Der Skandal um den Datenhandel und seine Folgen

abgedruckt in FIfF Kommunikation – Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V., Heft 4/2008, Dezember 2008, 25. Jahrgang, S. 5-9

Thilo Weichert

I. Auslöser

Als ich am 11. August 2008 nach zweiwöchigem Urlaub zur Arbeit zurückkehrte, wollte ich die Sommerpause nutzen, viel liegen gebliebene Arbeit zu erledigen. Doch die erste Nachricht, die ich bekam, machte mir klar, dass daraus nichts würde: Am Nachmittag würden wir im Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD) von der Verbraucherzentrale Schleswig-Holstein (VZ SH) eine Compact Disc (CD) erhalten, auf der mehr als 17.000 Datensätze mit Angaben zu Name, Adresse, Geburtsdatum und vollständiger Kontoverbindung enthalten sind. Die VZ SH hatte diese CD von einem Informanten aus einem Callcenter in Lübeck bekommen. Dies war der Auslöser einer intensiven **öffentlichen Debatte** über
- die Datenverarbeitung bei Callcentern,
- deren Kaltakquise am Telefon (sog. Cold Calls),
- das Fingieren von Verträgen und das unberechtigte Abbuchen von Girokonten,
- den Verkauf von Kontodaten bzw. den legalen und den illegalen Adressenhandel sowie
- die Sicherheit von Kundendaten auch in seriös erscheinenden Unternehmen.

Im Rahmen dieser Diskussion kamen weitere **illegale Datenbestände** ans Licht, die in vergleichbaren Zusammenhängen entstanden und genutzt wurden. Ein besonders markanter Fall war der Aufkauf von 6 Millionen Datensätzen im Auftrag der Verbraucherzentrale Bundesverband (vzbv) auf dem Schwarzmarkt für einen Preis von 850 Euro, wobei 4 Millionen der Datensätze Kontodaten enthielten. Dies sollte aber nicht alles sein: Anfang Oktober wurde bekannt, dass der Telekom-Tochter T-Mobil im Jahr 2006 17 Millionen Datensätze mit Telefon- und teilweise Geheimnummern, Geburtsangaben und E-Mail-Adressen von Kundinnen und Kunden abhanden gekommen sind, die nunmehr nach zwei Jahren auf dem Schwarzmarkt angeboten wurden.

II. Die Vorgehensweise der Datendealer

Der bei den bekannt gewordenen Fällen des Datenhandels regelmäßig erfolgte Ablauf stellt sich nach den bisherigen Erkenntnissen wie folgt dar: Die Kundendaten einschließlich der Kontoverbindung wurden auf unterschiedliche Weise erlangt. Die größten Bestände stammen offensichtlich aus Glücksspielunternehmen. Zwei dieser Unternehmen teilten unaufgefordert und umgehend nach Bekanntwerden des Skandals dem ULD mit, die Daten nicht verkauft zu haben. Es ist tatsächlich derzeit davon auszugehen, dass entweder unzuverlässige Mitarbeiter Firmendatenbestände kopiert

und an Adresshändler weiterverkauft haben oder im Rahmen von Callcenteraufträgen nach Abschluss der Aufträge die Daten nicht gelöscht, sondern angesammelt wurden. Als weitere **Datenquellen** kommen in Frage: Eigenangaben von Verbrauchern im Rahmen von telefonischen Kaltakquisen durch Callcenter, Daten aus der Inanspruchnahme von Internetdiensten, Angaben aus dem Zeitschriftenvertrieb, aus Spendensammlungen, aus Preisausschreiben u.Ä., Auszüge aus Kundendatenbeständen sonstiger Unternehmen. Die einzelnen Datenbestände, die wir Datenschützer sicherstellen konnten, haben jeweils einen Umfang im 4- bis 5stelligen Bereich, wobei in einigen Fällen aus Bezeichnung, Inhalt oder Datenstruktur auf die Herkunft von der SKL, der NKL oder von Lotto Team zu schließen ist. Teils handelt es sich um selektierte Datenbestände nur von älteren Menschen (z.B. Jahrgang 1930 bis 1940). Teilweise enthalten die Datensätze auch präzise Beschreibungen über die Reaktion der Betroffenen auf Callcenteranrufe.

Die erhobenen Daten werden offensichtlich in vielen Fällen an **Adresshändler** weitergegeben, die diese auf dem Schwarzmarkt – wiederum v.a. an **Callcenter** – weiterverkaufen. Die Callcenter nutzten diese, einschließlich der Kontodaten, für die weitere Telefonakquise oder für das **Fingieren von Verträgen** (in den unterschiedlichsten Branchen: z.B. Lotterie, Telekommunikation, Zeitschriftenvertrieb, Online-Angebote, Spenden). Die Daten werden daraufhin von den Callcentern an die Unternehmen weitergegeben, für die tatsächlich oder vermeintlich Verträge abgeschlossen werden, die hierfür Provisionen bezahlen und von den Konten der (vermeintlich) gewonnenen Kunden abbuchen. Bei der VZ SH meldeten sich Angehörige eines älteren Mannes, von dessen Konto über mehrere Monate hinweg 30 unterschiedliche Unternehmen auf der Basis von behaupteten Ermächtigungen Abbuchungen vorgenommen hatten. Beim ULD sprach ein über 80jähriger Mann persönlich vor mit einer schriftlichen Auftragsbestätigung für einen Online-Spielevertrag und erkundigte sich, was denn das wäre: Internet und Online-Spiele. An den ersten Tagen war das Zentraltelefon des ULD fast vollständig blockiert durch Anfragen von Betroffenen, die bei dieser Gelegenheit teilweise haarsträubende Geschichten schilderten. Immer ging es darum, dass unseriöse Firmen mit den illegal beschafften Daten versuchten, die Betroffenen zumeist finanziell über den Tisch zu ziehen. Es scheint, als hätten die Unternehmen, für die von den Callcentern Verträge vermittelt wurden, diese selbst dann nicht hinterfragt, wenn es zu auffällig vielen Stornos durch Widersprüche der Betroffenen kam. Erst wenn sich Aufsichts- und Strafverfolgungsbehörden einschalteten, sahen sich - so unser Eindruck - die Unternehmen veranlasst, sich von unseriösen Callcentern oder diese sich von angeblich unseriösen Mitarbeitern zu trennen.

Die **Kontoabbuchungen** wurden von den Banken durchgängig ungeprüft akzeptiert, selbst dann, wenn es sich um Massenabbuchungen handelte und auf Grund von Widersprüchen von Kunden und dadurch notwendigen Rückbuchungen Hinweise darauf bestanden, dass tatsächlich keine Abbuchungsermächtigungen der Kunden vorliegen. Rückbuchungen werden und wurden innerhalb einer Frist von 6 Wochen regelmäßig ohne weitere Hinterfragung von den Banken durchgeführt. Erfolgen Widersprüche später, so ist es den Betroffenen zumeist nicht mehr möglich, das überwiesene Geld zurückzuerhalten.

Kurz nach Bekanntwerden des Kontodatenskandals wies das ULD öffentlich darauf hin, dass auch bei den seriöseren Adresshändlern illegale Praktiken verbreitet sind: Adressvermittler, die im Auftrag von Privatpersonen und Unternehmen **Meldedaten** abfragen, speichern diese ab und nutzen diese dann für die eigene Auskunftstätigkeit. Damit umgehen sie die Schutzrechte der Betroffenen aus dem Melderecht und überschreiten ihre Befugnisse als Auftragsdatenverarbeiter. Auf Anregung des ULD hatten daher das Innenministerium Schleswig-Holstein schon im Mai 2008 und in der Folge auch die Ministerien in Nordrhein-Westfalen und in Rheinland-Pfalz die Meldebehörden darüber informiert, dass Adressvermittlern, die erlangte Daten für eigene Zwecke nutzen, künftig die Auskunft verweigert werden kann.

Wie im Jahr 2006 17 Millionen Bestandsdatensätze von Kunden des Mobilfunkbetreibers **T-Mobile** an illegale Datenhändler gelangen konnten, was Anfang Oktober 2008 bekannt wurde, ist bisher nicht aufgeklärt. Hierbei handelte es sich um Bestandsdaten von Kunden, die von Mitarbeitern entwendet worden sein sollen. Hierfür konnten aber bisher keine Belege vorgelegt werden. Die Datenbeschaffung könnte aber auch direkt aus den Rechnern von T-Mobile erfolgt sein, wobei nicht einmal ein dortiges Sicherheitsleck die Ursache sein muss. Nach den §§ 111 ff. Telekommunikationsgesetz (TKG) sind Netzanbieter verpflichtet, die Bestandsdaten ihrer Kunden den Sicherheitsbehörden über eine Schnittstelle direkt elektronisch zur Verfügung zu stellen. Wir Datenschützer hatten immer vor einem derart umfassenden unkontrollierten Datenzugriff für Sicherheitsbehörden gewarnt, da sich diesen auch kriminelle Hacker zunutze machen können, um unbeobachtet an riesige Datenbestände zu gelangen.

III. Änderungsbedarf im Datenschutzrecht

Zum Zeitpunkt des Bekanntwerdens des Kontodatenskandals liefen gerade **zwei Gesetzgebungsverfahren**, die einen direkten Bezug hierzu hatten. Beide Gesetzentwürfe wurden von der Bundesregierung auf ihrer 114. Kabinettssitzung am 30.07.2008 beschlossen. Ein „Gesetzentwurf zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen“, der von der allgemeinen Zielsetzung zwar begrüßt, aber in der Reichweite von Bundesländern und Verbraucherschützern kritisiert wurde, enthält bisher keine datenschutzrechtlichen Regelungen. Der „Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes“ erfasste zunächst lediglich die Bereiche Auskunfteien und Scoring.

Nachdem die Dimension des illegalen Datenhandels klar wurde - es kann z.B. davon ausgegangen werden, dass eine höhere zweistellige Millionenzahl von Bürgerinnen und Bürgern in Deutschland vom Datenklau betroffen sind - sahen sich Politiker von allen Parteien veranlasst, **gesetzgeberische Maßnahmen** zu fordern. Es entwickelte sich umgehend ein Konsens darüber, dass künftig Adresshandel für Werbezwecke nur noch nach Einwilligung der Betroffenen zulässig sein sollte. Wirtschaftsminister Michael Glos erwog sogar ein vollständiges Verbot des Adresshandels. Eine starke Verbraucherorientierung hatten die Forderungen der schleswig-holsteinischen Minister Lothar Hay (Innen) und Gitta Trauernicht (Soziales, Verbraucherschutz), die u.a. die Einführung einer Verbandsklage bei Datenschutzverstößen in die Diskussion brachten.

Die Forderung zur Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz, so z.B. die Bundestagsfraktion Bündnis 90/Die Grünen, hat mit dem konkreten Sachverhalt direkt nichts zu tun. Verfassungsrechtlich wünschenswert wäre – was indirekt eine Auswirkung auf entsprechende Fälle hätte – eine **Grundgesetzregelung**, die die Unabhängigkeit und eine ausreichende Ausstattung (institutionelle Absicherung) der Datenschutzkontrolle gewährleistet (s.u. IV.).

Es wurde von vielen Seiten der Vorschlag gemacht, die Weitergabe von personenbezogenen Daten für Werbezwecke generell unter Einwilligungsvorbehalt zu stellen, also von der **informierten Einwilligung der Betroffenen** (§ 4a Bundesdatenschutzgesetz – BDSG) abhängig zu machen (u.a. zunächst von Bundesverbraucherminister – BMELV – Horst Seehofer und Bundesjustizministerin – BMJ – Brigitte Zypries). Dies wird von Datenschutzbeauftragten seit Jahren immer wieder gefordert. Die bisherige Privilegierung der Werbenutzung mit dem sog. Listenprivileg ist verfassungsrechtlich fragwürdig und rechtspolitisch anachronistisch. Die Erfahrungen mit den bisherigen Regelungen ist, dass sie zu weit sind und selbst trotz ihrer Weite in der Praxis nicht beachtet werden. Dies gilt insbesondere für die Abwägungsklausel in § 28 Abs. 1 Nr. 2 BDSG, die von Datenverarbeitern regelmäßig immer zu ihren Gunsten und oft übermäßig ausgelegt wird, und in großem Umfang für die Hinweispflichten und Widerspruchsrechte in § 28 Abs. 4 BDSG.

Die Informationspflicht von Betroffenen bei Datenpannen wird in jüngerer Zeit intensiv diskutiert, nachdem dieses aus den USA kommende Datenschutzinstrument (**breach notification**) von der EU-Kommission in den Vorschlag einer Telekommunikations-Datenschutzrichtlinie (ePrivacy-Directive) Eingang fand. Der Vorschlag wurde u.a unterstützt von BMELV Seehofer und BMJ Zypries. Die Voraussetzungen einer solchen Informationspflicht müssen aber noch geklärt werden. Es muss verhindert werden, dass Menschen unnötig beunruhigt werden und ein unverhältnismäßiger Aufwand bei den Unternehmen entsteht. Wohl aber sollte die Benachrichtigung gewährleisten, dass bei der Gefahr einer direkten Schädigung durch den Datenklau die Betroffenen Vorkehrungen treffen können, z.B. durch den Wechsel von kompromittierten Geheimtelefonnummern oder von Kontoverbindungsdaten.

Vorgeschlagen wird weiter zu verbieten, dass Firmen die Zustimmung zur übermäßigen Datennutzung zur Bedingung für den Vertragsabschluss machen. BMELV Seehofer hat ein solches **Koppelungsverbot** zumindest für marktbeherrschende Unternehmen gefordert. Ein derartiges Verbot gibt es bisher nur im Telemedienrecht (§ 12 Abs. 3 TMG, § 95 Abs. 5 TKG). Da aber das Abfordern von Daten, die für die Vertragsabwicklung nicht benötigt werden, sich nicht auf diese Branche beschränkt, ist ein solcher Vorschlag sehr zu begrüßen. Es ist aber wenig sinnvoll, diese Maßnahme auf marktbeherrschende Unternehmen zu beschränken. Hinsichtlich des Datenschutzes gibt es bei Online- wie Offline-Anbietern derzeit noch keinen ausreichenden Wettbewerb, von dem datenschutzfreundliche Unternehmen profitieren könnten. Daher ist es sinnvoll und notwendig, ein generell wirksames Koppelungsverbot auszusprechen.

Von Vielen wird vorgeschlagen, die **Strafen** für unzulässige Datenverarbeitung stark heraufzusetzen und Lücken in den Strafbestimmungen zu schließen. Tatsächlich wurde der bisherige Sanktionsrahmen weder im Bereich des Ordnungswidrigkeitenrechts noch

im Strafrecht vollständig ausgeschöpft. Dies lag vor allem daran, dass die Sanktionswürdigkeit bisher von Seiten der zuständigen Staatsanwaltschaften nicht hinreichend anerkannt wurde. Dies hat sich offenbar auf Grund der jüngsten Ereignisse und der öffentlichen Resonanz hierauf geändert. Es ist absehbar, dass der Sanktionsrahmen mittelfristig nicht mehr ausreichen wird. Mit Lidl erhielt im September 2008 erstmals eine Wirtschaftsunternehmensgruppe wegen Datenschutzverstößen - hier lag der Schwerpunkt bei illegaler Videoüberwachung - eine Gesamtbußgeld in Höhe von 1,462 Mio. Euro auferlegt. Mit einer Erhöhung des Sanktionsrahmens würde die Bedeutung der Delikte politisch zum Ausdruck gebracht. Während bisher Datenschutzdelikte eher als individuelle Verstöße betrachtet wurden, handelt es sich bei den in jüngster Zeit bekannt gewordenen Delikten zweifellos um eine besondere Form der Wirtschaftskriminalität, die in einer Gesellschaft, in der wirtschaftlich relevante informationstechnische Kommunikation eine zunehmende Rolle spielt, immer gefährlicher zu werden droht.

Vorgeschlagen wurde weiterhin, den durch Datenmissbrauch entstandenen Gewinn wieder einzuziehen (BMJ Zypries; Bündnis 90/Die Grünen im Bundestag). Diese **Gewinnabschöpfung** setzt die weitgehende Ausermittlung der Sachverhalte voraus. Angesichts des Dunkelfelds beim Datenmissbrauch und der bisherigen Vollzugs- und Ermittlungsdefizite kann diese Maßnahme erst am Ende der Verfahren relevant und auch wirksam werden. Schon bisher ist es möglich, illegal erlangte Gewinne aus illegalem Datenhandel abzuschöpfen. Es ist derzeit nicht abschätzbar, welche praktische Bedeutung eine Verbesserung dieser Sanktionsmöglichkeit hätte.

Zu Recht werden Defizite im Bereich der **Datensicherheit** moniert. So wurde vorgeschlagen, im Fall des Datenhandels deren Herkunft, Nutzung und Weitergabe zu dokumentieren. Tatsächlich ist es derzeit ein Problem für die Datenschutzkontrolle, dass verantwortliche Stellen oft weder die Herkunft von Daten noch die Empfänger im Fall von Übermittlungen protokollieren, so dass Datenflüsse nicht nachvollzogen werden können und das Auskunftsrecht der Betroffenen leerläuft. Derartige Dokumentationspflichten bestehen im Grunde schon heute, auch wenn sie nicht gesetzlich ausdrücklich geregelt sind (abgeleitet z.B. aus § 9 BDSG). Da die aktuell festgestellten Vollzugsdefizite nicht nur im Bereich des Datenhandels für Werbezwecke bestehen, wäre es nicht sinnvoll, Protokollierungspflichten nicht hierauf zu beschränken. Eine rechtliche Verbesserung würde schon dadurch erreicht, dass die Ziele der technisch-organisatorischen Maßnahmen – wie in vielen Landesdatenschutzgesetzen (LDSG) – auch ausdrücklich in das BDSG aufgenommen würden: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit, Transparenz. Damit würde zugleich eine Konkretisierung des jüngst vom Bundesverfassungsgericht (BVerfG) geschaffenen Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme erfolgen (U.v. 27.02.2008, Az. 1 BvR 370/07 u.a.).

Die Möglichkeit von Datenschutzverstößen basiert oft auf ungenügender Datensicherheit bei den verarbeitenden Unternehmen und ungenügender Kontrolle vor Ort. Dies ließe sich durch eine Verbesserung der praktischen Rahmenbedingungen wie der rechtlichen Möglichkeiten von betrieblichen Datenschutzbeauftragten bekämpfen. Die Datenschutzbeauftragten müssen aber in ein umfassenderes unternehmensweites **Datenschutzmanagement** eingebunden sein, um optimal wirksam zu sein. Zu einem

solchen Management gehört auch die Auditierung von Verfahren sowie der Einsatz von hinsichtlich des Datenschutzes zertifizierten Produkten. Es kommt also nicht von ungefähr, dass anlässlich des Datenskandals an das 8 Jahre alte Versprechen eines Datenschutzauditgesetzes (§ 9a BDSG) erinnert wurde. Bei dessen Umsetzung muss aber gewährleistet werden, dass die Qualität der Audits und Gütesiegel durch unabhängige Prüfinstanzen gesichert wird.

Bisher wird von den Gerichten in Frage gestellt, dass es sich beim Datenschutzrecht um **verbraucherschützende Normen** handelt, die auch von den Verbraucherzentralen gerichtlich durchgesetzt werden könnten. Obwohl diese Rechtsprechung schon nach derzeitiger Gesetzeslage kaum haltbar ist, wäre es im Interesse einer klaren Aufgabenzuordnung und der Rechtssicherheit geboten, gesetzlich klarzustellen, dass den Verbänden auch eine Verbraucherdaten schützende Funktion zukommt. Dies hätte zur Folge, dass Verbraucherverbände gegen datenschutzwidrige Praktiken von Unternehmen zulasten von Verbrauchern klagebefugt würden. Damit würde das rechtlich eher dürftige Instrumentarium zur Ahndung von Verstößen massiv verbessert. Ein Konflikt zur Datenschutzaufsicht würde nicht entstehen; Datenschützer und Verbraucherschützer arbeiten zunehmend gut zusammen, wie das Beispiel des Kontodatenskandals zeigte.

Bisher sind die zivilrechtlichen Sanktionsmöglichkeiten gegen Datenschutzverstöße ohne erkennbare Wirkung. Dies hat u.a. einen Grund darin, dass sich der Datenschutzanspruch auf Schadenersatz nach § 7 BDSG nur auf den materiellen Schaden beschränkt. Zudem ist eine Exkulpation bei Beachtung der "gebotenen Sorgfalt" möglich. Eine äußerst disziplinierende Wirkung hätte ein Anspruch auf **immateriellen Schadenersatz**, also eine Art Scherzensgeld.

Im Datenschutzrecht besteht darüber hinausgehender **weiterer Novellierungsbedarf**, der mit dem aktuellen illegalen Datenhandel und dem Missbrauch von Kontodaten nicht in direktem Zusammenhang steht. Das BDSG ist in seiner heutiglen Fassung nicht mehr an die technischen Gegebenheiten des Internet angepasst. Seit mehreren Jahren ist unbestritten, dass es einer umfassenden Modernisierung des allgemeinen Datenschutzrechtes bedarf. Dies führt insbesondere auch im Bereich des Datenschutzes für Verbraucherinnen und Verbraucher zu rechtlichen Verunsicherungen. Dieses Thema war Gegenstand der Sommerakademie „Internet 2008 – alles möglich, nichts privat?“ am 01.09.2008 in Kiel.

IV. Sonstige Maßnahmen

Der Vorschlag von vielen Seiten, die Datenschutzkontrolle zu verbessern, kann nur nachhaltig unterstützt werden. Derzeit sind die **Aufsichtsbehörden** nach § 38 BDSG personell und sachlich so ausgestattet, dass sie ihre Aufgaben nicht ansatzweise befriedigend erfüllen können. Es gibt – soweit bekannt – derzeit kein Bundesland, in dem eine zweistellige Zahl von Personen für die Datenschutzaufsicht im Privatbereich eingesetzt wird. Der Umstand, dass diese öffentlich Bediensteten zumeist mehrere 100.000 Betriebe überprüfen sollen, erklärt u.a. die bestehenden Vollzugsdefizite.

Anfang Oktober 2008 wechselte die Datenschutzaufsicht von Rheinland-Pfalz zum

dortigen Landesbeauftragten für den Datenschutz. Weiterhin ist aber diese Aufsicht in 7 Bundesländern bei der Innenverwaltung angesiedelt: Baden-Württemberg, Bayern, Brandenburg, Hessen, Saarland, Sachsen-Anhalt und Thüringen. In diesen Ländern ist – unter Verstoß gegen die Vorgaben des Verfassungsrechts sowie der europäischen Datenschutzrichtlinie – eine **unabhängige Datenschutzkontrolle** im Bereich der Privatwirtschaft weiterhin nicht gewährleistet. Tatsächlich lässt sich feststellen, dass eine ernsthafte Verfolgung von Datenschutzverstößen – soweit dies personell möglich ist – eher bei unabhängigen Datenschutzbeauftragten erfolgt.

Der Vorschlag des Bundes Deutscher Kriminalbeamten (BDK), bei den Datenschutzaufsichtsbehörden **besondere Ermittlungsgruppen** einzurichten, die technische und die rechtliche Kompetenz sowie Ermittlungserfahrungen miteinander kombinieren und für die Strafverfolgungsbehörden die notwendigen Grundlagen für weitere strafrechtliche Ermittlungen liefern können, ist im Grunde ein richtiger Ansatz. Es kann festgestellt werden, dass die Sachverhalte regelmäßig länderübergreifend und von hoher technischer Komplexität sind. Solange aber einige der Aufsichtsbehörden noch überhaupt kein technisches Personal verfügbar haben, sollte zunächst dieses Defizit behoben werden, bevor weitergehende Maßnahmen stattfinden. Über die organisatorische Einbindung und die genauen Aufgaben und Befugnisse müsste eine weitere Diskussion erfolgen. Es muss verhindert werden, dass derartige Ermittlungstrupps im Vorfeld von Gefahren und Straftaten tätig werden, so wie dies in anderen Bereichen durch die Polizei der Fall ist. Angesichts der katastrophalen Ausstattung der Aufsichtsbehörden und teilweise sehr unterschiedlichen Kontrollstrategien in den Ländern scheinen derartige Ermittlungsgruppen noch in weiter Ferne.

Die FDP-Fraktion im Bundestag reagierte auf ihrer Herbstklausur auf den Kontodatenskandal mit einer "Liberalen Datenschutzoffensive", in der u.a. die Gründung einer "**Stiftung Datenschutz**" vorgeschlagen wird. Nach dem Vorbild der Stiftung Warentest sollen dort Produkte und Dienstleistungen von Unternehmen unter Datenschutzgesichtspunkten verglichen und bewertet werden.

Die Verbraucherschutzministerkonferenz hat vorgeschlagen, die Wirksamkeit von telefonisch geschlossenen Verträgen von einer **schriftlichen Bestätigung** abhängig zu machen. Entsprechendes wäre auch im Internet wünschenswert. Derartige Bestätigungen würden die Transparenz für die Betroffenen erhöhen, die beweiskräftig Kenntnis darüber erlangen, welches Unternehmen welche (Vertrags-) Daten über sie verarbeitet.

Sobald erste Beschwerden oder mehrfache Stornos von Abbuchungen in einer Bank über eine abbuchende Firma vorliegen, sollten alle weiteren finanziellen Transaktionen gestoppt, als Grundlage die schriftliche Ermächtigung der Betroffenen eingefordert und die Betroffenen informiert werden. Diese Pflichten dürften derzeit schon den Banken zukommen (vgl. Urteil des Bundesgerichtshofes – BGH – v. 06.05.2008, Az. XI ZR 56/07). Die Banken sind sich aber offensichtlich dieser Pflichten bei entsprechendem **Verdacht** bisher nicht hinreichend bewusst und betreiben die jährlich ca. 7 Milliarden Lastschriften im Jahr ohne wesentliche Sicherungen. Eine Konkretisierung dieser Pflichten ist auch im Sinne des Datenschutzes, da mit ihnen nicht nur unzulässige Geld-,

sondern auch Datentransaktionen vermieden werden können.

Die Erstellung von **Warndateien über Unternehmen**, bei denen der begründete Verdacht von Verbraucherschutzverstößen besteht, ist aus Datenschutzsicht möglich. Derartige Dateien über Verbraucher zum Schutz von Unternehmen bestehen schon heute und finden grds. in § 29 BDSG ihre rechtliche Grundlage. Es ist erstaunlich, dass bzgl. der erheblich größeren Gefährdung durch Unternehmen ein solches Angebot zum Schutz der Verbraucher bisher nicht besteht. Selbstverständlich müssen die strengen rechtlichen Anforderungen des § 29 BDSG, die heute oft nicht beachtet werden, erfüllt sein.

V. Perspektiven

Am 04.09.2008 lud Bundesinnenminister Wolfgang Schäuble die Landesbeauftragten für den Datenschutz, die Aufsichtsbehörden sind, sowie die Landesinnenministerien zu einem **Datenschutzgipfel** nach Berlin ein. Hierbei wurde angekündigt und Einigkeit darüber hergestellt, dass bis Ende November vom Bundesinnenministerium eine Gesetzesinitiative auf den Weg gebracht werden soll. In dem geplanten Artikelgesetz sind vorgesehen: neben der Einführung des "Permission Markting" ein begrenztes Koppelungsverbot, zusätzliche Dokumentations- und Transparenzpflichten im BDSG, Änderungen im Sanktionenrecht sowie ein Datenschutzauditgesetz, wobei die Vergabe der Siegel privaten Unternehmen vorbehalten bleiben soll. In einer Entschließung vom 16.09.2008 unterstützt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder (DSB-Konferenz) diese Ziele im Grundsatz und erhebt darüber hinausgehende Forderungen.

Dem gegenüber kam vom Bundesrat die Initiative, das, was kurzfristig geregelt werden kann, schon anlässlich der **aktuellen BDSG-Novellierung** zu Auskunfteien und Scoring ins Datenschutzrecht zu integrieren. Dies gilt vor allem für das sog. Permission Marketing, also die Zulassung des Adressenhandels für Werbezwecke nur noch bei Vorliegen einer Einwilligung der Betroffenen. Angesichts der sich formierenden Kräfte in der Wirtschaft, denen es darum geht, eine Novellierung zu sabotieren, sollte eine schnellstmögliche Umsetzung der Maßnahmen, über die politischer Konsens besteht, erfolgen. Der Zentralverband der deutschen Werbewirtschaft (ZAW), der Bundesverband der Deutschen Industrie (BDI) sowie 10 weitere Wirtschaftsverbände warnten schon anlässlich des Datenschutzgipfels davor, die Nutzung von Daten von der Einwilligung der Betroffenen abhängig zu machen. Angesichts des Umstandes, dass die Legislaturperiode auf Bundesebene im Sommer 2009 endet, ist Eile geboten, sollen die Reformen nicht auf den Sankt-Nimmerleins-Tag verschoben werden.

Der Innenminister von Brandenburg Jörg Schönbohm wurde beauftragt, eine **Arbeitsgruppe der Länder** einzuberufen und zu leiten, in der ein weitergehender Novellierungsbedarf des Datenschutzrechtes festgestellt und diskutiert wird. Ob gerade dieses Land hierzu geeignet ist, ist angesichts der dortigen dürftigen Situation des Datenschutzes im nicht-öffentlichen Bereich in Zweifel zu ziehen.

Die Hoffnung auf einen großen Wurf bei der Datenschutzgesetzgebung hat sich nach dem 11. September 2001 als Illusion erwiesen. Wir erinnern uns: Nachdem das BDSG

in einer ersten Stufe im Mai 2001 an die europäische Datenschutzrichtlinie angepasst worden ist, sollte eine umfassende Modernisierung des Datenschutzrechtes in einer zweiten Stufe in Angriff genommen werden. Angesichts der mit dem Terrorismus begründeten Hetzjagd auf den Datenschutz und eines unwilligen, aber zuständigen Bundesinnenministers Otto Schily kam es in der rot-grünen Koalition nicht dazu, dass das von Alexander Roßnagel, Hansjürgen Garstka und Andreas Pfitzmann erstellte Gutachten über die Notwendigkeit der **Modernisierung des Datenschutzes** zur Grundlage von Gesetzgebungsaktivitäten genommen wurde. Seitdem ist die rechtliche Landschaft noch unübersichtlicher geworden. Es wird noch in dieser Legislatur eine BDSG-Novelle zu Auskunfteien und Scoring geben. Diese wird hoffentlich auch schon die ersten Schlüsse aus den Datenskandalen ziehen. Ob auch noch ein Datenschutzauditgesetz kommt, das eine effektive Qualitätskontrolle gewährleisten kann, ist ungewiss. Angesichts der nicht enden wollenden Skandale bleibt der Handlungsdruck groß. Letztendlich muss aber das Novellierungs-Patchwork zu einem umfassenden neuen BDSG zusammengeführt werden, das sprachlich und inhaltlich bereinigt und technisch auf den neuesten Stand gebracht wird. Sollten wir das schaffen, so hat es sich gelohnt, dass ich im Sommer 2008 wegen des Kontodatenskandals die auf meinem Schreibtisch wartenden Akten vorläufig liegen ließ.

Dr. Thilo Weichert ist Landesbeauftragter für den Datenschutz Schleswig-Holstein und damit Leiter des Unabhängigen Landeszentrums für Datenschutz (ULD) in Kiel