiterung oder Stärkung des Widerspruchsrechts gesehen wird, sollte geprüft werden, ob nicht die **Robinson-Liste**, die seit langem von der Wirtschaft betrieben wird, aber offensichtlich wenig bekannt ist und wenig genutzt wird, als Angebot eines besseren Daten- und Verbraucherschutzes öffentlich gefördert werden könnte. Jedenfalls wäre es zu wünschen, dass dieses Angebot besser bekannt gemacht wird.

5. Weitere Nutzung rechtmäßig erhobener Daten

Nach der *Übergangsvorschrift* des **§ 47 BDSG** sollen die in der Vergangenheit wirksam eingeholten Einwilligungen vom Ende der Übergangsfrist an unwirksam

werden. Darin liegt eine rückwirkende Verschlechterung der Rechtsposition gerade der Unternehmen, die schon bisher die Einwilligung der Verbraucher eingeholt haben. Dass sie dies nicht in der Form getan haben, die § 28 Abs. 3a Satz 2 nunmehr vorschreiben will (s. oben II. 2.), ändert nichts an der Rechtmäßigkeit des Informationserwerbs; wie schon ausgeführt, hat der BGH die verwendete Opt-in-Klausel gebilligt. In § 47 sollte daher die **Befristung gestrichen** werden. Da die Daten ohnehin veralten und durch neu erhobene ersetzt werden müssen, wird die Umstellung auf die neue Rechtslage ohnehin erfolgen.

6. Gleichstellung von Markt- und Meinungsforschung

Ein Mangel, der schon im geltenden BDSG enthalten ist, wird von der Novelle *nicht* beseitigt: die Gleichstellung von Marketing und Marktforschung zu geschäftlichen Zwecken einerseits, der allgemeinen Meinungsforschung andererseits. **Meinungsforschung** liegt – jedenfalls typischerweise – im Allgemeininteresse, nicht (nur) im Interesse der forschenden Unternehmens. Der Bundesrat hat dies mit Recht in seiner Stellungnahme (Nr. 16) herausgestellt. Seiner Forderung, die Zulässigkeit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu Zwecken der Meinungsforschung in den §§ 28 und 30 BDSG klarzustellen, sollte gefolgt werden. Es ist nämlich zweifelhaft, ob die politischen Meinungen, die Einstellungen der Bevölkerung zu aktuellen sozialen, politischen und kulturellen Fragen oder ihre Urteile zu alltäglichen Problemen wirklich zuverlässig erforscht werden können, wenn jeweils zuvor die Einwilligung eingeholt wird (und wenn gar die Formerfordernisse des geplanten § 28 Abs. 3a beachtet werden müssen). Auch die etwas weitergehende Ermächtigung zur Datenverarbeitung zu *eigener* Meinungsforschung (§ 28 Abs. 3 Satz 2 Nr. 1) dürfte wenig zur Beseitigung der Schwierigkeiten beitragen, die insofern bestehen; denn sie setzt voraus, dass die Daten von der verantwortlichen Stelle selbst erhoben worden sind – was keineswegs den Normalfall darstellt.

III. Andere BDSG-Änderungen

1. Stärkung der Aufsichtsbehörden und der internen Datenschutzbeauftragten

Angesichts der heutigen Situation ist die Forderung des Bundesrates nach Stärkung der Aufsichtsbehörden (Stellungnahme Nr. 18) gut begründet. Diese sollten in der Tat das Recht zu **Anordnungen und Untersagungsverfügungen** erhalten, das seit langem vermisst wird. Die bisherigen Befugnisse, die sich nur auf technische und organisatorische Mängel beziehen, reichen nicht aus.

Zu begrüßen ist auch die in § 4f Satz 3 BDSG vorgesehene stärkere Absicherung des Arbeitsverhältnisses der **betrieblichen und behördlichen Datenschutzbeauftragten**. Diesen wird dadurch für den Fall eines Konfliktes mit der Unternehmens- oder Behördenleitung der Rücken gestärkt. Gleichwohl dürfen die Erwartungen an die Konflikt- und Durchsetzungsfähigkeit des Beauftragten nicht überhöht werden. Seine Unabhängigkeit ist unvermeidlich schon dadurch begrenzt, dass er bei seinen Bemühungen um die Verbesserung des Datenschutzes stets für die Unternehmens- oder Behördenleitung tätig ist. Im Außenverhältnis ist nur das Unternehmen bzw. die Behörde als Ganzes in der Pflicht, und etwaige Verstöße

gegen die datenschutzrechtlichen Vorschriften sind zunächst und vor allem der Leitung zuzurechnen. Zu dieser muss der interne Datenschutzbeauftragte ein Vertrauensverhältnis aufbauen; er kann letztlich nur dann erfolgreich wirken, wenn die Unternehmens- oder Behördenleitung sich seinen Vorschlägen anschließt oder wenn die Aufsichtsbehörde sie dazu zwingt.

Schließlich ist darauf hinzuweisen, dass auch die **Betroffenen** selbst stärker zur Durchsetzung des Datenschutzrechts beitragen könnten, wenn sie ohne allzu große Hürden Sammelklagen erheben könnten oder wenn entsprechende Verbände (Verbraucherschutzvereine usw.) zu gemeinsamen Klagen auf Unterlassung ermächtigt würden. Vorschläge hierzu (Änderung des Unterlassungsklagegesetzes) sind in der Diskussion.

2. Informationspflicht bei „Datenpannen“

Um Schäden zu vermeiden, die infolge rechtswidriger Datenverarbeitung eintreten können, ist eine Pflicht zur Information über derartige Vorgänge sinnvoll. Die neue Vorschrift des § 42a BDSG ist daher im Ansatz gerechtfertigt. Wichtig ist freilich, dass es bei der Voraussetzung „drohende schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen der Betroffenen“ bleibt. Eine Informationspflicht, die nicht der Verhütung von Nachteilen dient, sondern nur die verantwortliche Stelle „an den Pranger stellen“ soll, ist abzulehnen. Sie würde mehr Ärger, vor allem überflüssige Aufregung verursachen als dass sie nutzen würde. Die Streichungsbitte des Bundesrates (Stellungnahme Nr. 19) sollte daher abgelehnt werden. Wenn der Bundesrat meint, die Interessen der Betroffenen seien nicht gefährdet, wenn ein Schaden wieder rückgängig gemacht werden kann (Beispiel: Widerruf unberechtigter Abbuchungen im Lastschriftenverfahren), so interpretiert er den Tatbestand zu eng.

Zuzustimmen ist jedoch der Forderung des Bundesrates (Nr. 20), die allzu detaillierte Vorschrift in § 42a Satz 5 über die Form der öffentlichen Mitteilung zu streichen.

3. Erweiterung der Ordnungswidrigkeiten-Tatbestände und Erhöhung der Bußgelder?

Die Erweiterung der Bußgeldtatbestände, wie sie verschiedentlich vorgeschlagen wird (u.a. Bundesrats-Stellungnahme Nr. 22, 23, 24, 25), ist vertretbar, soweit dadurch Lücken von einiger Erheblichkeit geschlossen werden sollen. Insgesamt aber sollte von Ordnungswidrigkeitsverfahren und vor allem von der Androhung hoher Bußgelder nicht zuviel erwartet werden. Da viele Rechtsverstöße auf Unklarheiten über die Rechtslage beruhen, die ihrerseits vielfach durch zu generelle Gesetzesformulierungen verursacht sind, ist die möglichst genaue Festlegung der Pflichten der Datenverarbeiter wichtiger als die Komplettierung der Sanktionsnormen. Die Bußgeldrahmen werden von den Gerichten ohnehin nicht ausgeschöpft.

IV. Schlussbemerkung

1. Zum Stellenwert der Datenschutz-„Skandale“

Die Rechtsnormen über den Datenschutz werden umso sicherer wirken, je genauer sie der **Risikolage** in dem jeweiligen Bereich entsprechen. Um adäquate und weitgehend akzeptierte Regelungen zu schaffen, bedarf der Gesetzgeber einer zuverlässigen Analyse der jeweiligen Sachlage und ihrer voraussichtlichen Entwicklung; die Normen sollten auf einer sorgfältigen Abwägung der gegebenen und zu erwartenden Vor- und Nachteile beruhen. An diesen Voraussetzungen fehlt es teilweise in der aktuellen Diskussion. Die Risiken werden nur ganz grob eingeschätzt – manchmal bagatellisiert, manchmal übertrieben, meist undifferenziert über einen Leisten geschlagen.

Dies gilt besonders für die Wahrnehmung der Datenschutz-„Skandale“ der letzten Zeit. Berechtigte Empörung hat ausgelöst, dass in großem Maße Adressen und Telefonnummern für belästigende telefonische Werbung genutzt wurden, dass dabei leichtgläubige und unbeholfene Menschen zu unnützen Verträgen überredet wurden und dass sogar telefonische Vertragsschlüsse vorgetäuscht wurden. Dazu kam der Missbrauch von Angaben über Kontoverbindungen zu unbefugten Abbuchungen und Lastschriften. Diese Handlungen waren und sind rechtswidrig und ganz überwiegend bereits nach anderen als datenschutzrechtlichen Vorschriften, insbesondere durch § 7 UWG ausdrücklich verboten, z,T. strafbar oder bußgeldbewehrt. Änderungen des Datenschutzrechts können insofern nur unterstützende Wirkung haben, indem sie die Gelegenheiten zu solchen Taten verringern.

Wenn der Gesetzgeber sich dieser Aufgabe annimmt, darf er nicht das Kind mit dem Bade ausschütten. Er muss vielmehr die Interessenlage in Bezug auf alle in Betracht kommenden Verhaltensweisen analysieren und muss es vermeiden, sozialadäquate Handlungsformen ebenso einzuschränken oder zu erschweren wie die rechtswidrigen Handlungen. Tatsächlich besteht weithin Unklarheit über die konkreten **Nachteile,** die den Betroffenen schon durch die Verarbeitung ihrer Daten entstehen. Häufig wird nur argumentiert, es gebe ein „schutzwürdiges Interesse der Betroffenen am Ausschluss der Verarbeitung oder Nutzung ihrer personenbezogenen Daten“. Worin dieses schutzwürdige Interesse besteht, wird nicht erklärt; allenfalls wird gesagt, man wolle die Bürger vor verstopften Briefkästen schützen – eine Form staatlicher Fürsorge, die jedenfalls keinen gesetzgeberischen und administrativen Aufwand rechtfertigt.

2. Selbstbestimmung über die „eigenen“ Daten?

Anstelle wahrnehmbarer Veränderungen in der Rechtssphäre der Betroffenen wird von den Befürwortern eines „besseren“ Datenschutzes auf die „Selbstbestimmung des Bürgers über seine Daten“ verwiesen. Damit wird ein hochrangiges Prinzip angesprochen. In der volkstümlichen Form „Meine Daten gehören mir“ hat auch die Fraktion BÜNDNIS 90/DIE GRÜNEN dieses Prinzip zur Grundlage ihrer

datenschutzpolitischen Forderungen gewählt.[8] Schon im Volkszählungs-Urteil des Bundesverfassungsgerichts[9] ist demgegenüber dargelegt worden, dass eigentumsrechtliche Vorstellungen dem Gegenstand „personenbezogene Daten“ nicht gerecht werden können:

> „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 Betroffenen allein zugeordnet werden kann.“

Die Beschränkungen des „Rechts auf informationelle Selbstbestimmung“, die der Gesetzgeber geschaffen hat, sind wesentlich zahlreicher und weiterreichend als der Bereich des verbotenen Umgangs mit personenbezogenen Daten. Allein die Generalklauseln des BDSG enthalten erheblich mehr Erlaubnisse als Verbote, auch wenn in § 4 Abs. 1 das Gegenteil formuliert zu sein scheint. Niemand kann heute wirklich über „seine“ Daten frei bestimmen – es sei denn, er wolle sich wie Robinson auf eine einsame Insel und damit aus allen sozialen Kontakten zurückziehen. Dass für wirklich freiwillige Datenverwendung nur wenig Raum geblieben ist, folgt auch aus den Grundrechten selbst, nämlich den Entfaltungsrechten verschiedener Art (insbesondere Art. 2 Abs. 1, Art. 5, 12 und 14 GG), also z.B. aus der Freiheit der Individuen sich zu informieren und auf dieser Grundlage erwerbstätig zu sein, Rechtsgeschäfte abzuschließen oder ihr Eigentum zu verwalten. Wenn der Gesetzgeber sich der Materie „Datenerhebung, -verarbeitung und -nutzung“ annimmt, sind daher Abwägungen zwischen konfligierenden Interessen unvermeidlich, und der Satz „Meine Daten gehören mir“ gibt dafür keine Richtlinie her.

Wenn ein unerreichbarer Zustand zum Rechtsprinzip erklärt wird, werden bei den Bürgern falsche Erwartungen geweckt. Selbstbestimmung muss immer dort gelten und kann nur dort gelten, wo die freie Wahl zwischen mehreren Handlungsmöglichkeiten tatsächlich zu unterschiedlichen Folgen führt. Wenn nur virtuelle Folgen eintreten können, wird Selbstbestimmung zum Selbstzweck. Die Bürger, die mehr erwarten, werden bei nächster Gelegenheit enttäuscht.

3. Unterschied zu anderen Bereichen der Datenverarbeitung

Die besagte Unklarheit darüber, welche Folgen eigentlich durch eine strengere Regelung verhindert werden sollen, begründet den Unterschied zu anderen Bereichen der Datenschutzdebatte. Bei der Verwendung von Scoring-Verfahren zur Kreditwürdigkeitsprüfung, bei der Telekommunikationsüberwachung (die es, wie man kürzlich an aufsehenerregenden Beispielen lernen konnte, im privaten wie im öffentlichen Bereich gibt) und besonders bei der nunmehr im BKA-Gesetz ermöglichten heimlichen Computer-Infiltration ist die Risikolage klar: In solchen Zusammenhängen begründet jede falsche oder nur ungenaue Information einen Nachteil, gegen den das Gesetz schützen sollte, z.B. die Ablehnung eines Kredites, den Verdacht einer Straftat oder einen sonstigen Vorwurf, z.B. arbeitsrechtlicher Art, und in weiten Bereichen der gezielten Überwachung von Individuen ist sogar die

[8] Antrag in Drs. 16/10216 v. 12.9.2008
[9] BVerfGE 65, 1 (43 f.).

Sammlung und Auswertung richtiger Daten unangemessen, weil der Staat und die Unternehmen dadurch Angaben über die Betroffenen erfahren, auf deren Grundlage irgendwelche belastenden oder störenden Konsequenzen gezogen werden können. Es ist aber unrealistisch, vor der Tatsache die Augen zu schließen, dass es auch solche Formen von Datenverarbeitung gibt, die den Betroffenen keine Nachteile zufügen.

Grundsätzlich ist zu empfehlen, wie alles andere Recht auch den Datenschutz jeweils so zu gestalten, dass unerwünschte Handlungen möglichst *zielgenau* verhindert, erwünschte Verhaltensweisen aber so wenig wie möglich behindert werden. Das ist mit Regelungen, die „für alle die gleichen Rechte und Pflichten“[10] konstituieren, nicht zu erreichen, sondern nur mit einer Kombination allgemeiner Grundsätze (einschließlich allgemeiner subjektiver Rechte) und *bereichsspezifischer* Einzelvorschriften. Denn Datenschutz ist Annex zu den Sachmaterien und sollte sich von diesen nicht zu weit entfernen. Deshalb ist der Gedanke, ein allgemeines Datenschutzgesetzbuch zu schaffen, skeptisch zu beurteilen. Wirksamen Datenschutz wird es nur geben, wenn hinreichend differenziert wird, wie auch sonst die Kunst von Rechtsetzern wie Rechtsanwendern darin besteht, richtig zu unterscheiden: „Bene iudicat, qui distinguit“.[11]

[10] So der Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN Drs. 16/10216 zu I. 2. Übrigens erwägen auch diese Autoren die Schaffung von Sondervorschriften „zu Gunsten besonders schutzbedürftiger Gruppen“, „beispielsweise im Arbeitnehmerdatenschutz oder im Verbraucherdatenschutz“.

[11] Detlef Liebs (Hrsg.), Lateinische Rechtsregeln und Rechtssprichwörter, 1982, S. 33.