Prof. Dr. Ralf B. Abel

Innenausschuss
A-Drs. 16(4)176

Schriftliche Stellungnahme
für die Anhörung des Innenausschusses des Deutschen Bundestages am 5. März 2007

zur Thematik

„Modernisierung des Datenschutzes“

Vorbemerkung:

Mit Blick darauf, dass vier der acht anzuhörenden Sachverständigen Datenschutzbeauftragte des öffentlichen Bereichs sind, wird in dieser Stellungnahme in erster Linie der nicht-öffentliche Bereich angesprochen.

Zum Themenkreis 1: Modernisierung des Datenschutzes

1. Grundsätzliches

Struktur des Datenschutzrechts

In der heutigen Informationsgesellschaft sind drei Tendenzen bestimmend. Zum einen ist es der nahezu sämtliche Lebensbereiche erfassende Einsatz EDV-basierter Technik („Ubiquitous Computing“), zum anderen die immer dichtere Vernetzung der einzelnen Systeme und zum dritten die Fähigkeit, die in solchen dezentral-vernetzten Systemen vorhandenen Daten aufzufinden, zu verfolgen, zu analysieren und auszuwerten. Die Nutzung, aber auch schon das bloße Vorhandensein

dieser technologischen Möglichkeiten kann eine Gefährdung individueller Persönlichkeitsrechte in Form einer nahezu totalen Kontrolle über das Verhalten jedes Einzelnen ermöglichen.

Bundes- und Landesgesetzgeber haben versucht, derartigen Gefährdungen durch zahlreiche datenschutzrechtliche Regelungen entgegenzuwirken. Dabei steht der Gesetzgeber im Spannungsfeld zwischen dem gewünschten Schutz des informationellen Selbstbestimmungsrechts einerseits und der Meinungs- und Informationsfreiheit andererseits. Bei beiden handelt es sich um besonders hochwertige Grundrechte in einer freiheitlich-demokratischen Gesellschaft. Das BDSG als Grundregel des Datenschutzes und eine Vielzahl bereichsspezifischer Vorschriften versuchen diese von Verfassungs wegen gebotene Güterabwägung auf der Ebene des einfachen Rechts jeweils umzusetzen. Der dabei oft unvermeidlich hohe Abstraktionsgrad wird freilich von nicht wenigen Stimmen als zu unklar und zu schwammig bemängelt. Andererseits führt die Verwendung unbestimmter Rechtsbegriffe und die gesetzliche Verpflichtung zur Güterabwägung im Einzelfall auch dazu, dass neue Sachverhalte bzw. neue technische Entwicklungen unter die bestehenden Vorschriften subsumiert werden können und es nicht ständig neuer Einzelvorschriften bedarf. Ein gutes Beispiel dafür bildet das BGB, das bei seiner Entstehung wegen seines hohen Abstraktionsgrades vielfach gescholten, dennoch oder gerade deshalb der für seine Schöpfer völlig unvorhersehbaren Rechtsentwicklung im 20.Jahrhundert gewachsen war und weiterhin ist. Demzufolge kann und darf „Modernisierung“ des Datenschutzrechtes nicht bedeuten, dass die bestehenden und in ihren Grundzügen bewährten gesetzlichen Lösungen durch eine immer unüberschaubarer werdende Vielzahl von einzelfallbezogenen Rechtsvorschriften um- oder überwuchert werden. Dies widerspräche auch dem gesetzgeberischen Ziel der Normenklarheit.

Vielmehr erscheint es geboten, die Grundzüge des geltenden Datenschutzrechtes nur dort, wo dies im Interesse einer klaren und einheitlichen Rechtsanwendung unvermeidlich ist, zu verdeutlichen. Ebenso, wie die Straßenverkehrsordnung für die Millionenzahl von Einzelvorgängen beim Straßenverkehr einen überschaubaren Kanon einzuhaltender Regeln geschaffen hat, sollte das Datenschutzrecht auch in Zukunft aus den allgemeinen Bestimmungen des BDSG und bereichsspezifischen Regelungen bestehen, die ihrerseits durch Selbstregulierung im Wege individueller oder verbandlicher Regelungen im Sinne von § 38 a BDSG ergänzt werden.

Verbesserungsmöglichkeiten

Aus der Sicht des Unterzeichners ließe sich dabei an folgende Verbesserungen denken:

- Effektivere institutionelle Vorkehrungen. Darunter fällt nicht nur die Möglichkeit der Zertifizierung von Produkten oder Verfahren, sondern auch die Verbesserung der Stellung und Qualifizierung betrieblicher und behördlicher Datenschutzbeauftragter sowie eine nachhaltige Ermöglichung und Förderung betrieblicher und verbandlicher Selbstregulierung. Zwar findet sich in § 38a BDSG bereits eine entsprechende gesetzliche Regelung. Sie hat jedoch in der bisherigen Praxis kaum Bedeutung erlangt, was von Beteiligten mit der restriktiven Haltung der Aufsichtsbehörden gegenüber der Erteilung der dort vorgesehenen Konformitätserklärungen erklärt wird.

- Ergänzende zivilrechtliche Instrumente. In diesem Zusammenhang wäre an eine Konkretisierung des Wettbewerbsrechts dahingehend zu denken, dass datenschutzrechtliche Verstöße und auch das Unterlassen datenschutzrechtlich er-

forderlicher Maßnahmen als unlauterer Vorsprung durch Rechtsbruch anzusehen und mit dem wettbewerbsrechtlichen Instrumentarium zu ahnden wäre. Eine solche Bestimmung läge nicht zuletzt im Interesse des redlichen Geschäftsverkehrs.

- Eine Verschärfung der Sanktionen, insbesondere im Bereich der Ordnungswidrigkeiten. Es ist insbesondere für redliche und sich gesetzestreu verhaltende Unternehmen schwer einzusehen, wenn Wettbewerber, die auf datenschutzrechtliche Aufwendungen verzichten, dadurch ungerechtfertigte wirtschaftliche Vorteile erhalten, die auch durch eine Sanktion nicht geschmälert werden.

- Die rasche Beseitigung von Vollzugsdefiziten innerhalb der EU. Obwohl der Datenschutz EU-weit materiellrechtlich einheitlich geregelt ist, werden die in den Mitgliedstaaten bestehenden Gesetze in teilweise sehr unterschiedlicher Weise vollzogen. Vollzugsdefizite in anderen Ländern können jedoch im Rahmen der internationalen Zusammenarbeit zu einer Benachteiligung deutscher Unternehmen führen, die sich gesetzeskonform verhalten. Insbesondere darf bei international aufgestellten Unternehmen ein niedrigeres Datenschutzniveau bei ausländischen Töchtern nicht zu Wettbewerbsverzerrungen der deutschen Standorte führen. Die bisher von der Kommission ergriffenen Maßnahmen sind zu begrüßen, bedürften aber aus Sicht des Unterzeichners einer Intensivierung.

- Eine Vereinheitlichung bzw. Anpassung der Nomenklatur und Fortschreibung der verwendeten Legaldefinitionen. So könnte klargestellt werden, dass Voice over IP (VoIP) dem

TKG unterfällt und damit das Fernmeldegeheimnis auch bei Anwendung dieser Technologie zu wahren ist.

Zusammenfassend lässt sich das Datenschutzrecht nach Ansicht des Unterzeichners weder in einem „großen Wurf“ noch durch eine unüberschaubare Vielzahl detaillierter gesetzlicher Vorschriften modernisieren. Ein solches Vorgehen widerspräche auch dem im Koalitionsvertrag vereinbarten Ziel des Bürokratieabbaus. Die nachfolgenden Überlegungen setzen daher auf eine pragmatische, sachverhaltsorientierte Fortschreibung der bestehenden Bestimmungen.

Zum Themenkreis 2: Datenschutz-Audit (Anträge FDP, Bündnis 90/Die Grünen)

1. Antrag: Erlaß eines Ausführungsgesetzes zu § 9 a BDSG

a) Beim Audit-Verfahren muss aus kompetenzrechtlichen Gründen differenziert werden zwischen dem öffentlichen und dem nichtöffentlichen Bereich. Für die Landesverwaltungen liegt die Kompetenz für die Auditierung bei den Ländern, die in einigen Fällen (Schleswig-Holstein, Mecklemburg-Vorpommern) bereits davon Gebrauch gemacht haben. Grundsätzlich sind einheitliche Bedingungen wünschenswert, können aber nach Einschätzung des Unterzeichners im öffentlichen Bereich der Länder nicht durch Bundesgesetz vorgegeben werden. Hier wäre allenfalls eine Bund-Länder-Vereinbarung, etwa über die gegenseitige Anerkennung von Zertifikaten, denkbar.

b) Die Feststellung ist richtig, dass die Bestimmungen des § 9a BDSG bisher leer laufen. Ein Datenschutz-Audit-Verfahren kann, ähnlich wie beim Umwelt-Audit oder bei Zertifizierungsverfahren

in anderen Bereichen, zu einer Verbesserung von Datenschutz und Datensicherheit beitragen. Es stellt sich allerdings die Frage, ob es dazu so, wie bisher in § 9 a BDSG vorgesehen, der äußeren Form eines Parlamentsgesetzes bedarf. Es handelt sich der Sache nach um technische Regelungen und Verfahren, etwa bei der Gutachterbestellung oder der Durchführung der Zertifizierung. Diese sind, unabhängig von ihrer Ausgestaltung im Einzelnen (dazu unten) abhängig von technisch-organisatorischen Entwicklungen und dem Wandel der Erkenntnisse. Üblicherweise werden derartige Einzelheiten in Rechtsverordnungen geregelt (als Vergleich könnte das Verhältnis von Straßenverkehrsgesetz zur Straßenverkehrsordnung dienen). Rechtsverordnungen dienen in erster Linie der Entlastung des Parlaments, das weder dazu berufen noch aus zeitlichen und sachlichen Gründen in der Lage ist, alle Einzelheiten, insbesondere solche mehr technischer Art, selbst zu regeln. Ferner ermöglicht die Rechtsverordnung eine rasche Anpassung an sich ändernde Verhältnisse, was häufig gerade bei technischen Einzelfragen notwendig ist. Demzufolge wäre zu überlegen, § 9 a BDSG zu ändern und eine Verordnungsermächtigung aufzunehmen. Die Regelung eines Audit-Verfahrens in einer Rechtsverordnung führt zu einer besseren Steuerungsfähigkeit und lässt eine höhere Detaillierung sowie eine schnellere Anpassung an neuere Erkenntnisse zu. Gerade der letzte Gesichtspunkt ist von Bedeutung, weil es mit datenschutzrechtlichen Audit-Verfahren bisher erst wenige Erkenntnisse und Erfahrungen gibt.

Die Regelung des Datenschutz-Audits in Form einer Rechtsverordnung kommt damit auch dem Anliegen in Ziffer 5 des Antrages von Bündnis 90/Die Grünen („ebenso effiziente wie wenig bürokratische Regelungen“) entgegen.

Auch die Länder Schleswig-Holstein und Mecklenburg - Vorpommern haben für das Audit den Weg der Rechtsverordnung gewählt.

c) Eine neue in § 9 a BDSG aufzunehmende Verordnungsermächtigung könnte sich am bestehenden Inhalt der Vorschrift orientieren. Aus rechtssystematischen Gründen sollte die Regelung der Zuständigkeiten im BDSG verbleiben. Hierzu bieten sich als Wurzelinstanz eine Zuständigkeit des BSI und/oder, für Scoring-Verfahren im Kreditbereich, die BAFin an. Insbesondere beim BSI sind hervorragende Kompetenzen gebündelt, vor allem im organisatorisch-technischen Bereich. Demgegenüber würde die Zuweisung dieser Aufgabe an den BfDI zu einer erheblichen zusätzlichen Belastung dieser ohnehin mit einem im Verhältnis zur Personalausstattung erheblichen Aufgabenvolumen belasteten Behörde führen, wobei angesichts der allgemeinen Haushaltslage eine Personalaufstockung kaum in Betracht kommen dürfte. Ebenso wenig erscheint es realistisch, den Aufsichtsbehörden bzw. Datenschutzbeauftragten der Länder derartige zentrale Funktionen durch Bundesgesetz zuweisen zu wollen.

Gegen eine Übertragung der Zertifizierung auf die Datenschutz-Aufsichtsbehörden spricht auch der Umstand, dass diesen die unabhängige Kontrolle obliegt. Zertifizierung und Kontrolle sollten nicht in einer Hand liegen, zumal auf diese Weise auch die Sachverständigen, die das Audit durchführen, ihrerseits einer Qualitätskontrolle durch unabhängige staatliche Instanzen unterliegen.

d) Bei der Auditierung muss grundsätzlich zwischen Produktaudit und Verfahrensaudit unterschieden werden. Ein freiwilliges Produktaudit im nicht-öffentlichen Bereich erscheint sinnvoll. Bei der Entwicklung von Standards und Methoden kann auf die Erfahrun-

gen von Datenschutz-Aufsichtsbehörden einzelner Länder im nicht-öffentlichen Bereich zurückgegriffen werden.

Ob und in welchem Umfange ein Verfahrens-Audit für den nicht-öffentlichen Bereich, d. h. für Unternehmen Sinn macht, lässt sich aus Sicht des Unterzeichners derzeit nicht abschließend beurteilen. Gegenüber den Vorteilen einer Zertifizierung – wie zum Beispiel dem mit einem Zertifikat möglicherweise verbundenen Marketingeffekt – werden auch vielfach Nachteile gesehen, und zwar vor allem durch die Belastung mit bürokratischem Aufwand und nicht unerheblichen Kosten. Ein auf ein Verfahren bezogenes Zertifikat betrifft stets nur eine Momentaufnahme. Es ist jedoch üblich, dass die DV-technischen Verfahren in der Wirtschaft kontinuierlich an Marktveränderungen, technologische Entwicklungen, gesetzliche Erfordernisse, sich verändernde Unternehmensstrukturen u. dgl. angepasst und damit verändert werden. Ein solcher „immerwährender Veränderungsprozess“ entzieht sich vielfach einer verlässlichen Zertifizierung. Wenn und soweit im nicht-öffentlichen Bereich ein Bedürfnis für die Zertifizierung eines Verfahrens besteht, bestehen für eine gesetzliche bzw. untergesetzliche Regelung derzeit keine hinreichend verbindlichen Standards. Daher sollte von einer normativen Regelung in Bezug auf Verfahren jedenfalls zum derzeitigen Zeitpunkt abgesehen werden.

Einen Sonderfall könnte ein Audit für Auftrags-Datenverarbeiter im Sinne von § 11 BDSG darstellen, und zwar dadurch, dass ein zertifizierter Betrieb durch die Erteilung des Zertifikats die nach § 11 BDSG erforderliche Gewähr für datenschutzgerechte Verfahren bieten könnte. Allerdings ist auch diese Überlegung nicht gänzlich überzeugend. § 11 BDSG erfordert zu Recht eine individuell auf das jeweilige Auftragsverhältnis bezogene und vom Auftraggeber nachzuprüfende Vereinbarung, die nicht durch das bloße

Vorhandensein eines Zertifikats ersetzt werden kann. EDV-technische Verfahren sind in den wenigsten Fällen standardisiert bzw. standardisierbar, vielmehr umfasst die Auftragsverarbeitung die gesamte Bandbreite EDV-technischer und organisatorischer Anwendungen (z. B. sog. „Letter-Shops“ im Direktmarketing, ausgelagerte Personalabteilungen, Kundenverwaltung, Forderungseinzug und Forderungsmanagement u. dgl.). Zumindest zum heutigen Zeitpunkt fehlt es an Erfahrungen, um verlässliche normative Vorgaben für ein Verfahrens-Audit bei der Auftragsdatenverarbeitung machen zu können.

Hinzu kommt der Umstand, dass die datenschutzrechtliche Zulässigkeit von Verfahren einer rechtlichen Bewertung und damit vielfältigen Abwägungsprozessen unterliegen. Derartige rechtliche Einschätzungen entziehen sich grundsätzlichlich den Möglichkeiten eines Audit. Die Feststellung rechtlicher Verpflichtungen ist vielmehr Angelegenheit der Aufsichtsbehörden und ggf. Rechtsprechung. Es erscheint ausgeschlossen, dass Auditoren bzw. Zertifizierungsinstitutionen eine verbindliche Auslegung von Rechtsnormen vornehmen können, an die möglicherweise dann auch Aufsichtsbehörden und Gerichte gebunden wären.

2. Notwendigkeit einer verbesserten Transparenz

Das Anliegen ist zu befürworten. Wie bereits oben erläutert, wird es jedoch zumindest zum heutigen Zeitpunkt nur für Produkte anwendbar sein, etwa durch die Erteilung eines Gütesiegels. Allerdings gilt es auch zu bedenken, dass sich zahlreiche Produkte und Verfahren, die von der Wirtschaft bundesweit angeboten werden, wegen ihrer Anwendungsvielfalt in der Praxis nicht zu einer standardisierten Auditierung eignen. Es muss daher sichergestellt werden, dass es nicht zu

Wettbewerbsbeeinträchtigungen kommt, die darauf beruhen, dass die verschiedenen Anwendungen unterschiedlich „gütesiegelfähig“ sind, ein Umstand, den der Verbraucher in aller Regel nicht zu erkennen vermag.

Wenig plausibel ist die Forderung, einen über den gesetzlichen Mindeststandard hinausgehenden Datenschutz nachweisen können zu sollen. Dies setzt nämlich die Annahme voraus, dass der gesetzliche Mindeststandard „eigentlich“ keinen ausreichenden Persönlichkeitsschutz mit sich bringe. Davon kann aber nicht ausgegangen werden. In Umsetzung des Volkszählungsurteils des BVerfG und der Europäischen Datenschutz-Richtlinie wird durch die deutsche Gesetzgebung die Wahrung der Persönlichkeitsrechte sichergestellt. Wo dies nicht der Fall sein sollte, sind etwaige Umsetzungsdefizite oder Gesetzeslücken durch Aufsichtsbehörden, Rechtsprechung und ggf. den Gesetzgeber zu beseitigen. Die gesetzlichen Anforderungen sind damit keine Mindestanforderungen, sondern sie entsprechen dem jeweiligen Schutzzweck und Schutzbedürfnis. Der Vorschlag erscheint daher nicht sinnvoll und auch nicht in die Praxis umsetzbar.

3. Mitwirkung der betrieblichen Datenschutzbeauftragten

Die normative Verankerung einer Verpflichtung, den betrieblichen Datenschutzbeauftragten einzubeziehen, führt zu einer Überregulierung und kann daher nicht befürwortet werden. Es bietet sich naturgemäß an, den betrieblichen Datenschutzbeauftragten bei einer einschlägigen Auditierung hinzuziehen. Wie, wann und in welchem Umfang dies geschieht, ist jedoch Sache der Organisationsgewalt im Unternehmen und muss es auch bleiben. Nicht in jedem Falle macht die Hinzuziehung des betrieblichen Datenschutzbeauftragten Sinn: Bei einem Produktaudit beispielsweise geht es um die datenschutzgerechte

Gestaltung des Produktes, also der Anwendung beim Kunden. Über dessen Erfordernisse wird der betriebliche DSB des Herstellers keineswegs immer informiert sein (können).

4. Konzept für weitere Maßnahmen

Die Erarbeitung eines solchen Konzeptes ist zu begrüßen. Im nichtöffentlichen Bereich besteht durchaus ein Bedürfnis nach einheitlichen Standards. Dies wären jedoch nicht nur nationale, sondern richtigerweise internationale oder zumindest europäische Standards, um Wettbewerbsverzerrungen zu Lasten deutscher Anbieter entgegenzuwirken. Zu denken wäre auch an eine Norm entsprechend den DIN EN ISO 9000 ff..

Zum Themenkreis 3: Scoring

Allgemeines

Dem Anliegen, wonach der Einzelne davor geschützt werden soll, durch ein elektronisches DV-System zu Unrecht wirtschaftliche Nachteile zu erleiden, ist grundsätzlich zuzustimmen. Die dazu unterbreiteten Vorschläge (Antrag Bündnis 90/Die Grünen vom 15.02.2006) sind eine hilfreiche Anregung, über die Problematik nachzudenken.

Man muss indessen davon ausgehen, dass Scoring-Systeme heute in der Wirtschaft ein unverzichtbares Instrument bilden, um – insbesondere bei Massengeschäften – die vermutlichen Interessen und das vermutliche Verhalten potentieller Kunden sachgerecht einschätzen zu können, ohne dass dazu die Erhebung konkreter personenbezogener

Daten oder die Bildung individuell-konkreter Profile erforderlich ist. Da es sich um bloß statistische Wahrscheinlichkeiten handelt, sind Transparenz und die leicht und für jedermann realisierbare Möglichkeit, Fehleinschätzungen korrigieren zu können, ein unverzichtbares Korrelat der technologisch-organisatorischen Handlungsmöglichkeiten.

Zu den Anträgen im Einzelnen:

1. Begrenzung und Regelung von Auskunftssystemen

a) Der Wunsch nach einer gesetzliche Regelung von Auskunftssystemen, wie sie der Antrag sehr allgemein formuliert, bedeutet einen sehr erheblichen und nachhaltigen Eingriff in die Informationsverarbeitung bei Einzelnen und bei Unternehmen. Das Recht, sich zu informieren, aus diesen Informationen Schlüsse zu ziehen und sich danach zu verhalten, kurz: die Anwendung und Verwertung von Wissen, gehören zu den elementaren Bürgerrechten, die in erster Linie in Art. 5 GG und darüber hinaus auch in Art. 14 GG als Teil der unternehmerischen Betätigungsfreiheit und auch der Vertragsfreiheit verfassungsrechtlich gewährleistet werden. Jeder gesetzliche Eingriff in diese Grundrechte bedarf der Abwägung – hier: mit dem Grundrecht auf informationelle Selbstbestimmung – und der Verhältnismäßigkeit. Die für den Bereich der Auskunftssysteme anwendbaren Vorschriften des BDSG erfüllen diese Voraussetzungen, und zwar insbesondere dadurch, dass sie in diesem Bereich eine Güterabwägung zwischen berechtigten Interessen der Datenhalter und Datenempfänger einerseits und den berechtigten Ausschlussinteressen des Betroffenen andererseits erfordern. § 6 a BDSG enthält eine den verfassungsrechtlichen Voraussetzungen

sowie den europarechtlichen Vorgaben entsprechende Regelung für automatisierte Einzelentscheidungen.

Diese Regelungen decken die allgemeinen Auskunftsverfahren ebenso ab, wie die im Zusammenhang mit Scoring-Verfahren auftretenden Rechtsfragen (dazu im Einzelnen: Abel, RDV 2006, S. 108 ff.).

Ferner ist eine „Begrenzung“ im geltenden Recht bereits vorhanden, und zwar durch die Berücksichtigung des Rechts auf informationelle Selbstbestimmung des Betroffenen bei der vom BDSG gebotenen Abwägung (z. B. in § 28 Abs. 1 Nr. 2 und Abs. 2, 3, 6-9, 29 BDSG). Der Verweis auf unbestimmte Rechtsbegriffe und Güterabwägungsprozesse im Einzelfall mag der Vorstellung von „Normenklarheit“ im Sinne einfacher, immer gleicher Regeln widersprechen, stellt aber nach Auffassung des Unterzeichners die einzige handhabbare Möglichkeit dar, der Vielfalt der konkreten Verarbeitungsprozesse vor dem Hintergrund des Grundrechts der Informationsfreiheit einerseits und der informationellen Selbstbestimmung andererseits gerecht zu werden. Eine gesetzliche Festlegung technischer Einzelheiten würde zudem wegen der hohen Entwicklungsdynamik EDV-basierter Expertensysteme schon nach kurzer Zeit anzupassen bzw. nachzubessern sein.

b) Zudem ist zu berücksichtigen, dass es am Markt sehr unterschiedliche Scoring-Systeme und eine Vielfalt von Anwendungen gibt. So muß beispielsweise unterschieden werden zwischen internem und externem Scoring, zwischen allgemeinen Scores für bestimmte Branchen oder Geschäftsfelder (z. B. Geschäftsfeld „Kfz-Versicherung“) und individuell entwickelten Scores für einzelne Unternehmen oder Anwendungen. So gibt es Scores für Werbe- und Marketingzwecke, die mögliche Kunden nach dem Interesse

für bestimmte Produkte oder Produktgruppen „heraussuchen“, aber auch „Fraud-Scores“, die eine Betrugswahrscheinlichkeit zu identifizieren vermögen. Dazu ein Beispiel: Bei einem der großen deutschen Versender werden Score-Werte zwischen 1 (schlechtester Wert) und 1000 (bester Wert) gebildet. Im Jahre 2006 waren unter den Kunden mit einem Score-Wert bis 499 nur 5,03 % sog. „Gute“. 54,1 % der Kundenbeziehungen dieser Gruppe mussten ausgebucht oder ins Inkasso abgegeben werden. Von der Gruppe mit Score-Werten ab 560 galten hingegen 73,78 % als „gut“, zu einer Ausbuchung oder Abgabe ins Inkasso kam es nur noch in 5,27 % der Fälle.

Derart unterschiedliche Scoring-Verfahren, die zudem kontinuierlich den veränderten Bedürfnissen und Erkenntnissen angepasst werden, entziehen sich einer ins Detail gehenden gesetzlichen Regelung.

c) Die Forderung, dass Scoring-Systeme nur valide statistische Methoden verwenden dürfen, ist eine unabdingbare Voraussetzung für die Zulässigkeit solcher Systeme. Auch sie bedarf freilich keiner neuen gesetzlichen Regelung, denn die Verwendung wissenschaftlich nicht abgesicherter oder unseriöser Verfahren würde ein schutzwürdiges Ausschlussinteresse des Betroffenen an dieser Verarbeitung etwa im Sinne von § 28 Abs. 1 Nr. 2 und Abs. 2, § 29 Abs. 1 und 2 Nr. 2 BDSG begründen.

Demgegenüber kann der Forderung, durch Gesetz oder Verordnung die einzelnen in Scoring-Verfahren verwendeten Merkmale durch den Gesetz- oder Verordnungsgeber festzulegen, nicht gefolgt werden. Welche Merkmale die Trennschärfe der Score-Werte erhöhen und daher für den jeweiligen (sehr unterschiedlichen) Zweck geeignet sind, lässt sich nur auf mathematisch-statistischem

Wege ermitteln. Nur darauf kann es ankommen. Die Überlegung, einzelne Merkmale gesetzlich auszuschließen, wie es bei § 10 KWG der Fall ist, ist aus diesem Gesichtspunkt heraus mehr als bedenklich. Selbstverständlich muss jede Diskriminierung ausgeschlossen sein. Dies ist aber der Fall, wenn anerkannte wissenschaftliche Methoden zum Einsatz kommen. Diese stellen ausschließlich auf die Trennschärfe für die jeweilige Anwendung ab, also beispielsweise auf die Zahlungsbereitschaft und Zahlungsfähigkeit, ohne nach den Ursachen zu fragen. Da es sich bei Score-Werten um die Zusammenführung verschieden gewichteter Einzelmerkmale handelt, die im Ergebnis auf die jeweilige Anwendung bezogen werden, also beispielsweise auf die Kreditwürdigkeit, erscheint eine Diskriminierung wegen einzelner Merkmale ausgeschlossen.

Umgekehrt sollte berücksichtigt werden, dass bei dem Scoring für Marketing-Zwecke Merkmale wie z. B. der Glaube eine große Rolle spielen können, da es weder wirtschaftlich sinnvoll wäre noch dem erforderlichen Respekt vor Andersgläubigen entspräche, wenn beispielsweise Muslime mit alkoholhaltigen oder auf Schweinefleisch basierenden Produkten beworben würden. Es erscheint daher nicht sachangemessen, die Verwendung bestimmter einzelner Merkmale durch Bundesgesetz festzulegen.

d) Wegen der Vielzahl der möglichen Anwendungen und Bedürfnisse sind Selbstverpflichtungserklärungen (Codes of Conduct) der Hersteller und Anwender von Auskunftssystemen einer gesetzlichen Regelung vorzuziehen. § 38 a BDSG bietet dafür die gesetzliche Grundlage. Allerdings hat sich gezeigt, dass die damit vom Gesetzgeber gewollte Selbstregulierung in der Praxis nicht angewendet wird, weil die vom Gesetz vorgesehene Konformitätserklärung durch die Aufsichtsbehörden von inhaltlichen Forderungen

abhängig gemacht wurden („Mehrwert“), die von den Verfassern solcher Verhaltensregeln als inhaltlich überzogen angesehen wurden. Es wäre zu erwägen, § 38 a BDSG im Hinblick auf eine bessere Handhabbarkeit und bessere Durchsetzung des Gedankens der verbindlichen Selbstregulierung zu konkretisieren.

2. Transparenz

a) Die Forderung nach Transparenz ist grundsätzlich berechtigt. Transparenz ist für die Wahrung des informationellen Selbstbestimmungsrechtes ebenso wie für die Akzeptanz der Systeme unverzichtbar. Gleichermaßen müssen die hinter den Scoring-Systemen stehenden Betriebsgeheimnisse gewahrt werden können. Auch muss vermieden werden, dass eine zu genaue Kenntnis der Systeme dolos handelnde Personen in die Lage versetzt, die Ergebnisse von Scoring-Verfahren zu manipulieren.

b) Nach geltendem Recht besteht ein Auskunftsanspruch des Betroffenen nach § 34 Abs. 1, 2 BDSG. Zu beauskunften sind die zur Person des Betroffenen gespeicherten Daten, und zwar in bestimmten Fällen auch dann, wenn sie weder in einer automatisierten Verarbeitung noch in einer nicht automatisierten Datei gespeichert sind (§ 34 Abs. 2 S. 1 BDSG). Hier bietet sich zur Schaffung besserer Transparenz eine Ergänzung an, etwa um die Formulierung *„… für einzelne Auskunftsfälle selbst oder durch Dritte erzeugt worden sind, ohne auf Dauer gespeichert zu sein“*.

c) § 6 a BDSG erstreckt das Auskunftsrecht nicht nur auf die jeweiligen Daten selbst, sondern auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten. Dass eine Auskunft für den Betroffenen verständlich und nachvollziehbar sein muss, versteht sich von selbst. Die Praxis sieht hier jedoch er-

hebliche Schwierigkeiten bei der konkreten Umsetzung. Am einfachsten dürfte es in dem Fall sein, in dem ein Score-Wert in Form einer Zahl errechnet oder gespeichert wird. Diese Zahl kann in ein Verhältnis zum Bewertungsrahmen gesetzt und in ihrer Bedeutung pauschal erklärt werden (Beispiel: Bei einem Bewertungsrahmen zwischen 1 und 1000 und einer Segmentierung der Gruppen 1 bis 499, 500 bis 550, 551 bis 599, > 599) lässt sich die inhaltliche Bedeutung einer Score-Zahl durchaus erläutern. Neuerdings und wohl zunehmend handelt es sich bei Score-Werten um digitale Zeichenfolgen, die erst beim Anwender in Verbindung mit ergänzenden Informationen einen bestimmten Sinn ergeben. Für den Betroffenen sind derartige Auskünfte nicht sinnvoll. Ebenso wenig wären es Auskünfte über mathematisch-statistische Verfahren. Für den Betroffenen ist es vielmehr entscheidend und auch ausreichend, den wesentlichen Inhalt des Scores bei der konkreten Anwendung in verbaler Form mitgeteilt zu erhalten (Beispiel: „Kunde kommt weniger als Käufer hubraumstarker Fahrzeuge in Betracht“ oder: „Kunde gehört zur Gruppe, die mit …prozentiger Wahrscheinlichkeit den Kredit ordnungsgemäß bedient und zurückführt“). Für den Betroffenen ist daher weniger der logische Aufbau der ihn betreffenden Datenverarbeitung von Bedeutung, sondern das sich auf ihn beziehende Ergebnis.

Die Forderung, die einfließenden Daten und Merkmale sowie ihre Gewichtung bei der Berechnung des Score-Werts zu beauskunften, kollidiert nach Auffassung des Unterzeichners vielfach mit dem Anspruch der Hersteller und Verwender auf Wahrung ihrer Geschäftsgeheimnisse. Vertretbar erscheint das Anliegen dann, wenn sich die Offenlegungspflicht auf die drei entscheidungserheblichsten Merkmale beschränkt, z.B. durch eine Ergänzung des § 6a Abs.3 um folgenden Wortlaut: „*... oder, bei elektronischen Bewer-*

tungssystemen (Scoring), auf die drei für die Scorebildung entscheidenden Merkmale."

Zwar stellt ein Score-Wert eine Gesamtbetrachtung als Inbegriff der Kombination aller eingeflossenen Merkmale dar. In aller Regel lassen sich jedoch, etwa bei Kreditentscheidungen, Hauptmerkmale identifizieren. Für den Betroffenen geht es darum, herauszufinden, ob das von ihm für die jeweilige konkrete Anwendung erzeugte „elektronische Außenbild" auf richtigen oder auf falschen Annahmen beruht. Wenn der Betroffene die Hauptmerkmale kennt, kann er in aller Regel erkennen, ob die Basisdaten richtig oder falsch sind.

d) Vielfach wird die Handhabung der Auskunft über Scoring-Prozesse in den USA als Beispiel und Vorbild herangezogen. Eine Übertragung dieser Maßnahmen in die deutsche Gesetzgebung ist jedoch nicht angezeigt. Sie ist nicht erforderlich und wäre systemfremd, weil es einen wie in Deutschland auf gesetzlicher Grundlage beruhenden umfassenden Schutz der informationellen Selbstbestimmung in den USA nicht gibt. Deshalb speichern und verwerten Kreditauskunfteien Daten über das Kaufverhalten der Betroffenen in einem erheblichen und nach deutschem Datenschutzverständnis ganz unzulässigen Ausmaß. Daher erklärt sich der Umfang der in den USA zu erteilenden Auskünfte. Auf Deutschland lassen sich diese Verhältnisse nicht übertragen.

3. Keine ungerechtfertigte Schlechterstellung aufgrund eines Score-Werts (Antrag Bündnis 90/Die Grünen vom 15.12.2006, Nr. 3)

Das Anliegen, den Betroffenen vor einer unrichtigen Eingruppierung zu schützen, ist im Ansatz berechtigt. Es dient nicht nur dem erforderlichen Schutz der Persönlichkeitsrechte des Betroffenen, sondern auch

dem Interesse der die Score-Werte verwendenden Unternehmen. Jedes Unternehmen möchte möglichst hohe Umsätze erzielen. Daher wäre es kontraproduktiv, wenn potentielle Kunden aufgrund einer sachlich falschen Negativbeurteilung abgelehnt würden. Allerdings kann es Unternehmen nicht verwehrt werden, sich – vor allem im Massen- und Distanzgeschäft – generell-typisierender Einschätzungen zu bedienen, um das eigene Risiko zu verringern, ebenso wie es beispielsweise dem Gesetzgeber verfassungsrechtlich unbedenklich erlaubt ist, Massenvorgänge generell-typisierend zu regeln (z.B. im Steuerrecht).

§ 6 a BDSG gestattet es, automatisierte Einzelentscheidungen zu Lasten des Betroffenen zu fällen, unter der Voraussetzung, dass der Betroffene über diese Vorgehensweise informiert und geeignete Maßnahmen getroffen werden, die die Wahrung der berechtigten Interessen des Betroffenen gewährleisten. Dem Anliegen des Antrags könnte dadurch Rechnung getragen werden, dass § 6 a BDSG ergänzt wird um eine Bestimmung etwa folgenden Inhalts:

> *„Elektronische Bewertungsverfahren (Scoring-Verfahren) sind zulässig, wenn sie im berechtigten Interesse der verantwortlichen Stelle liegen und auf wissenschaftlich anerkannten Methoden beruhen. Die Bestimmungen der Absätze 1 bis 3 gelten sinngemäß.“*

Damit wäre unmissverständlich klargestellt, dass Scoring-Verfahren immer dann zulässig sind, wenn organisatorische Vorkehrungen sicherstellen, dass eine verlässliche Korrektur etwa über unrichtige Scores in zumutbarer Weise möglich sind.

Wie solche Korrektursysteme im Einzelnen aussehen können, lässt sich nicht generalisierend festlegen. Hier bieten sich Ansatzpunkte für branchenspezifische Regelungen im Wege der Selbstregulierung an. Dieser Gedanke könnte durch eine ergänzende Gesetzesbestimmung verdeutlicht werden mit etwa folgendem Inhalt:

„Näheres kann durch Unternehmen, Berufsverbände oder andere Vereinigungen, die bestimmte Gruppen vor verantwortlichen Stellen vertreten, in Form von Verhaltensregeln näher festgelegt werden. § 38 a BDSG gilt sinngemäß."

Zum Themenkreis 3 a: Unternehmensinformationspflicht bei Datenschutzpannen

1. Allgemeines

Der Antrag enthält die sinnvolle Anregung, sich mit der angeschnittenen Thematik intensiver zu befassen. Nach Ansicht des Unterzeichners ist er in der vorliegenden Form jedoch nicht entscheidungsreif. Dazu im Einzelnen:

2. Einzelfragen

a) Zunächst sind zahlreiche Vorfragen zu klären, vor allem die, welche Sachverhalte es im Einzelnen gemeint sein sollen. Datenmissbrauch mit Hilfe rechtswidrig beschaffter personenbezogener Informationen kann in vielfältigen Formen vorkommen. Neben Fällen von „Informationsdiebstahl" durch gefälschte elektronische Identitätsnachweise und Berechtigungen sind Szenarien denkbar wie z.B. der Missbrauch von Gesundheitskarten (etwa in Form einer Behandlung unter fremdem Namen) oder der bereits jetzt häufig zu verzeichnende „virtuelle Diebstahl" von Kreditkarten. Diese unterschiedlichen Fallgestaltungen sind im Hinblick auf Informationspflichten und Haftung nicht mit einer einzigen Regelung zu erfassen. Es müsste zunächst geprüft und danach differenziert werden, ob und bei welchen Fallgruppen welche Probleme auftreten.

Sobald einzelne Problemfelder identifiziert sind, gilt es zu untersuchen, ob und in welchem Umfang das geltende Recht für die einzelnen Fallgruppen bereits Informationspflichten vorsieht und wenn ja, ob diese ausreichen. Die hier angesprochenen DV-Anwendungen dürften in ihrer großen Mehrzahl auf vertraglichen Regelungen beruhen. Damit können sich Informationspflichten aus vertraglichen Haupt- und Nebenpflichten ergeben, und zwar punktuell, jeweils abhängig vom Grad der Rechtsgutgefährdung, etwa im Bereich der Produkthaftpflicht bei Rückrufaktionen.

b) Die zum Vergleich herangezogene US-Gesetzgebung eignet sich nicht als Vorbild. Zum einen bezieht sich der „Security Breach Information Act“ des US-Bundesstaats Kalifornien bezüglich der Informationspflicht keineswegs auf alle personenbezogenen Daten, sondern nur auf den sehr engen Begriff der „Personal Information“. Dazu zählen der Name in Kombination mit u.a. der Sozialversicherungsnummer, der Führerschein- oder Ausweisnummer, ferner die Kontonummer, Kredit- oder Kontokarte mit Zahlfunktion, wiederum in Kombination mit PIN-Nummer oder Passwort, das den Zugang zum Konto des Betroffenen ermöglicht. Die Sozialversicherungsnummer dient in den USA als einheitliches Identifizierungsmerkmal als eine Personenkennziffer, die in Deutschland unzulässig ist. Im übrigen handelt es sich nach deutschem Verständnis entweder um Bankdaten, die dem Bankgeheimnis unterliegen, oder um Datenbestände des öffentlichen Bereichs.

Das amerikanische Recht kennt – anders als die deutsche und europäische Rechtsordnung – keine mit den deutschen Datenschutzbestimmungen vergleichbaren Regelungen. Daher existieren dort weder Datenschutz-Aufsichtsbehörden, datenschutzrechtliche

Straf- und Bußgeldvorschriften noch zivilrechtliche Schadensersatzansprüche wie die in § 7 BDSG oder in § 812 Abs. 2 BGB i. V. m. den datenschutzrechtlichen Verbotsnormen, so dass es dort - systemadäquat- anderer Rechtsnormen bedarf, als dies in Deutschland der Fall ist.. Aus diesem Grunde lässt sich die US-Gesetzgebung nicht auf deutsche Verhältnisse übertragen.

d) Schließlich muss die Auferlegung einer Informationspflicht dem Prinzip der Verhältnismäßigkeit entsprechen. Die Tatsache, dass Diebstahl und Ausspähung eines Notebooks Hunderte oder Tausende von personenbezogenen Daten oder der unberechtigte Zugriff auf größere Datenbanken Hunderttausende oder Millionen von Datensätzen betreffen kann, zeigt die Dimension etwaiger Informationspflichten und damit die Schwierigkeit, die Verhältnismäßigkeit einer gesetzlichen Regelung zu wahren, wenn alle potentiell Betroffenen ungeachtet der im Einzelfall möglicherweise nur geringen Gefährdung mit hohem Aufwand zu informieren wären. In vielen Fällen werden der Aufwand für die Wirtschaft und der Ertrag für den Betroffenen außer Verhältnis stehen.

e) Zu berücksichtigen ist auch die europäische Rechtsentwicklung. Deutsche Insellösungen könnten die bevorstehende Revision des europäischen Rechtsrahmens für die elektronische Kommunikation erschweren, ferner kann es dadurch zu Wettbewerbsverzerrungen zu Lasten deutscher Unternehmen kommen.