Sonderheft
2008

Datenschutz Nachrichten

31. Jahrgang
ISSN 0137-7767
5,00 Euro

Dokumentation Datenschutztag 2007 30 Jahre DVD Jubiläumsveranstaltung

Peter Schaar ■ Bettina Sokol ■ Burkhard Hirsch ■ Thilo Weichert ■ Johann Bizer ■ Reinhard Fraenkel

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine

Mittwoch, 4. Juni 2008
Arbeitnehmer-Datenschutz aktuell
Datenschutz-Fachtagung 2008, BTQ Niedersachsen, in Hannover
weitere Informationen siehe unter www.btq.de

Donnerstag, 5. Juni 2008
Datenschutzgerechter Umgang mit Studierendendaten
Universität Stuttgart (Campus Stadtmitte)
weitere Informationen unter www.zendas.de

Sonntag, 20. Juli 2008
DVD-Vorstandssitzung in Bonn
(Interessierte DVD-Mitglieder mögen sich bitte bei der Geschäftsstelle melden.)

Mittwoch, 8. Oktober 2008
Datenschutz bei E-Learning-Plattformen
Universität Stuttgart (Campus Stadtmitte)
weitere Informationen siehe unter www.zendas.de

Donnerstag/Freitag, 9./10. Oktober 2008
2. Fachtagung für Datenschutzbeauftragte an Hochschulen und anderen wissenschaftlichen Einrichtungen
Freie Universität Berlin, weitere Informationen unter www.datenschutz.fu-berlin.de

Sonntag, 12. Oktober 2008
DVD-Vorstandssitzung in Frankfurt
(Interessierte DVD-Mitglieder mögen sich bitte bei der Geschäftsstelle melden.)

Freitag, 24. Oktober 2008
Verleihung der Big Brother Awards
Bielefeld, weitere Informationen unter www.bigbrotheraward.de

Dienstag, 9. Dezember 2008
Datenschutz in Forschung und Lehre - Technische Aspekte
Universität Stuttgart (Campus Stadtmitte)
weitere Informationen unter www.zendas.de

DANA
Datenschutz Nachrichten
ISSN 0137-7767
31. Jahrgang
Sonderheft 2008

Herausgeber
Deutsche Vereinigung für
Datenschutz e.V. (DVD)
DVD-Geschäftstelle:
Bonner Talweg 33-35, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutz.de

Redaktion (ViSdP)
Hajo Köppen
c/o Deutsche Vereinigung für
Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Layout und Satz
Sascha Hammel
Gießen
Hammelwood@web.de

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Leserbriefe
Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Titelbild: Sascha Hammel

Datenschutztag 2007 – Die Jubiläumsveranstaltung

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) beging ihren dreißigsten Geburtstag mit einer Festveranstaltung, dem Datenschutztag 2007. Seit ihrer Gründung im Jahre 1977 setzt sie sich für das Recht auf informationelle Selbstbestimmung ein – auch wenn diese von Steinmüller, Lutterbeck und Mallmann bereits 1972 erdachte Wortschöpfung[1] erst durch das Urteil des B undesverfassungsgerichts zur Volkszählung 1983 ins Bewusstsein der Öffentlichkeit gedrungen ist.

Für drei Tage wurde Bielefeld so zur Datenschutzhauptstadt Deutsch-lands. Den Auftakt bildete am 11. Oktober die Mitgliederversammlung der DVD, der Tagung und Verleihung der BigBrotherAwards am nächsten Tag folgten. Das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FifF e.V.) beschloss die Serie am 13. Oktober 2007 mit seiner Mitgliederversammlung.

Die Jubiläumsveranstaltung der DVD kam beim zahlreich erschienenen Publikum, trotz einiger, teils bahnstreik-bedingter Ausfälle, gut an, was man auch an den lebhaften Diskussionen erkennen konnte. Wir dokumentieren in dieser Sonderausgabe der DANA die Vorträge dieser Veranstaltung. Die Grußworte des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar und der Landesbeauftragten für Datenschutz und Informationsfreiheit in Nordrhein-Westfalen, Bettina Sokol schlugen die Brücke zwischen dem Anlass der Feier und aktuellen Entwicklungen im Datenschutz. In seinem Festvortrag kommentierte der Bundesminister a.D. Dr. Dr. h.c. Burkhard Hirsch kritisch das nachlassende Interesse am Datenschutz bei manchen Bürgern und Politikern. Dr. Thilo Weichert (Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein) blickt auf 30 Jahre Datenschutz zurück und Reinhard Fraenkel (Datenschutzbeauftragter TollCollect) lieferte einen „praxisorientierten Werkstattbericht“.

Wir dokumentieren in dieser Sonderausgabe außerdem den durch Bahnstreik leider ausgefallenen Vortrag von Dr. Johann Bizer – eine Bestandsaufnahme mit Ausblick.

1 W. Steinmüller, B. Lutterbeck, C. Mallmann, U. Harbort, G. Kolb, J. Schneider; Grundfragen des Datenschutzes, Gutachten im Auftrag des Bundesministeriums des Innern, Bundestagsdrucksache 6/3826 vom 7.9.1972

Peter Schaar

Grußwort des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit

Meine Damen und Herren,

seit dreißig Jahren gibt es die Deutsche Vereinigung für Datenschutz als engagierte Verfechterin des Grundrechts auf informationelle Selbstbestimmung und der Bürgerrechte - das ist ein Grund zum Feiern. Dreißig Jahre lang unermüdlicher Einsatz, ja Kampf für einen besseren Datenschutz, und ein Ende ist noch lange nicht abzusehen, denn die Gefahren für dieses Grundrecht und die Herausforderungen für seine Verteidiger nehmen stetig zu. Seit dreißig Jahren gibt es auch das Bundesdatenschutzgesetz, und dies ist keineswegs so selbstverständlich, wie es heute vielleicht vielen scheinen mag. Vorausgegangen war eine mehrjährige Diskussion um ein entsprechendes Gesetz, und es stand mehrfach auf des Messers Schneide, ob es überhaupt ein solches Gesetz geben würde. Schon im Januar 1970 hatte eine dafür eingesetzte Kommission den „Vorentwurf eines Gesetzes zum Schutze der Privatsphäre gegen Missbrauch von Datenbankinformationen“ vorgelegt. Nach langem Hin und Her, mehreren Gutachten, Anhörungen und heftigem Widerstand aus Wirtschaft und Verwaltung wurde dann am 10. Juni 1976 das Bundesdatenschutzgesetz gegen die Stimmen der Fraktion von CDU und CSU, die keine unabhängige Kontrollinstanz für den Datenschutz wollte, vom Deutschen Bundestag verabschiedet. Danach wurde es aber erst richtig spannend, denn die Legislaturperiode ging im Herbst 1976 zu Ende und der Bundesrat rief im Juni 1976 den Vermittlungsausschuss an. Der neue Bundestag war schon gewählt aber noch nicht zusammengetreten, als der alte Bundestag im November 1976 dem Gesetz in der Fassung des Vermittlungsausschusses zustimmte, ein wohl einmaliger Vorgang in der Geschichte der Bundesrepublik Deutschland. Der Bundespräsident zögerte deswegen auch mit der Ausfertigung des Gesetzes und ließ zunächst ein Rechtsgutachten erstellen. Im Januar 1977 war es dann soweit und am 1. Februar 1977 wurde das Gesetz im Bundesgesetzblatt verkündet.

Der erregten Auseinandersetzung um den Datenschutz, die damit zunächst abgeschlossen war, sollten bald weitere folgen. Die Volkszählung stand an und viele werden sich noch an die leidenschaftlichen Diskussionen und das heftige Ringen um diese umfassende Datenerhebung erinnern, die dann im Dezember 1983 in das sog. „Volkszählungsurteil“ des Bundesverfassungsgerichts mündeten, ein weiterer Meilenstein der Entwicklung. Der Datenschutz bekam Verfassungsrang, Gesetzgebung und Rechtsprechung mussten dem Rechnung tragen. Wieder vergingen Jahre, bis die erforderlichen Anpassungen im Bundesdatenschutzgesetz vollzogen waren, flankiert von einer Vielzahl von Spezialregelungen, die die neue Verfassungsrechtslage erforderte.

Die nächste große öffentliche Debatte um den Datenschutz in Deutschland wurde zum sog. Großen Lauschangriff geführt, und wieder war es das Bundesverfassungsgericht, das in einem Grundsatzurteil den Datenschutz stärkte und einen Kernbereich der privaten Lebensführung unter absoluten Schutz stellte.

Die zunächst letzte Phase einer auch in der Öffentlichkeit geführten und wahrgenommenen Auseinandersetzung um den Datenschutz wurde durch die Terroranschläge vom 11. September 2001 und den dadurch bedingten „Anti-Terror-Kampf“ ausgelöst. Sie ist noch nicht beendet, hat aber jetzt schon in vielen Bereichen zu schmerzlichen Eingriffen in das Grundrecht der informationellen Selbstbestimmung geführt, ohne dass dadurch tatsächlich eine nachhaltige Verbesserung der Sicherheitslage garantiert wäre.

Blickt man nun auf diese dreißig Jahre zurück, kann man zwei Feststellungen treffen: Die Ängste derer in Wirtschaft und Verwaltung, die das Bundesdatenschutzgesetz seinerzeit verhindern wollten, haben sich als unbegründet erwiesen. Weder wurde die Wirtschaft durch den Datenschutz beeinträchtigt noch in ihrem Wachstum behindert. Auch die elektronische Datenverarbeitung hat sich rasant entwickelt, trotz Datenschutz und unabhängiger Datenschutzaufsicht. Im Gegenteil, wahrscheinlich haben datenschutzrechtliche Regelungen und unabhängige Aufsicht erst zu der Akzeptanz bei den Bürgerinnen und Bürgern geführt, die für die eingetretene Entwicklung unerlässlich war.

Die Befürchtungen derer, die damals nachdrücklich für den Datenschutz eingetreten sind und seine gesetzliche Regelung letztlich durchgesetzt haben, sind hingegen leider durch die Entwicklung bestätigt worden. Trotz aller Bemühungen konnte die Tendenz zu immer mehr Überwachung und elektronischer Kontrolle in allen Lebensbereichen nicht gestoppt werden, es waren allenfalls datenschutzrechtliche Leitplanken möglich.

Zwar leben wir nicht in einem Überwachungsstaat, wohl befinden wir uns aber auf dem Weg in eine Überwach-ungsgesellschaft, in der die Gefahren, die damals das Bundesverfassungsgericht zu seinem Volkszählungsurteil veranlasst hatten, immer mehr Realität werden, und das keineswegs nur seitens staatlicher

Institutionen, sondern vor allem auch im nicht-öffentlichen Bereich.

Es würde den Rahmen eines Grußwortes sprengen, diese Entwicklung und die aktuelle Lage im Detail darzustellen. Deswegen möchte ich nur einige Punkte kurz anreißen, die für die akute Gefährdung des Persönlichkeitsrechts maßgeblich mit verantwortlich sind: Da wäre zunächst das Vordringen der modernen Informationstechnologie und der elektronischen Datenverarbeitung in praktisch alle Lebensbereiche zu nennen, wodurch eine Flut personenbezogener Daten produziert wird, teilweise gewollt, teilweise auch nur als Nebenprodukt. Weiter ist Information zu einem Wirtschaftsgut geworden; auch für sich genommen unbedeutende personenbezogene Daten haben einen wirtschaftlichen Wert, der sich durch das Zusammenführen mit anderen Daten noch steigern lässt. Der technologische Fortschritt führt dazu, dass das Sammeln, Speichern, Zusammenführen und Auswerten von Daten immer schneller und billiger wird; deswegen wird in immer mehr Bereichen menschliche Arbeitsleistung, aber auch Bewertung und Beurteilung von Sachverhalten durch Menschen durch den Einsatz von elektronischer Datenverarbeitung ersetzt, weil dies umfassendere und zuverlässigere Bearbeitung in viel kürzerer Zeit und zu viel geringeren Kosten verspricht. Darin steckt ein Stück Dehumanisierung unserer Lebenswelt und unserer Gesellschaft, die dazu verleitet, die elektronische Datenverarbeitung, das Anlegen zentraler Datensammlungen, den Abgleich möglichst vieler verschiedener Dateien als den Schlüssel zur Lösung aller Probleme anzusehen. So werden Planstellen abgebaut, beispielsweise beim Bahnhofsaufsichtspersonal, und stattdessen die elektronische Überwachung ausgebaut.

Meine Damen und Herren, diesen Ansatz halte ich für falsch. Denkt man ihn zu Ende, müsste die totale elektronische Kontrolle eines jeden Einzelnen zu einer Gesellschaft führen, in der es weder Terror noch Kriminalität noch irgendwelche Probleme des gesellschaftlichen Zusammenlebens mehr gibt – eine ziemlich fade Variante des alten Menschheitstraums des Paradieses auf Erden. In Wirklichkeit aber ein Albtraum, weil dieses Versprechen nicht eingelöst werden kann, aber zugleich jede individuelle Freiheit verloren wäre. Es ist ein Irrweg, die Prävention immer weiter vorzuverlegen und dafür immer umfangreichere Datenerhebungen über alle Bürgerinnen und Bürger zu verlangen. Nur am Rande sei hier erwähnt, dass in den USA trotz der ausgefeilten Ratingsysteme und Scoreverfahren die Hypothekenkrise eingetreten ist. Das Risiko wurde nicht beherrscht, trotz weit reichender elektronischer Bewertungssysteme und obwohl die datenschutzrechtlichen Anforderungen an diese Systeme viel geringer sind.

Für die nicht allzu ferne Zukunft sehe ich die konkrete Gefahr eines „genormten Menschen“. Damit meine ich, dass in immer mehr Lebensbereichen jedes Verhalten von Menschen, das von vorgegebenen staatlichen, aber auch gesellschaftlichen Normen oder auch nur angeblichen Vorgaben der Vernunft abweicht, elektronisch kontrolliert und sanktioniert wird. Wer unvernünftig Auto fährt, zahlt dann höhere Versicherungsbeiträge. Wer sich ungesund ernährt, muss für die Krankenkasse mehr bezahlen. Wer sich einen SCHUFA-Eintrag leistet, wird ins soziale Abseits gestellt, weil niemand mehr mit ihm Verträge abschließen will. Die Beispiele ließen sich beliebig fortsetzen. In jedem Einzelfall werden gute Argumente angeführt, warum diese „fürsorgliche Kontrolle“ nur zum Besten der Betroffenen ist, die vor ihrer eigenen Unvernunft geschützt werden müssen, und natürlich zum Besten der Gemeinschaft, deren Solidarität nicht durch das Verhalten einzelner über Gebühr ausgenutzt werden soll. Aber in der Summe wird jede Individualität erstickt. Diese Entwicklung stellt eine große Herausforderung an die freiheitliche Gesellschaft dar; im Ergebnis bekämen wir eine Gesellschaft, in der jedes individuelle Verhalten erfasst, kontrolliert und bewertet würde. Eine solche Entwicklung dürfen wir nicht widerspruchslos hinnehmen.

Meine Damen und Herren, Sie sehen, es gibt genug zu tun, um auch weiterhin unsere Freiheit und unsere informationelle Selbstbestimmung zu bewahren und zu verteidigen. Die Deutsche Vereinigung für Datenschutz bleibt unverzichtbar, für die nächsten dreißig Jahre und darüber hinaus. In diesem Sinne möchte ich Ihnen für die geleistete Arbeit danken und viel Kraft und Erfolg für die Zukunft wünschen.

Bettina Sokol

Grußwort der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen

Meine sehr geehrten Damen und Herren, liebe Datenschützerinnen und Datenschützer,

zu aller erst einmal einen ganz herzlichen Glückwunsch zum 30. Geburtstag! Nachdem die Entwicklungen in den letzten 30 Jahren schon von meinem Vorredner skizziert wurden, möchte ich mich in meinem Grußwort stärker der aktuellen Situation zuwenden, denn eines dürfte unbestreitbar sein: Nie waren die Existenz und das Engagement der Deutschen Vereinigung für Datenschutz so wertvoll und wichtig wie in unserer heutigen Zeit.

Als die Deutsche Vereinigung für Datenschutz 1977 ins Leben gerufen wurde, war die Datenschutzwelt zwar schon nicht mehr ganz in Ordnung, aber sie sah doch lange nicht so aus wie heute. Heute sind wir auf dem Weg zur allgegenwärtigen Datenverarbeitung, zum sogenannten „ubiquitous computing". Die Fülle der Informationen, die über uns in Staat und Wirtschaft existieren, sind für die Einzelperson – wenn überhaupt – nur noch mit viel Energie und Aufwand überblickbar. Die Privatwirtschaft lockt mit Gewinnspielen, natürlich für den Adresshandel. Sie lockt mit Kunden bindungsprogrammen, natürlich für höheren Absatz und Umsatz. Sie lockt mit allen möglichen und unmöglichen Zusatzdiensten für das Handy – zum Beispiel der jederzeitigen Ortung von Kindern, Arbeitnehmerinnen und Arbeitnehmern oder Eheleuten. Die RFIDs haben mittlerweile ihren Weg in die Herrenoberbekleidungsabteilungen der Kaufhäuser gefunden. Und wenn die Entwicklung der Biometrie weiter so rasant fortschreitet, wird es nicht mehr lange dauern, bis uns die Umkleidekabine schon beim Betreten derselben rät, es doch lieber gleich mit einer Hose der nächstgrößeren Konfektionsnummer zu versuchen, weil sie unseren Körper sofort automatisch vermessen hat.

Biometrie und Funkchips sind aber auch Verfahren und Instrumente, auf die der Staat setzt. In unseren Reisepässen und Personalausweisen findet sich demnächst beides. Und wie von Kriminellen werden uns auch die Abdrücke des rechten und des linken Zeigefingers abgenommen, um sie in das Dokument aufzunehmen. Nach dem Motto: „Was man hat, hat man", wurde auch sogleich vom Bundesinnenminister gefordert, die Fingerabdrücke bei den Behörden dauerhaft vorzuhalten, weil es doch zu schade wäre, einmal erhobene Daten gleich wieder zu löschen. Dieses Ansinnen konnte sich glücklicherweise aber nicht durchsetzen. Ob es allerdings gelingen wird, zu verhindern, dass sich die gerade eingeführte lebenslange Steueridentifikat ionsnummer zu einer verfassungswidrigen Personen-kennziffer entwickeln wird, ist völlig offen.

Obgleich wir inzwischen wissen, dass die Videoüberwachung kein Allheilmittel ist, boomt dieser Industriezweig in einem erstaunlichen Ausmaß. Und wer sich mit offenen Augen durch die Straßen und durch andere öffentlich zugängliche Räume bewegt, kann sich in manchen Ballungsgebieten kaum noch in überwachungsfreie Zonen flüchten, weil die Kameradichte immer höher wird. Dabei spielt es aus der Sicht der Überwachten letztlich keine große Rolle mehr, ob die jeweilige Videoüberwachung von einer staatlichen oder einer privaten Stelle betrieben wird. Denn der Konformitätsdruck, mit dem normangepasstes Verhalten erzwungen werden soll, wird allein schon durch den Umstand der Beobachtung erzeugt. Nicht umsonst hat das Bundesverfassungsgericht in seiner grundlegenden Volkszählungsentscheidung, aber auch später immer wieder vor den Folgen einer übermäßigen Sozialkontrolle gewarnt. Ich darf zitieren: „Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist."

Ob die einzelne Kamera staatlich oder privat betrieben wird, ist zudem auch deshalb inzwischen von untergeordneter Bedeutung, weil staatliche Stellen unter bestimmten Voraussetzungen auf die Daten aus privat betriebenen Kameras ebenfalls zugreifen können. In Baden-Württemberg besteht die Absicht, einen solchen polizeilichen Zugriff systematisiert zu institutionalisieren. Dort sollen in eine Art „Video-Atlas" alle privat betriebenen Kameras eingetragen werden, um sich ihrer bei Bedarf bedienen zu können. Aber nicht nur die Zahl der Überwachungskameras wächst, sondern auch die Technik und die Einsatzumstände entwickeln sich weiter. Zwar war der Feldversuch einer Kombination von Überwachungskameras und Gesichtserkennungssoftware am Mainzer

Hauptbahnhof noch erfolglos, aber der Wille der Sicherheitsbehörden zur Nutzung dieser Verknüpfungsmöglichkeiten ist ungebrochen, sodass eifrig an der Verbesserung von Gesichtserkennungsprogrammen gearbeitet wird. In der Entwicklung befinden sich auch Programme zur Analyse von Körperbewegungen. Bei Personen, deren Verhalten als „verdächtig" klassifiziert wird, schlägt die Kamera dann automatisch Alarm.

Ein Blick nach England kann uns erahnen lassen, was womöglich noch so alles auf uns zukommen kann. England kann wohl getrost als Mutterland der Videoüberwachung bezeichnet werden. Allein in London sind in den letzten 10 Jahren mehr als 300 Millionen Euro für den Betrieb von 10524 Überwachungskameras in 32 Stadtteilen ausgegeben worden. Obgleich jede Person in London durchschnittlich 300 mal am Tag gefilmt wird und die zum Teil miteinander vernetzten Kameras Personen sogar einander „weiterreichen" können, ist weder die Verbrechensrate gesunken, noch ist die Aufklärungsrate nennenswert gestiegen. Aber diese Ziele werden oftmals auch schon gar nicht mehr verfolgt. Vielmehr geht es in einer anderen britischen Stadt um den Erhalt von Sauberkeit und Ordnung. Wer beim Wegwerfen des Papiertaschentuchs den Mülleimer nicht ganz genau trifft, wird von einer Stimme „aus dem Off" laut und deutlich ermahnt, den Abfall doch bitte schön ordnungsgemäß zu entsorgen. Wäre es nicht so bitter, könnte es als Erfolg gefeiert werden, dass die Ahnungen und Vermutungen Wirklichkeit geworden sind, die auch die Deutsche Vereinigung für Datenschutz immer wieder kritisch als mögliche Entwicklungsszenarien befürchtet hat: Die „sanfte Kontrolle" durch Überwachungskameras hat hauptsächlich Bagatelldelikte, Ordnungswidrigkeiten und das im Blick, was früher ungebührliches Verhalten genannt wurde. Die gesellschaftlichen Wirkungen werden einerseits dem Konformitätsdruck angepasstes Sozialverhalten sein und andererseits die Verdrängung sozialer Randgruppen, ihr Ausschluss aus den sauberen Konsumgegenden und ordentlichen Wohnvierteln.

Jahr für Jahr steigt, nein explodiert die Zahl der Überwachungsmaßnahmen in der Telekommunikation. Die Vorratsdatenspeicherung kommt, so dass künftig die Verkehrsdaten aller Telekommunikationsvorgänge über sechs Monate gespeichert werden. Geht es nach dem Bundesinnenministerium, folgt dem großen Lauschangriff, also der Verwanzung der Wohnung bald die Computerwanze unter der etwas irreführenden Bezeichnung „Online-Durchsuchung". In aller Regel dürfte damit nämlich keine einmalige Durchsicht der Festplatte stattfinden, sondern eine kontinuierliche Überwachung der verschiedensten Betätigungen am Computer über einen bestimmten Zeitraum. Laut gerufen wird nach diesem Instrument zu Strafverfolgungszwecken, was hinsichtlich der Beweiskraft derart gewonnener Erkenntnisse unüberwindbare Probleme aufwerfen dürfte. Die Polizei will es zur Gefahrenabwehr und der Verfassungsschutz zur Terrorismusbekämpfung. Ob dabei die Festplatte nach „Anleitungen zum Bombenbau" durchforstet wird oder verschlüsselt geführte Internettelefonie vor ihrer Ver- und nach ihrer Entschlüsselung abgehört wird (das Stichwort heißt hier Quellen-TKÜ), in beiden Fällen ist im Prinzip der gleiche technische Vorgang gemeint, nämlich der heimliche Zugriff auf die Computerfestplatte.

Das Verfassungsschutzgesetz Nordrhein-Westfalen erlaubt dem Landesverfassungsschutz seit der Jahreswende unter bestimmten Voraussetzungen einen solchen heimlichen Zugriff auf – wie es wörtlich heißt – „informationstechnische Systeme". Dieses Gesetz ist mit Verfassungsbeschwerden angegriffen worden, über die das Bundesverfassungsgericht in Karlsruhe in dieser Woche mündlich verhandelt hat. Aus den Stellungnahmen, die die Sachverständigen für die technischen Fragen dort abgegeben haben, sind zwei Punkte sehr klar geworden: Erstens verändert jeder Zugriff auf die Festplatte unvermeidbar das System. Und zweitens können Systeme, die der Staat infiltrieren kann oder infiltriert hat, auch von anderen Dritten manipuliert werden. Diese technischen Umstände haben die Verhältnismäßigkeit solcher Maßnahmen noch einmal mehr in Frage gestellt. Es kommt hinzu, dass es nicht möglich ist, auf der Festplatte gespeicherte sensible Daten, die den Schutz des Kernbereichs privater Lebensgestaltung genießen, automatisch durch die Technik selbst zu schützen. Wenn zudem noch berücksichtigt wird, dass sich die technisch versierten Personen mit den verschiedensten Maßnahmen wirksam gegen solche Zugriffe schützen können, fragt sich, welchen Erfolg das Instrument noch haben kann. Der einschneidenste Effekt bestünde dann im Abbau unserer Freiheitsrechte.

Den Abbau unserer Freiheitsrechte, den wir allerorten zu verzeichnen haben, begleitet einen Wandel des Staatsverständnisses. Der Rechtsstaat, der eigentlich einen Anlass oder einen Verdacht braucht, um eine Bürgerin oder einen Bürger eingehenderer staatlicher Kontrolle zu unterziehen, wird Stück für Stück zum Präventionsstaat umgebaut, für den wir nicht mehr als unverdächtig, sondern als Risiko gelten. Die innere Logik des Präventionsstaates heißt Maßlosigkeit. Diese Maßlosigkeit kommt nicht nur in der Vorratsdatenspeicherung zum Ausdruck, die anlass- und verdachtslos die gesamte Bevölkerung trifft. Sie zeigt sich bei der flächendeckenden Erfassung aller Kraftfahrzeugkennzeichen ebenso wie bei der Rasterfahndung, der Schleierfahndung, den Finger-abdrücken in den Personalausweisen, der Erfassung und Speicherung von Fluggastdaten sowie der Videoüberwachung, um nur einige Beispiele zu nennen.

Der Entwicklung zum Präventionsstaat Einhalt zu gebieten, ist das Gebot der Stunde und dafür sind solche Organisationen wie die Deutsche Vereinigung für Datenschutz unverzichtbar. Gegen den Abbau unserer Freiheitsrechte, für den Datenschutz und dagegen, die Bevölkerung unter Generalverdacht zu stellen, kämpft die Deutsche Vereinigung für Datenschutz seit nunmehr 30 Jahren unermüdlich. Und das ist gut so, denn der Datenschutz ist ein wesentliches Funktionselement der Demokratie.

Ohne gesellschaftliche Aktionen, Demonstrationen – ich nenne nur die 15.000 Menschen im September in Berlin – und Organisationen wäre auch die Arbeitssituation für uns Datenschutzinstitutionen eine andere. Meine Freude über die Aktivitäten von Bürgerrechtsorganisationen hat selbstverständlich auch ein eigennütziges Element. Je stärker das gesellschaftliche Engagement für den Datenschutz ist, umso besser sind auch die Bedingungen zur Durchsetzung von Datenschutzforderungen in der institutionellen Beratungs-, Aufsichts- und Kontrolltätigkeit. Daher schließt mein umfassender Dank an die Deutsche Vereinigung für Datenschutz auch einen ganz persönlichen Dank mit ein. Toll, dass es sie gibt! Für die nächsten 30 Jahre Engagement für den Datenschutz wünsche ich der Deutschen Vereinigung für Datenschutz viel Energie, Mut, Ausdauer, Spaß und Erfolg! Vielen Dank.

Dr. Dr. h.c. Burkhard Hirsch

Datenschutz als Grundrecht

So viel Zeit muss sein, zunächst der Datenschutzvereinigung zu ihrem 30. Jahrestag zu gratulieren. Ich wünsche ihr, dass sie in weiteren 30 Jahren mit demselben Stolz auf ihre Arbeit zurückblicken wird, wie sie das heute tun kann.

Thilo Weichert hat in seinem Artikel „Dreißig Jahre sind nicht genug“ [1] das Auf und Ab dieser Jahre, die Erfolge und Hoffnungen zutreffend und mit großer Sympathie beschrieben. Ich schließe mich ihm an und unterstreiche seine Forderung, grundrechtsorientierten Organisationen in der Informationsgesellschaft ähnliche Rechte einzuräumen wie den Verbraucher- und den Umweltverbänden - also die Beteiligung an Entscheidungsprozessen und Verbandsklagerechte.

„Privatheit und Persönlichkeitsschutz“ schreibt Weichert, sind eben nicht mehr Privilegien gehobener Gesellschaftsschichten, sondern Existenzbedingung einer demokratischen und rechtsstaatlichen Informationsgesell schaft“. So ist es und damit ist eigentlich alles Wesentliche gesagt.

Leider besteht keine Veranlassung, sich beruhigt zurückzulehnen.

Schon vor dem 11. 9. 2001 haben wir Jahrzehnte wachsender staatlicher und privater Begehrlichkeiten nach personenbezogenen Daten erlebt – aus wachsender Kriminalitäts- und Terrorismusfurcht, aus natürlich stets wohlmeinender staatlicher Fürsorge, aus administrativen Vereinfachungswünschen, aus Perfektionismus und aus dem ökonomischen Wunsch, Risiken zu minimieren und Gewinne zu maximieren.

Diese Wünsche, Begehrlichkeiten und Forderungen sind mit den technischen Möglichkeiten und der lawinenartigen Verbreitung der öffentlichen und privaten Datenverarbeitung immer größer geworden. Ein Ende ist nicht abzusehen, im Gegenteil! Seit dem 11. 9. 2001 werden insbesondere die staatlichen Instrumente in einem kaum noch zu übersehenden Umfang vervielfältigt. Dem sog. Großen Lauschangriff folgten die sog. Sicherheitsgesetze, der weitere Ausbau der Telekommunikationsüberwachung, die Überwachung von Kontobewegungen und Postdienstleistungen, die Standort - Ortung von Handys und der sog. IMSI-Catcher, gemeinsame Dateien von Polizeien und „Diensten“, umfangreiche Sicherheitsüberprüfungen, die biometrische Erfassung der in bestimmten Ländern lebenden Bewerber um ein Visum und die nachrichtendienstliche Beurteilung ihrer Einlader, die biometrischen Merkmale in den Ausweispapieren, die präventive Telefonkontrolle, die Rasterfahndung mit dem absurden Fahndungskriterium, dass die gesuchten „Schläfer“ bisher polizeilich nicht in Erscheinung getreten sind – die Unbescholtenheit als besonderes Verdachtsmoment! Man kann die Aufzählung fortsetzen und dabei die online Überwachungen von PC´s und die Vorratsdatenspeicherung nicht vergessen.

Man weiß nicht, was man mehr bewundern soll, den Erfindungsreichtum der handelnden Personen in Politik und Verwaltung oder die Unverfrorenheit, mit der auf die Privatheit des anderen zugegriffen wird. Als wir in der mündlichen Verhandlung zum sog. Großen Lauschangriff fragten, ob man denn z.B. auch das Schlafzimmer verwanzen müsse, antwortete einer der Sachverständigen: Ja, genau das müsse man machen. Denn wenn die Leute miteinander schlafen, dann fassen sie ja gerade Vertrauen zueinander – und dann fangen sie an zu reden! Das sind so Momente, in denen man sich als Anwalt über einen ehrlichen Sachverständigen freut.

In der Rhetorik mancher Politiker wurden die „Datenschützer“ zu einer Art vergangenheitsbezogener Trachtengruppe, die nicht begreifen will, dass der nichts zu befürchten habe, der nichts zu verbergen hat. Dabei vergaßen sie, dass man mit derselben Logik die klassischen Datenschutzrechte, wie das Beichtgeheimnis, die beruflichen Versc hwiegenheitspflichten, Zeugnisverweig erungsrechte, die Un-schuldsvermutung bis hin zu dem Verbot, unter Zwang,

1 vgl. DANA 07, S.56 ff.

Täuschung oder Drohung zu vernehmen, als Hindernisse einer effektiven Gefahrenverhütung und Strafverfolgung diskreditieren und ihre Abschaffung verlangen könnte.

Das ist keine Theorie, die in einer Demokratie westlicher Prägung nicht verwirklicht werden könnte. Es ist die Wirklichkeit in den Vereinigten Staaten unter dem USA Patriot Act, und nicht nur dort. Diese Gedanken tauchen auch in manchen Forderungen auf, die aus dem sog. Feindstrafrecht des Bonner Strafrechtlers Jakobs entwickelt werden oder aus der Vorstellung, daß wir uns in einem „asymmetrischen Krieg" befänden, in dem weder das humanitäre Kriegsvölkerrecht, noch das traditionelle europäische Rechtssystem etwas zu suchen habe. Kriegsrecht im Inland bedeutet, dass die Regierung das Recht haben will, das Kriegsrecht im Verhältnis zur eigenen Bevölkerung anwenden zu können – ein bemerkenswerter Vorgang.

Die elementare Bedeutung des Rechts auf Privatheit und des Rechts auf informationelle Selbstbestimmung für eine funktionsfähige Demokratie ist erst spät erkannt worden.

Im Wortlaut des Grundgesetzes ist vom Datenschutz oder vom Schutz der Privatheit bekanntlich keine Rede. Die Verfassungsgeber hielten sich an den klassischen Katalog der Menschen- und Freiheitsrechte. Sie hätten gewarnt sein können. In der amerikanischen Literatur tauchen schon gegen Ende des 19. Jhdts. in den Schriften von Brandeis, Warren und Cooley die Begriffe „privacy" und das „right to be let alone" – das Recht, in Ruhe gelassen zu werden – auf. Sie vertreten die Auffassung, daß das Common Law jedem Individuum das Recht einräume, regelmäßig selbst zu bestimmen, in wieweit seine Gedanken, Meinungen und Gefühle anderen mitgeteilt werden sollen.[2]

Der Weg selbst zu einer einfachgesetzlichen Regelung der Datenverarbeitung war in Deutschland lang und steinig. Es hatte schon Ende der 60er Jahre massive Versuche zur Einführung einer zentralen, bundesweiten und umfassenden Informationsbank für Verwaltung, Polizei, Statistik und Wissenschaft gegeben, als die Datenschutzgesetzgebung allmählich einsetzte, in Hessen 1970, in Schweden 1973, im amerikanischen Privacy Act von 1974, dem kanadischen Human Rights Act von 1977.

Am Bundesdatenschutzgesetz haben wir von 1970 bis 1977 gearbeitet, von Anfang an unter den heftigsten Beschwörungen von Verwaltung und Wirtschaft, dass jeder geordnete und bezahlbare Geschäftsablauf unter der Belastung mit einer reglementierten Datenverarbeitung unweigerlich und unverzüglich zusammenbrechen würde, eine Schreckensvision, an der sich auch die Bundesbank beteiligte. Es war schließlich leichter, in NRW mit einer fortgeschrittenen, aber natürlich streng in Statistik, Verwaltung und Kriminalpolizei getrennten Datenverarbeitung ein Datenschutzgesetz zu machen und den Datenschutz in der Landesverfassung zu verankern, als in Bonn das Bundesgesetz durchzusetzen.

Es gibt dazu keine Alternative. Wenn der Staat nicht den Charme eines blankgeputzten Räderwerks bekommen soll, dann muss man dafür sorgen, dass er menschlich bleibt, dass er nicht allmächtig und allwissend wird, dass er vergessen kann, dass der Bürger vor ihm nicht wie bei einer Musterung nackt dasteht, sondern seine selbstbestimmte Individualität erhalten kann. Die Möglichkeiten der elektronischen Datenverarbeitung verlangen ein Umdenken wie bei der Montesquieu'schen Gewaltenteilung. Da kündigte sich die Entscheidung an, die bis heute immer wieder gefordert wird, nämlich zwischen Effektivität und Wirtschaftlichkeit auf der einen Seite und Rechtsstaatlichkeit auf der anderen. Man muß zwischen Freiheit und Sicherheit entscheiden, was für das Persönlichkeitsrecht unverzichtbar ist und was dem Allgemeininteresse entspricht.

Seit Jahren wird immer wieder versucht, diese Entscheidung mit dem schlichten Argument zu verschleiern, dass es einen Paradigmenwechsel gebe, dass ein Schutz gegen den demokratisch verfassten Staat überholt sei, da wir ja selbst mit ihm identisch seien und dass es die wichtigste Aufgabe des Staates sei, für die Sicherheit des Bürgers zu sorgen. Er sei Sicherheitspartner geworden.

Das ist eine Selbsttäuschung. Der Staat ist kein Partner, sondern die auf Durchsetzung angelegte Rechtsordnung einer arbeitsteiligen Gesellschaft. Dass es die Aufgabe des Staates ist, den Bürger vor privater Gewalt zu schützen, ist nun wirklich nicht neu. Das wissen wir seit dem Mainzer Ewigen Landfrieden von 1495. Wir wissen auch, dass staatliche Macht nicht nur in einer Volksdemokratie, sondern auch in einer Demokratie westlicher Prägung ausgeübt wird, auf eine definierte Zeit und gesetzlich kontrolliert. Darum bleibt es eine völlig unveränderbare Aufgabe, dafür zu sorgen, dass es eine rechtsstaatliche Demokratie bleibt. Das Recht und die Gesetze müssen den Bürger ermutigen und befähigen, diesen Staat zu bejahen und in ihm Verantwortung zu übernehmen. Wo Macht ist, ist auch der Wille, sie zu gebrauchen und die Versuchung, sie zu mißbrauchen. Darum gibt es kein Recht des Bürgers auf absolute Sicherheit, das den Staat dazu legitimiert könnte, alle anderen Rechte der Bürger einzuschränken. Sicherheit ist eine Hilfsfunktion, die dem Bürger dazu dienen soll, im sicheren Besitz seiner Freiheit zu sein – wie Wilhelm v. Humboldt formuliert hat – mit der Folge, dass der Staat zur Sicherheit seiner Bürger eben nur die Mittel einsetzen darf und kann, die ihm die Verfassung erlaubt.

Es ist das Verdienst des Bundesverfassungsgerichts, daß es in seiner denkwürdigen Entscheidung zum Volkszählungsgesetz den Gedanken eines Rechts zur informationellen Selbstbestimmung aufgegriffen und es zu einem auf den Art. 1 und 2 GG, also auf der Menschenwürde und dem Recht zur freien Entfaltung der Persönlichkeit beruhenden Grundrecht gemacht hat. Wer damals hoffte, es handele sich um eine alsbald revidierte Einzelentscheidung, täuschte sich gründlich. Das Urteil war die konsequente Fortsetzung einer ständigen Rechtsprechung, die der

2 zitiert nach Bull, Datenschutz oder Die Angst vor dem Computer, Piper 1984, S. 78.

Menschenwürde, der Privatheit und der Selbstbestimmung den Vorrang vor Effektivität und Perfektionismus gab.[3]

Auch der Begriff „informationelles Selbstbestimmungsrecht“ war nicht neu, sondern von Steinmüller, Podlech, Denninger und anderen in der wissenschaftlichen Literatur eingeführt und sogar schon einmal in einem Urteil des Bundesverfassungsgerichts verwendet worden.[4]

Alle unsere späteren Bemühungen, dieses im Kern bürgerlich – liberale Grundrecht ausdrücklich in der Verfassung zu verankern, blieben erfolglos und scheiterten im Bundestag – zuletzt nach der Wiedervereinigung in der Gemeinsamen Verfassungsreformkommission des Bundes und der Länder 1993 am Widerstand einer konservativen Minderheit. Deren Hauptargument war formal. Es sei doch durch die Rechtsprechung alles hinreichend geregelt, ein offenkundig vorgeschobener Grund. Nichts kennzeichnet den demokratischen und bürgerrechtlichen Kern der Privatheit mehr als die Tatsache, dass die sog. neuen Bundesländer einschließlich Berlins nach ihren Erfahrungen in der DDR sämtlich die informationelle Selbstbestimmung in ihre Verfassungen aufgenommen haben – wie übrigens auch die Bundesländer Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und das Saarland.[5]

Es verdient hervorgehoben zu werden, dass der Datenschutz in der Grundrechts-Charta der EU und dementsprechend in den Verfassungsvertragsentwurf als Art II - 68 aufgenommen wurde.

Und das Bundesverfassungsgericht beschreibt das informationelle Selbstbestimmungsrecht[6] als ein auf Art. 1 und 2 gegründetes allgemeines Persönlichkeitsrecht und räumt ihm damit einen verfassungsrechtlich hohen Rang ein.

Ich bin alarmiert durch einen Aufsatz Hassemers, des früheren hessischen Datenschutzbeauftragten und jetzigen Vizepräsidenten des Bundesverfa ssungsgerichts, den er unter dem Titel „Partner Staat“ unlängst in einer großen Tageszeitung veröffentlicht hat.[7] Darin vermutet er den Niedergang des Datenschutzes. Er gehöre nicht mehr zum Kernbereich des Rechtsstaates. Der Wunsch nach Wahrung der Privatheit habe rapide abgenommen. Der Staat sei zum Genossen im Kampf gegen die Risiken der modernen Welt geworden. Der Bürger rufe nach Ausweitung der Kontrollen und verstehe nicht mehr, warum die Daten der Nachrichtendienste, Sozialverwaltungen, Fluglinien und Polizeien nicht zusammengeführt werden sollten. Die Sicherheitsoption sei vorrangig geworden.

Es ist schwer zu sagen, ob der Schluss dieses Artikels nur eine Verbeugung vor der Vergangenheit ist, oder doch ein Bekenntnis. Das informationelle Selbstbestimmungsrecht beruht nach Hassemer auf zwei Grundlagen: auf der philosophischen Begründung der bürgerlichen Freiheit und dem pragmatischen Sinn für die Entwicklung der Moderne. Für den Schutz der Privatheit streite das Freiheitspathos, das die hohe Rechtskultur begründet habe, in der die Traditionen der Aufklärung noch lebendig sind. Der Datenschutz sei nichts anderes, als diese Freiheit, gespiegelt an den Bedingungen der modernen Inform ationsgesellschaft.[8]

Noch vor wenigen Jahren hatte Hassemer zum Spannungsverhältnis von Freiheit und Sicherheit zwar dargestellt, dass sich dieses Spannungsverhältnis zum Pol der Sicherheit bewege und dass das zu Lasten der Freiheit gehe. Und dann formuliert er die These:

„Vor diesem Hintergrund ist es an der Zeit, für die Verwirklichung der Grundrechte in einer auf Prävention und Sicherheit ausgerichteten Gesellschaft aktiv und offensiv zu werben. Die bittende Warnung, bei der Herstellung innerer Sicherheit die Grundrechte nicht allzu sehr in Mitleidenschaft zu ziehen, ist gut gemeint, aber nicht hinreichend.“[9] Es ist zweifellos richtig, dass ein Teil unserer Mitbürger nicht die geringsten Hemmungen hat, mit persönlichen Daten herumzustreuen wie eine Pusteblume. Da werden ganze Großraumabteile des ICE mit dem Handy akustisch zugemüllt. Andere lassen es sich gefallen, in bestimmten Fernsehsendungen zum Kasper gemacht zu werden, indem sie intimste Details verkünden oder sich entlocken lassen und sie auch noch ins Internet stellen. Es ist schwer zu sagen, ob das Dummheit, Geltungsbedürfnis oder eine Art Autismus ist, dem es gleichgültig ist, was andere sehen, hören und ohnehin nach 10 Minuten vermutlich vergessen haben werden. Rechtlich geben diese Zeitgenossen ihr informationelles Selbstbestimmungsrecht nicht auf, sondern machen von ihm in großzügigster Weise Gebrauch. Sie entscheiden selbst, was sie von sich preisgeben und was nicht. Mit anderen Worten: das Absinken der Schamgrenze bei vielen Mitbürgern berechtigt den Staat keineswegs, auch für alle anderen den Datenschutz als obsolet oder geringwertig zu betrachten und ihn als ein nachrangiges Rechtsgut zu behandeln.

Es ist richtig, wenn Hassemer feststellt, dass das Sicherheitsbedürfnis in einer Weise vorherrschend geworden ist, die man noch vor wenigen Jahren für undenkbar hielt. Keine der zahlreichen Zumutungen staatlicher Schnüffelei, Überwachung, Ausforschung, Datensammlung, vom Lauschangriff bis zur heimlichen PC- Überwachung – irreführend onlinie-Durchsuchung genannt –

3 vgl. BVerfGE 65, 1 ff; E 54, 148 (153) Eppler; E 27 1 Mikrozensus; E 27, 344 (350) Scheidungsakten; E 32, 373 (379) Arztkartei; E 34 238 (245) Heiml. Tonbandaufnahme 34 238 (246) Recht am gsprochenen Wort, E 34, 269 (282) Soraya; E 56 37 (41) Selbstbezichtigung; E 63, 131 (142) Gegendarstellung.

4 vgl. die Nachweise bei Denninger, Das Recht auf informationelle Selbstbestimmung und Innere Sicherheit, in v. Schoeler (Hrsg), Informationsgesellschaft oder Überwachungs-staat ? 1986, S. 108 ff, 111; BVerfG (1981) E 57, 170 ff, 201, Sondervotum M. Hirsch.

5 Die Formulierungen differieren z.T. erhelich, legen aber stets fest, daß ein Eingriff in das Recht auf informationel le Selbstbestimmung nur durch oder auf Grund eines Gesetzes erfolgen dar, das im überwiegenden Allgemeininteresse erforderlich ist. Verschiedentlich weren auch Informations- und Kontrollrechte begründet.

6 vgl. z.B. BVerfG zur Abfrage v. Kontostammdaten, Beschl. v. 13. 6. 07 NJW 07, 2464 ff

7 vgl, FAZ v, 5. 7. 07, S. 6

8 vgl. Hassemer a.a.O..

9 vgl. Hassemer, Zum Spannungsverhältnis von Freiheit und Sicherheit, in Vorgänge 159, S. 10 ff.

ist bisher am geschlossenen Widerstand der Bevölkerung gescheitert. Selbst in juristischen Fachzeitschriften wurde die Möglichkeit der Folter als ultima ratio ernsthaft erörtert. Man kann lange überlegen, ob dieses Sicherheitsdenken das typische Kriterium einer bürgerlichen Wohlstandsgesellschaft ist oder mit dem Vorrang der Effektivität in einer ökonomisch determinierten Gesellschaft zusammenhängt.

Aber man kommt auch an der Be-obachtung nicht vorbei, daß die Haltung des Bürgers wesentlich davon abhängt, ob er glaubt, von den jeweils geforderten staatlichen Eingriffsmöglichkeiten selbst berührt zu werden oder nicht. Viele Bürger sind der Überzeugung, daß es sie schon nicht treffen werde. Sie haben zwar ein Privatleben, - und damit etwas zu verbergen -, aber eben nichts, was die staatliche Aufmerksamkeit auf sie ziehen würde. Sie möchten mehr Sicherheit auf Kosten der Freiheit anderer. Transparenz ist gut, wenn sie sich auf den anderen bezieht. Es ist eine Art politischer Zechprellerei. Sie haben nicht verstanden, dass es keine individuelle Freiheit ohne gesellschaftliche Freiheit gibt. Es ist nicht in das öffentliche Bewusstsein gedrungen, dass manche moderne Überwachungsinstrumente weder einen konkreten Anlass, noch eine strafbare Handlung voraussetzen – typische Merkmale des Wandels zu einem Präventions- und Überwachungsstaat. Dessen polizeiliches Ideal besteht ja gerade darin, nach Möglichkeit „vor dem Täter am Tatort zu sein“, den potentiellen Täter und seine Kontaktpersonen schon im Vorfeld zu ermitteln und zu beobachten, mit anderen Worten, schon die Absicht zur Tat zu machen.

Dieser Weg ist nicht unausweichlich. Ermutigung sehe ich allerdings weniger in der gegenwärtigen Gesetzgebung als in der Rechtsprechung des Bundesverfassungsgerichts. Die Reaktionen des Gesetzgebers auf die neueren Entscheidungen des Gerichts waren eher zähneknirschend bis halbherzig. Und er fährt ungerührt fort, die Zweckbindung gespeicherter Daten aufzulockern und zentrale Speichersysteme aufzubauen, deren Missbrauch man mit absoluter Sicherheit voraussehen kann, wie bei der Vorratsdatenspeicherung oder der Steueridentifikationsnummer – früher und in der DDR als „einheitliches Personenkennzeichen“ bezeichnet.

Das Bundesverfassungsgericht hat jedoch in einer Reihe von Entscheidungen an seiner bisherigen Linie überzeugend festgehalten. Bei den Entscheidungen zum Großen Lauschangriff und zum Zollkriminaldienst hat es einen unantastbaren Kern der privaten Lebensführung anerkannt, der keiner Abwägung mit anderen Interessen unterworfen werden kann. Es hat den Schutz der Privatheit auch für engste persönliche Vertraute außerhalb der eigentlichen Familie akzeptiert, enge Verfahrensregeln und die Benachrichtigung aller von einem Lauschangriff betroffenen Personen vorgeschrieben. In dem Urteil zur präventiven Telefonkontrolle nach dem niedersächsischen Polizeirecht hat es die Ausforschung des sog. Vorfelds durch die Voraussetzung begrenzt, dass ein auf Tatsachen gestützter konkreter Tatverdacht vorliegen muss. Für die vorbeugende Rasterfahndung verlangt das Gericht eine konkrete Gefahr für hohe Rechtsgüter. In der Entscheidung zum Luftsicherheitsgesetz hat es den absoluten Vorrang der Menschenwürde nachhaltig bekräftigt. Gespannt sehen wir der Entscheidung zu dem nordrhein-westfälischen Gesetz zur Computer - Überwachung entgegen, das ich nach Stil und Inhalt für haarsträubend halte. Die mündliche Verhandlung vorgestern in Karlsruhe war für Nordrhein-Westfalen und die Vertreter von Landesregierung und Landtag von äußerster Peinlichkeit.

An Bundesregierung und Bundestag kann man nur appellieren, endlich damit aufzuhören, die Belastbarkeit der Verfassung auszuprobieren. Die Geringschätzung des Grundrechts auf Datenschutz stärkt nicht etwa den Staat, sondern beginnt, ihm wesentliche Teile der Gesellschaft zu entfremden. Wir wünschen uns, dass die teilweise atemberaubenden Berichte der Datenschutzbeauftragten nicht als lästige Zwischenrufe, sondern als ernsthafte Aufforderung und Anlass zur Beseitigung von Missständen verstanden und aufgenommen werden. Wir wünschen uns, dass die Datenverarbeitung im privaten Bereich angesichts der neuen technischen Entwicklungen wesentlich transparenter gemacht wird als bisher. Wir möchten, dass die Arbeit der betrieblichen Datenschutzbeauftragten erleichtert wird. Ebenso wie zu jedem veröffentlichungspflichtigen Geschäftsbericht das Testat des Wirtschaftsprüfers gehört, sollte die Aufnahme eines Berichts des Datenschutzbeauftragten selbstverständlich werden, auch im Interesse der Arbeitnehmer, für die natürlich ein bereichsspezifischer Datenschutz formuliert werden kann, wenn man es wirklich will.

Mit anderen Worten: Wir wünschen uns, dass Regierung und Parlament unsere Grundrechte und unsere persönliche Freiheit nicht als Bremsklotz und Belästigung betrachten, sondern sie respektieren und dass sie denselben Stolz auf unsere freiheitlichen Traditionen empfinden wie wir und die Richter in Karlsruhe.

Dr. Thilo Weichert

30 Jahre Bundesdatenschutzgesetze

I. Erste Generation

Die Gründung der Deutschen Vereinigung für Datenschutz e.V.[1] hängt eng zusammen mit der Datenschutzgesetzgebung in Deutschland. So kommt es, dass diese Bürger-rechtsorganisation und das Bundesdatenschutzgesetz (BDSG) fast zeitgleich den 30. Geburtstag feiern können.[2] Richtigerweise kann nicht von einem BDSG, sondern müsste von „den" Bundesdatenschutzgesetzen gesprochen werden, nämlich denen von 1977, von 1990 und von 2001.

Das erste BDSG, das „Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung" vom 27.01.1977[3] trat am 01.01.1978 in Kraft.[4] Es gehörte der 1. Generation von Datenschutzgesetzen an, die keine umfassende Gestaltung der personenbezogenen Datenverarbeitung anstrebten, sondern lediglich eine Missbrauchsbekämpfung und dies fast ausschließlich in Bezug auf die elektronische Verarbeitung, also der Umgang mit personenbezogenen Daten, die „in Dateien gespeichert, verändert, gelöscht oder aus Dateien übermittelt werden" (§ 1 Abs. 2 S. 1 BDSG ´77).

Das BDSG ´77 reihte sich bei Datenschutzgesetzen ein, die auf Länderebene teilweise schon erheblich früher entstanden waren. Dies gilt - allen voran und als erstes Datenschutzgesetz weltweit - für das Hessische Datenschutzgesetz aus dem Jahr 1975 oder das „Gesetz gegen missbräuchliche Datennutzung (Landesdatenschutzgesetz)" Rheinland-Pfalz von 1974[6]. Der Bund sollte auch in der Zukunft bis zum heutigen Tag in Bezug auf die Modernisierung in diesem Rechtsgebiet immer einigen fortschrittlicheren Ländern hinterherhinken. Die föderale Führungsrolle wurde zunächst von Hessen wahrgenommen, angeleitet durch dessen zweitem Datenschutzbeauftragten Spiros Simitis von 1975 bis 1991.

Der Schwerpunkt der Regelungen lag im öffentlichen Bereich, über den es schon eine intensive Debatte gab. Diese führte dazu, dass - entgegen ersten Planungen - kein zentrales Melderegister in Deutschland eingerichtet wurde und dass einheitliche Personenkennzeichen (PKZ) als verfassungswidrig abgelehnt wurd.[7] Die Menschen waren sensibilisiert durch Affären wie die um das Abhören des Atomwissenschaftlers Klaus Traube im Zusammenhang mit den Ermittlungen gegen den Terrorismus der Roten Armee Fraktion (RAF) oder durch die Kontrollphantasien des damaligen Präsidenten des Bundeskriminalamtes Horst Herold.[8] Doch nicht nur der staatliche große Bruder war in den Fokus eines technikkritischen liberalen Bürgertums geraten, das die zentralisierte Verarbeitung in Großrechnern als Bedrohung empfand, sondern auch schon die Privatwirtschaft, insbesondere in Form von Auskunfteien und Adressenhändlern.[9]

Das BDSG ´77 hatte mit allen seinen Nachfolgern gemein, dass schon vor seiner Verabschiedung dessen baldige Novellierung gefordert wurde, weil es nicht mehr technikadäquat wäre, und, dass es davon unbeeindruckt erst nach vielen Jahren wirklich novelliert wurde

Zu seiner Ehrenrettung muss aber auch festgehalten werden, dass es einige Instrumente bereitstellte, die sich etablierten und für gut erwiesen, so z.B. die Verpflichtung zur Einrichtung betrieblicher Datenschutzbeauftragter (§§ 28 f. BDSG ´77) oder ein schon relativ weit gehender Auskunftsanspruch der Betroffenen, selbst im nicht-öffentlichen Bereich (§§ 13, 34 BDSG ´77).

II. Der Beginn der zweiten Generation

Das Ende der ersten Generation der reinen Missbrauchsverhinderungsgesetze wurde eingeläutet mit der Reaktion des Bundesverfassungsgerichtes (BVerfG) auf den Widerstand gegen die geplante Volkszählung im Jahr 1983.[10] Aus der gesetzlichen Konkretisierung des allgemeinen Persönlichkeitsrechtes nach den Art. 2 Abs. 1 i.V.m. 1 Abs. 1 GG wurde ein eigenständiges Grundrecht entwickelt, das „Recht auf informationelle Selbstbestimmung".[11] Eingriffe bedurften nun einer gesetzlich hinreichend bestimmten Grundlage. Auch die private Datenverarbeitung wurde bald danach durch das BVerfG vom Grundrechtsschutz mit erfasst.[12] Revolutionär war, dass das BVerfG die zu jeder Relativierung einladende, bisher geltende Schwellentheorie[13] und ebenso die bisher von ihm selbst ver-

1 Zur Geschichte der DVD Weichert DANA 2/2007, S. 56.

2 Historische Darstellungen des Datenschutzrechtes finden sich z.B. bei Simitis in Simitis, Bundesdatenschutzgesetz, 6. Aufl. 2006, Einleitung, Rz. 1-126; Abel in Roßnagel, Handbuch Datenschutzrecht, 2003, S. 194.

3 BGBl. I S. 201.

4 Zur Vorgeschichte instruktiv Steinmüller RDV 2007, 159; ders. FIfF-Kommunikation 3/2007, 17.

5 Hess. GVBl. 1970, 625.

6 GVBl. Rh. Pf. 1974, 84.

7 Kirchberg ZRP 1977, 137; Weichert RDV 2002, 172; Bizer DuD 2004, S. 45.

8 Herold, Interview mit Sebastian Cobler, Transatlantik 11/1980, S. 29.

9 Weichert DANA 2-1996, 4.

10 BVerfGE 65, 1 = NJW 1984, 419.

11 Zur Genese des Grundrechts Steinmüller RDV 2007, 158.

12 BVerfG NJW 1991, 2411.

13 Weichert, Informationelle Selbstbestimmung und strafrechtliche Ermittlung, 1990, S. 27.

tretene Sphärentheorie[14] aufgab und jede Form der Verarbeitung, selbst im öffentlichen Bereich und bei „Bagatellen" für grundrechtsrelevant erklärte. Selbst auf das Erfordernis der automatisierten Verarbeitung wurde für die Annahme eines Eingriffs weitgehend verzichtet. Mit dem Hinweis auf die Notwendigkeit verfahrensrechtlich-organisatorischer Vorkehrungen zum Grundrechtsschutz schuf das BVerfG zudem die Grundlage für die technischen und prozeduralen Schutzmaßnahmen.

Die Debatte um die Novellierung des Datenschutzrechtes wurde derzeit fast ausschließlich rechtlich geführt. Sie war bestimmt von der Frage, wie lange der Übergangsbonus für gesetzlose Datenverarbeitung gelten kann[15] und wie am besten die vorhandene Datenverarbeitung durch mehr oder weniger spezifische Regelungen legitimiert werden könne. Reinhard Riegel, Festredner der DVD-Tagung 1989 in Bonn und Referent beim Bundesbeauftragten für den Datenschutz (BfD) für den Sicherheitsbereich, war der vielschreibende Protagonist der Vergesetzlichung, die sich im Nachhinein in mancher Hinsicht als Vergesetzlichungsfalle erwies.[16]

Diese Falle konnte darin gesehen werden, dass der Gesetzgeber wegen der verfassungsrechtlichen Notwendigkeit von spezifischen Eingriffsregelungen - um nichts unzulässig sein zu lassen, was der Verwaltung sinnvoll oder notwendig erschien - alles und jedes zu erlauben versuchte. Dies führte letztlich 1990 nicht nur zu einem neuen BDSG, sondern in einem Paket zu den damals als viel zu weit gehend empfundenen Sicherheitsgesetzen, mit denen u.a. dem Bundeskriminalamt (BKA), dem Bundesamt für Verfassungsschutz (BfV), dem Militärischen Abschirmdienst (MAD) und dem Bundesnachrichtendienst (BND) Rechtsgrundlagen für deren Datenverarbeitung geschaffen wurden.[17] Es war nicht nur – wie heute regelmäßig über die Medien kolportiert wird – die geplante Volkszählung, sondern es waren die Entwürfe dieses Sicherheitspaketes aus dem Haus des Innenministers Friedrich Zimmermann, die den Widerstand gegen den zweiten Volkszählungsversuch 1987 anfeuerten.[18]

Der Verrechtlichungsdruck hatte aber auch seine positiven Seiten: Er zwang zur gesellschaftlichen Offenlegung der Begehrlichkeiten bei der Datenverarbeitung. Er zwang zudem zur bereichsspezifischen Eingrenzung der erforderlichen Datensätze sowie zur Suche nach bereichsspezifischen Verfahrensanforderungen und nach technisch-organisatorischen Sicherungen. Insofern bewirkte der Zwang zur Regelung in dieser Entwicklungsphase die schmerzhafte wie heilsame Übung für die Verwaltung, ihre Datenverarbeitung aus dem Arkanbereich in die Öffentlichkeit zu holen.

Bei der Verrechtlichung wurden einige Irrwege beschritten. Der eine bestand darin, alles umfassend bereichsspezifisch in einer Vollregelung festlegen zu wollen. Das BDSG bzw. generell das allgemeine Datenschutzrecht sollte zur subsidiären, tendenziell überflüssig werdenden Auffangregelung werden. Während dieser Versuch im Sozialrecht – der schon im Jahr 1975 begann[19] und sich durch die umfassende Normierung um das Sozialgeheimnis des § 35 des Sozialgesetzbuches I (SGB I) und mit der Konkretisierung im SGB X[20] fortsetzte – noch einigermaßen konsistent war, arteten entsprechende Bestrebungen in anderen Bereichen, z.B. im Strafvollzugsrecht in gesetzgeberischen Extremismus aus.[21] Die Einsicht, dass vieles Spezifische dann doch nicht im Gesetz geregelt werden kann, weil es zu sehr der technischen und gesellschaftlichen Entwicklung ausgesetzt ist, lief zudem darauf hinaus, Regulierungen per Rechtsverordnung (RVO) vorzunehmen, etwa zu regelmäßigen Datenübermittlungen oder zu automatisierten Abrufverfahren. Bei diesen Bestrebungen wurde zumeist nur ein beschränkter Grundrechtsschutz erreicht: Auch dieses Regelungskonzept erwies sich oft als nicht flexibel genug, und die Normen wurden dann einfach schlicht nicht mehr beachtet.[22] Oder die Verwaltung, für den Erlass der sie beschränkenden RVOs selbst zuständig, genehmigte sich all das, was sie zu benötigten glaubte.

III. Die Not mit der zweiten Generation

Das BDSG ´90 setzte den vom BVerfG formulierten Gesetzesvorbehalt um. Letztlich wurde dabei weitgehend auf Generalklauseln zurückgegriffen. Doch brachte das Gesetz auch einige Eingrenzungen und Präzisierungen.

14 Weichert, Informationelle Selbstbestimmung (Fn. 13), S. 13.

15 Alberts ZRP 1987, 193, Simitis NJW 1989, 21; Vogelsang DVBl. 1989, 962.

16 Nachweise zu dessen Veröffentlichungen in Weichert, Informationelle Selbstbestimmung (Fn. 13), S. 243 f.; siehe Nachruf von Weichert DANA 1/2000, 15.

17 BDSG v. 29.12.1990, in Kraft seit 01.06.1991, BGBl. I S. 2955.

18 Vgl. z.B. die Dokumentation in Bürgerrechte & Polizei Cilip 23 (1/1986).

19 BGBl. I S. 3015.

20 SGB X v. 18.08.1980, BGBl. I, 1469, ber. 2318.

21 Weichert in Feest, Kommentar zum Strafvollzugsgesetz (AK-StVollzG), 5. Aufl. 2006, vor § 179 Rz. 15 ff., § 187 Rz. 1 ff.

22 Die letzte Rechtsbereinigung erfolgte insofern mit der Novellierung des BbgDSG Ende 2007, Krempl www.heise.de 15.11.2007.

Dessen innovatives Potenzial hielt sich aber in Grenzen, weshalb z.B. die DVD die Novellierung als zu kurz gesprungen ansah und umgehend eine Modernisierung forderte, die eine adäquate Reaktion auf die Kleinrechnertechnologie, auf die Vernetzung und auf die komplexe Auswertbarkeit der Daten sein sollte.[23]

Die Notwendigkeit eines modernen Datenschutzrechtes war inzwischen auch in Europa angekommen, wo die ungebremste Datenverarbeitung und die damit einher gehende Beeinträchtigung der Menschen sowie die in Reaktion hierauf erlassenen Gesetze als Hindernisse für die Verwirklichung des europäischen Informations-Binnenmarktes empfunden wurden. Die langwierigen und sehr kontrovers geführten Diskussionen über eine Europäische Datenschutzrichtlinie (EU-DSRL) waren mit deren Erlass im Jahr 1995 erfolgreich.[24] Neben inzwischen Bewährtem wie dem allgemeinen Verbot mit Erlaubnisvorbehalt, der Zweckbindung oder den Regelungen zur Datenverarbeitung im Auftrag wurden die positiven Erfahrungen mit den betrieblichen Datenschutzbeauftragten nach Europa exportiert und einige für das deutsche Recht neue Regelungsansätze eingeführt, die durchgängig als befruchtend und modern zu bewerten sind.[25]

Als Maßnahme des präventiven Datenschutzes wurde die Vorabkontrolle (Art. 20 EU-DSRL) eingeführt, die zu einer frühen Implementierung des Datenschutzes in neue EDV-Verfahren zwingt und insofern weit über die rein dokumentarische Funktion des Dateiregisters der damaligen §§ 26 Abs. 5, 32 BDSG ´90 hinausging. Bis heute in Deutschland noch nicht nutzbar gemachtes Potenzial liegt in den in Art. 27 EU-DSRL normierten Verhaltensregeln, die später in § 38a BDSG nur eine unzureichende Umsetzung gefunden haben. Mit dem bis dahin im deutschen Recht unbekannten Verbot automatisierter Einzelentscheidungen (Art. 15 EU-DSRL) wurde zum ersten Mal das Problem adressiert, dass die elektronische Datenverarbeitung (EDV) eine Eigendynamik entwickeln kann, mit der sich diese von personalen Bestimmungen freimacht (vgl. jetzt § 6a BDSG).

Die Praxis der Datenverarbeitung sowie die Gesetzgebung nahmen die Modernisierungsangebote der EU-DSRL teilweise nicht an. Die Vorabkontrolle wurde in einem Absatz 5 (des § 4d BDSG) versteckt und wird bis heute als ein formales bürokratisches Erfordernis wahrgenommen, nicht als ein Bestandteil eines Datenschutzmanagements[26], über das schon zu einem frühen Zeitpunkt der Systemgestaltung materiell Datenschutz integriert werden kann.[27] Die Möglichkeiten der Verhaltsregeln für die Schaffung von bereichsspezifischer Rechtssicherheit durch die Datenverarbeiter selbst – im Sinne positiver Selbstregulierung – wurden mangels Einsicht in die Notwendigkeit bis heute nicht wahrgenommen. Und sogar bei so eindeutigen Fallgestaltungen wie dem Kreditscoring tut sich die Praxis schwer zu erkennen, dass das Verbot automatisierter Einzelentscheidungen nichts anderes ist als ein Instrument zur Wahrung der Rationalität automatisierter Verwaltungsabläufe.

Eine weitere Modernisierungschance wurde mit dem sog. Modernisierungsgutachten vertan, das vom Bundes-ministerium des Innern Ende der 90er Jahre in Auftrag gegeben und über das ein übergreifender gesellschaftlicher Diskurs zur Novellierung des Datenschutzrechtes losgetreten wurde. Im Rahmen dieses Diskurses entstand ein von Datenschutzfachleuten unter Moderation der DVD erarbeiteter Entwurf eines BDSG, der 1997 als Gesetzentwurf der Fraktion Bündnis 90/Die Grünen in den Bundestag eingebracht wurde.28 Obwohl mit einer rot-grünen Regierungskoalition die politischen Voraussetzungen für eine Modernisierung des Datenschutzrechtes besser als je zuvor waren, erwies sich das federführende Innenministerium unter Otto Schily als reformunwillig und reformunfähig. An dieser Situation hat sich leider bis heute – jetzt unter Wolfgang Schäuble – nichts geändert. Die Veröffentlichung des von Alexander Roßnagel, Andreas Pfitzmann und Jürgen Garstka verfassten Gutachtens[29] wurde immer wieder hinausgezögert bis nach dem 11.09.2001, also den terroristischen Anschlägen in den USA. Seitdem wurde das Thema einer umfassenden Datenschutzreform auf den Sankt-Nimmerleins-Tag verschoben.

Neue Aspekte des Datenschutzes eröffneten sich durch die technische Entwicklung. Diese ließ nicht nur neue Risiken und Gefahren entstehen, sondern eröffnete auch neue Chancen. Anstelle der großrechnerorientierten 10 goldenen Regeln der Datensicherheit des § 9 BDSG mit Anlage wurden übergreifende Ziele für technisch-organisatorische Maßnahmen formuliert: Sicherung von Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz. Diese fanden zwar bis heute keinen Eingang ins BDSG, wohl aber in moderne Landesdatenschutzgesetze, die sich anschickten, nicht nur die EU-DSRL umzusetzen, sondern auch den Anspruch technikadäquater Regulierung zu erfüllen.[30]

Angesichts der nationalen Begrenztheit des Datenschutzrechtes und der Globalität der Datenschutzrisiken insbesondere bei der Nutzung des Internet gewann der Selbstdatenschutz des Betroffenen eine steigende Bedeutung. Dieser Selbstschutz kann durch die Absicherung der Datenverarbeitung des Betroffenen (Virenschutz, Firewall, Anonymisierung, Verschlüsselung) erfolgen wie auch durch die (technisch geförderte) Wahrnehmung von Betroffenenrechte (z.B. Identitätsmanagement). Da hierfür zumeist technische Infrastrukturen nötig sind, besteht gegenüber staatlichen

23 Leitlinien für eine moderne Datenverkehrsordnung DANA 1/2 1991, 5.

24 EU-DSRL 95/46/EG v. 24.10.1995, AmtsBl. EG Nr. L 281/31; kritisch z.B. Lütkemeier DANA 3-1996, 4; Dippoldsmann KJ 1994, 369.

25 Dammann/Simitis, EG-Datenschutzrichtlinie, Kommentar, 1997.

26 Grundlegend dazu Weichert DANA 3/2006, 113.

27 Der Begriff des Systemdatenschutzes wurde von Podlech geprägt in Beiträge zum Sozialrecht, Festschrift H. Grüner, 1982, S. 451.

28 Entwurf eines Bundesdatenschutzgesetzes (BDSG) v. 14.11.1997, BT-Drs. 13/9082.

29 Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechts, 2001; diess. DuD 2001, 253.

30 Z.B. § 5 LDSG SH; am vorbildlichsten ist wohl § 10 Abs. 2 DSG NRW; Ernestus RDV 2000, 146.

Instanzen weiterhin ein Gewährleistungserwartung. Das Prinzip des Selbstschutzes wurde ausführlich zum ersten Mal von Alexander Roßnagel im Jahr 1997 in die Diskussion eingebracht.[31] Eingang in das BDSG hat es bis heute nicht gefunden.

Die oben dargestellten Tendenzen finden ihre Zusammenfassung in dem, was sich schon seit Anfang der 90er Jahre abzeichnete: die Entwicklung von datenschutzfördernden Technologien, bzw. der - gemäß dem von John Borking geprägten Begriff - Privacy Enhancing Technologies – PET.[32] Datenschutz muss nicht gegen die Technik durchgesetzt werden, sondern dieser kann mit deren Hilfe verwirklicht werden. Grundsätze der PET sind Datensparsamkeit, Systemdatenschutz, Selbstdatenschutz und Transparenz.

IV. Mäßige Enttäuschung: BDSG 2001

Angesichts der starken Modernisierungsbestrebungen in einzelnen Ländern, in der Wissenschaft, in der Wirtschaft, bei den Technikangeboten auf dem Markt, angesichts einer heranwachsenden Generation von jungen Menschen mit einer sehr funktionalen positiven Grundeinstellung gegenüber den Informationstechniken, angesichts der Reformbereitschaft bei den Regierungsfraktionen SPD und Bündnis 90/Die Grünen und einer damals – aus heutiger Sicht – relativ entspannten Situation im Bereich der inneren Sicherheit ist es überraschend wie auch enttäuschend, dass zu Beginn des 3. Jahrtausends keine umfassende Reform des Datenschutzrechtes möglich war.

Vielmehr setzte sich das Innen-ministerium damit durch, das Datenschutzrecht in zwei Stufen überarbeiten zu wollen. In einer ersten Stufe sollte eine Anpassung an die EU-DSRL erfolgen und nicht aufschiebbarer Regelungsbedarf befriedigt werden. In einer zweiten Stufe sollte dann die umfassende Runderneuerung stattfinden, mit der auch eine Verbesserung der Anwenderfreundlichkeit und Verständlichkeit des über viele Novellen unlesbar und unübersichtlich gewordenen Datenschutzrechtes verbunden sein sollte.

Tatsächlich trat dann die „erste Stufe“ am 23.05.2001 in Kraft.[33] Die Realisierung einer zweiten Stufe wurde – bis heute – nicht weiter verfolgt. Dessen ungeachtet fanden in der nun geltenden Fassung des BDSG Normen Eingang, die über den Anpassungsbedarf an die EU-DSRL hinaus positive Neuansätze enthalten. Hierzu gehören zunächst technologienahe Normen zur Videoüberwachung (§ 6b BDSG), zum Einsatz von mobilen Speichermedien, also insbesondere Chipkarten (§ 6c BDSG) sowie zum elektronischen Veröffentlichen von personenbezogenen Daten (§ 29 Abs. 3 BDSG). Deren Ziel ist es, den Betroffenen trotz der zunehmenden Unübersichtlichkeit der Verarbeitung Wahlmöglichkeiten und Transparenz zu sichern. Diese Ziele wurden teilweise befriedigend, so bei der Videoüberwachung[34], teilweise aber auch nur ungenügend, so bei elektronischen Verzeichnissen, verwirklicht.

Neu und zukunftsweisend war die gesetzliche Formulierung des strategischen bzw. systemgestaltenden Ziels der Datensparsamkeit bzw. der Datenvermeidung (§ 3a BDSG) und damit verbunden die begriffliche Aufnahme der pseudonymen Datenverarbeitung (§ 3 Abs. 6a BDSG). Zwar sind diese Ansätze dadurch unvollendet geblieben, dass mit beiden Regelungen keine direkten Rechtsfolgen verknüpft wurden. Insofern blieb das BDSG etwa gegenüber dem schleswig-holsteinischen Landesdatenschutzgesetz (LDSG SH) zurück, welches als Instrument für die Umsetzung der Datensparsamkeit die Vergabe von Gütesiegeln vorsieht (§ 4 Abs. 2 LDSG SH) und die pseudonyme Datenverarbeitung privilegiert (§ 11 Abs. 6 LDSG SH). Doch wurden die rechtlichen Begrifflichkeiten eingeführt, mit deren Hilfe unterhalb des Gesetzesrechtes die Modernisierung des Datenschutzes vorangetrieben werden konnte und kann.

Ähnliches gilt für die rein programmatische Regelung des § 9a BDSG zum Datenschutzaudit. Zwar kommt in ihr ausschließlich der gesetzgeberische Wille zum Ausdruck, Datenschutz-Gütesiegel und -Audits als Maßnahmen des präventiven Datenschutzes künftig zu verwirklichen. Er war und ist aber dennoch ein Signal, dass das schon zuvor vom Land Schleswig-Holstein eingeführte Verfahren zur Zertifizierung von Produkten und IT-Verfahren auf nationaler Ebene und darüber hinausgehend weiterverfolgt werden soll.

Letztendlich blieb das BDSG ´01 der zweiten Generation noch weitgehend verhaftet. Dass es auch anders möglich ist, machte insbesondere das Land Schleswig-Holstein vor, das, auf den sorgfältigen Vorbereitungen des damaligen Landesbeauftragten für den Datenschutz Helmut Bäumler[35] aufbauend, durch Schaffung eines Unabhängigen Landeszentrums für Datenschutz (ULD) und eines völlig überarbeiteten Landesdatenschutzgesetzes die organisatorischen wie die rechtlichen Voraussetzungen für den Sprung des Datenschutzes in das 21. Jahrhundert schuf.[36] Neben den oben genannten neuen Instrumenten spielen im ULD insbesondere auch die Technikentwicklung und -forschung, die Beratung und die Schulung wichtige Rollen.[37]

Mit der EU-DSRL und dem BDSG ´01 wurden insofern die Weichen für eine globale Informationsgesellschaft gestellt, als die Realität der weltweiten personenbezogenen Kommunikation anerkannt wurde und Instrumente beim grenzüberschreitenden Datenfluss ins Auge genommen wurden. Die gegenseitige Anerkennung der Datenschutzstandards innerhalb der EU und der EFTA-Staaten sowie von weiteren Ländern setzt auf mit der Schaffung eines hohen Datenschutzstandards

31 Roßnagel, Globale Datennetze: Ohnmacht des Staates Selbstschutz der Bürger, Thesen zur Änderung der Staatsaufgaben in einer „civil information society“, ZRP 1997, 26.

32 Hansen in Roßnagel (Fn. 2), S. 291.

33 BDSG v. 18.05.2001, BGBl. I S. 904.

34 Kritisch aber Weichert DANA 3/2001, 5, wegen einer fehlenden Meldepflicht.

35 Bizer/von Mutius/Petri/Weichert, Innovativer Datenschutz 1992-2004 – Wünsche, Wege, Wirklichkeit, für Helmut Bäumler, 2004.

36 LDSG SH v. 09.02.2000, GVOBl. SH 2000, 169.

37 Weichert, Regulierte Selbstregulierung - Plädoyer für eine etwas andere Datenschutzaufsicht, RDV 2005, 1.

verbundene wirtschaftliche Erleichterungen. Durch Standardvertragsklauseln sowie Binding Corporate Rules werden weitere Anreize zur freiwilligen Hebung des Datenschutzes geschaffen. Dies gilt auch für die Verabredung der Safe-Harbour-Prinzipien mit den USA. Das große Manko der freiwilligen ökonomischen Anreize besteht aber darin, dass diese nicht die staatliche Datenverarbeitung mit erfassen. Dies kann dazu führen, dass trotz formal korrekter Beachtung der Regeln sämtliche Grundgedanken des Datenschutzes über Bord gehen, wie dies der Umgang mit den Fluggastdaten (Passenger Name Records - PNR)[38] sowie das Abgreifen der internationalen Banktransaktionsdaten durch US-amerikanische Geheimdienste von einem ausgelagerten Rechner der belgischen Firma SWIFT zeigen.[39]

Die Globalisierung der Datenverarbeitung und insbesondere die Existenz des Internet, v.a. des World Wide Web, wurden weder von deutschen noch von anderen nationalen Datenschutzgesetze bisher rezipiert, obwohl seit mindestens 10 Jahren die weitere Entwicklung absehbar war und weiterhin ist: Die Verschmelzung der Netze, die Einkehr des Ubiquitous Computing in den Lebensalltag,[40] das Aufkommen von Mobilem Internet, Semantischem Netz und den Anwendungen, die mit dem Begriff Web 2.0 gekennzeichnet sind, stellen uns vor neue soziale und technische Gegebenheiten und Herausforderungen.

V. Merkmale eines marktgängigen zivilisierten Datenschutzes

Zentraler Ansatz des Datenschutzes der dritten Generation ist es, ergänzend zum staatlichen Datenschutz-Ordnungsrecht mit Kontrollen und Sanktionen den Datenschutz als Wettbewerbsfaktor zu etablieren. Angesichts der Komplexität und der Globalität der Datenverarbeitung ist es nicht mehr möglich, ausschließlich mit einem hoheitlichen Regelungsansatz hinreichenden informationellen Grundrechtsschutz zu gewährleisten. Dies ist auch nicht nötig, soweit die Datenverarbeitung einen direkten Betroffenenbezug dadurch hat, dass der Betroffene in spezifische Work-Flows einbezogen ist und hierüber für die Betroffenen Transparenz und Wahlmöglichkeiten geschaffen werden können.

Der Wettbewerbsansatz kommt derzeit z.B. positiv im Verhältnis USA-Europa zum Tragen. Das Erfordernis eines angemessenen Datenschutzstandards durch die EU-DSRL hat in vielen Drittstaaten zur Schaffung mehr oder weniger funktionsfähiger Datenschutzregelungen geführt. Dem gegenüber erlitten die USA, die sich bis heute standhaft gegen eine Anpassung zur Wehr setzen, zunehmend Wettbewerbsnachteile, wie sich erst jüngst in der Ankündigung von SWIFT erwies, die bisherige Datenverarbeitung in den USA – zumindest weitgehend – nach Europa zu verlegen.[41]

Auch im nationalen Rechtsrahmen ist der Datenschutz gerade erst an Anfang eines Durchbruchs ins Zivilrecht. Dies gilt insbesondere für die Anerkennung des Datenschutzrechtes als besondere Form des Verbraucherschutzrechts.[42] Die Verarbeitung von Kundendaten erfolgt weitgehend über Regelungen in Allgemeinen Geschäftsbedingungen (AGB), die der verbraucherrechtlichen Kontrolle unterworfen werden können.[43] Bisher haben sich Datenschützerinnen und Datenschützer noch nicht genügend mit den Möglichkeiten auseinandergesetzt, die Wettbewerbsregelungen wie das Gesetz zur Bekämpfung unlauteren Wettbewerbs oder das Unterlassungsklagegesetz eröffnen. Schon anlässlich der Bundestagswahl 1998 wurde von der DVD die Einbeziehung von Datenschutzverbänden nach dem Vorbild des Umwelt- und des Verbraucherschutzrechtes gefordert.[44] Insofern lassen sich zwar noch wenige Fortschritte bei den Datenschutzorganisationen selbst erkennen.[45] Wohl aber nutzen inzwischen Verbraucherverbände wie der vzbv die Verbraucherklage regelmäßig für Ziele des Datenschutzes. Selbst in kartellrechtlichen Verfahren können sich aus der Verschmelzung von Unternehmen ergebenden Datenschutzverstößen konkrete wettbewerbsrechtliche Konsequenzen ergeben.[46]

Auf die Potenziale von Datenschutz-Gütesiegel und -Audit wurde schon hingewiesen. Diese freiwilligen Angebote, die eine Win-Win-Situation für alle Beteiligten zum Ziel haben, erweisen sich in Schleswig-Holstein als ein auf nationaler wie europäischer Ebene umsetzbares Modell.[47] Selbst ein großer Konzern wie Microsoft nimmt die Zertifizierung in Anspruch, um auf dem Markt eine Erhöhung des Kundenvertrauens und damit einen Marktvorteil zu erzielen.[48] Inzwischen hat offensichtlich auch das Bundesministerium des Innern erkannt, dass mit der Zeritifizierung von Verfahren und Produkten positive Effekte erzielt werden können. Es hat einen - noch verbesserungsfähigen - Entwurf eines Auditgesetzes vorgelegt.[49]

Datenschutz lässt sich schon lange nicht mehr auf Grundrechtsschutz reduzieren. Die Bezüge zum Schutz von Betriebs- und Geschäftsgeheimnissen liegen bei der Wahrung der Vertraulichkeit der Daten auf der Hand. Aber nicht nur das. Datensicherheit im weiteren Sinn ist ein zentraler Bestandteil jedes IT-Managements. Es ist daher nahe liegend, bei der Etablierung neuer IT-Verfahren integrierte Datenschutz- und Datensicherheitskonzepte zu erstellen und zu verwirklichen. Datenschutzkonformität setzt gut

38 DANA 1/2007, 21.

39 Weichert in Müller-Heidelberg/Finckh/Steven/Assall/Micksch/Kaleck/Kutscha/Gössner/Engelfried, Grundrechte-Report 2007, S. 46.

40 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), https://www.datenschutzzentrum.de/taucis/index.htm.

41 Krempl, Swift entzieht EU-Daten dem einfachen Zugriff durch die USA, www.heise.de 04.10.2007.

42 Weichert VuR 2006, 377.

43 Heidemann-Peuser DuD 2002, 389.

44 DANA 4/1998, 36.

45 Weichert DANA 2/20002, 5.

46 Z.B. in Bezug auf den Aufkauf von DoubleClick durch Google Weichert DuD 2007, 724.

47 ULD, https://www.datenschutzzentrum.de/guetesiegel.

48 ULD PE v. 03.09.2007.

49 Krempl, Schäuble will Datenschutz als Wettbewerbsfaktor fassen, www.heise.de 28.09.2007.

organisierte Datenverarbeitung voraus. Diese bedingt eine gute Dokumentation, eine stringente Planung, Entwicklung, Testung und Freigabe bis hin zu einer laufenden Kontrolle. Weitsichtige Betriebe integrieren in ihr IT-Management Komponenten der Datensicherheit und des Datenschutzes. Diese Erkenntnis macht vor der öffentlichen Verwaltung nicht halt. Behörden in Schleswig-Holstein haben im Interesse der Effizienzerhöhung wie auch der Bürgerakzeptanz schon eine Vielzahl von Auditierungen ihrer Verarbeitungsabläufe vornehmen lassen, so etwa das für die Landes-IT zentral federführende Finanzministerium für das Landesnetz, das Umwelt-ministerium für die Abwicklung von EU-Subventionsverfahren oder der Landtag bei so unterschiedlichen Verarbeitungsprozessen wie dem Internetauftritt, der Durchführung von Petitionsverfahren oder seinem Zutrittberechtigungssystem.[50]

Zweifellos wird der Datenschutz auch künftig immer auf eine funktionstüchtige verwaltungsrechtliche Umsetzung angewiesen sein. Dessen ungeachtet müsste er aber in der zivilrechtlichen Praxis heute schon eine erheblich größere Rolle spielen, als dies bisher akzeptiert wird. Ein Beispiel hierfür ist der jüngste Verkauf von Darlehensforderungen ins datenschutzfreie Ausland. Zwar hat der Bundesgerichtshof bisher nicht anerkannt, dass mit einem Datenschutzverstoß vertragliche Konsequenzen bzgl. des Kerngeschäftes verbunden sein können.[51] Dabei wurde aber von ihm ignoriert, dass Verstöße gegen den Datenschutz durch Vertragspartner zivilrechtlich zu sanktionierende Vertragsverletzungen sind, die bis zur Nichtigkeit des Grundgeschäfts führen können.[52]

Als abschließendes Beispiel für die Möglichkeiten des Privatrechts zur Sicherung des Datenschutzes sei auf den Arbeitnehmerdatenschutz verwiesen, der schon seit Jahren von den Arbeitsgerichten als ein integraler Bestandteil des Arbeitsrechtes anerkannt ist. Dies erfolgte trotz des seit über 20 Jahren währenden Widerstandes der Arbeitgeberseite gegen ein spezifisches Arbeitsnehmerdatenschut zgesetz.[53] Das Arbeitsrecht setzt individualrechtlich der Befragung von Bewerbenden im Auswahlverfahren klare Grenzen und verbietet systematische elektronische Verhaltens- und Leistungskontrollen. Kollektivrechtlich sind die Arbeitnehmervertretungen im Interesse des Arbeitnehmerdatenschutzes in die Einrichtung neuer IT-Verfahren einbezogen und können über die Inanspruchnahme ihrer Mitbestimmungsrechte diese mit gestalten. Das bisher weitgehend richterrechtlich entwickelte Recht wird im Hinblick auf den absehbaren Einsatz neuer biotechnischer Methoden am Arbeitsplatz, im Hinblick auf die Allgegenwärtigkeit der Informationstechnik im Arbeitsleben und der unübersichtlich gewordenen Gesundheitsdatenverarbeitung von Beschäftigten sowie deren eingeschränkter Willensfreiheit komplexer und verlangt nach normativen Präzisierungen. Diese Erkenntnis hat sich inzwischen auch in der Europäischen Kommission festgesetzt, die im Jahr 2002 eine 2. Konsultationsrunde zur Schaffung einer Richtlinie für den Arbeitnehmerdatenschutz durchgeführt hat.[54] Arbeitsrecht ist nichts anderes als spezielles Zivilrecht.

Nicht nur hier, sondern auch in anderen Lebensbereichen bietet es sich an, spezifische Regelungen für die Datenverarbeitung durch private Stellen zu erlassen. Diese sollten nicht das ohnehin schon bestehende Regelungswirrwarr im dritten Abschnitt des BDSG erhöhen, so wie es mit den jüngsten Vorschlägen für eine BDSG-Novellierung zum Thema Scoring und Auskunfteien der Fall wäre.[55] Wohl aber macht es Sinn, für spezifische Datenschutzprobleme gerade im privaten Bereich auch gesetzlich spezifische Lösungen zu suchen, sollten sich andere Regulierungsversuche, z.B. über Verhaltensregeln nach § 38a BDSG, als unwirksam erweisen. Ziel muss es hierbei in jedem Fall sein, die wirtschaftlich schwächere Seite zu stärken, also z.B. den Arbeitnehmer, den Mieter oder den Verbraucher. Diese Stärkung kann in der Erhöhung der Transparenz der Datenverarbeitung liegen sowie in der Verbesserung der individuellen oder auch kollektiven Rechte – in materieller wie in prozeduraler Hinsicht.

Deutschland ist nun schon seit über 30 Jahren international Vorreiter im Datenschutz. Hierbei hatte das BDSG zunächst eine wegweisende Bedeutung. Dieser Glanz hat in jüngster Zeit an Strahlkraft verloren. Die deutsche Datenschutzkultur hat aber das Potenzial und die Qualität, neuen Glanz zu verbreiten. Dies setzt voraus, dass die Politik diese Chance erkennt und sich im internationalen Diskurs nutzbar macht.

50 ULD, https://www.datenschutzzentrum.de/audit/.

51 BGH BB 2007, 793.

52 Weichert VuR 2007, 373.

53 Däubler RDV 1999, 243.

54 EU-Kommission, Second stage consultation of social partners on the protection of workers´ personal data, 2002.

55 Referentenentwurf des BMI v. 08.08.2007; dazu z.B. GDD-Stellungnahme, GDD-Mitteilungen 5/2007, 2.

Dr. Johann Bizer

30 Jahre DVD - Neuere Entwicklungen -

30 Jahre sollen ja so etwas wie eine magische Grenze sein. Da die meisten der hier Anwesenden diese Altergrenze überschritten haben dürften, verrate ich wohl kein Geheimnis, dass das Leben auch ab 30 keineswegs eintönig und langweilig ist. Man muss selbst mit 75 Jahren nicht zum alten Eisen gehören, jedenfalls solange man im Kopf noch jung ist. Umgekehrt soll es auch Menschen geben, die trotz unter 30 sich wie Frühvergreiste verhalten. Entscheidend ist mit anderen Worten die jugendliche Frische im Kopf, kurz die Neugierde auf das Neue. **Kurz und gut: Die Zahl an Jahren ist kein aussagekräftiges Barometer für Alter.**

1. Mit drei Mythen aufräumen

30 Jahre DVD sind ein guter Anlass, auf der Grundlage einer Bestandsaufnahme der datenschutzpolitischen Situation nach vorne zu blicken und die maßgeblichen Eckpunkte einer zukünftigen Datenschutzpolitik zu fixieren. Dabei gilt es zunächst mit ein paar Mythen aufzuräumen:

- Datenschutz als politische Massenbewegung.
- Datenschutz ist technikfeindlich.
- Datenschutz ist wirtschaftsfeindlich.

Das Gegenteil ist der Fall:

1.1 Datenschutz als politische Massenbewegung

Die These, der **Datenschutz als politische Massenbewegung**, ist eine unreflektierte altlinke Fixierung auf die eigene politische Sozialisation. Das Kribbeln im Bauch, gemeinsam mit anderen Menschen einer Meinung zu sein, indem man sich die Socken durch leere Straßen qualmend läuft, mag eine nette Erfahrung sein, aber sie ist keine conditio sine qua non für eine erfolgreiche Grundrechtspolitik.

Um keine Missverständnisse aufkommen zu lassen: Das Demonstrationsrecht ist ein Grundrecht. Und nichts spricht dagegen, für einen besseren Datenschutz auf die Straße zu gehen. Das gefährliche an dieser These ist aber, dass der Erfolg der politischen Intention gemessen wird an einer spezifischen politischen Sozialisationserfahrung. Pointiert gefragt: Ist die Datenschutzpolitik gescheitert, wenn die Menschen nicht massenhaft auf die Straße gehen? Natürlich nicht.

Erfolgreiche Datenschutzpolitik ist die Wahrnehmung von Grundrechtsfreiheit vor allem „in kleiner Münze". Die These stützt sich auf die tagtägliche Sichtung der Eingaben der Bürgerinnen und Bürger in einer Einrichtung wie dem Landesbeauftragten für den Datenschutz Schleswig-Holstein: Sie betreffen den Datenschutz von Arbeitslosen, Soziahilfeempfängern oder Patienten. Sie betreffen besorgte Bürgerinnen und Bürger, deren Daten von der Polizei erhoben worden sind. Die Erhebung von Rundfunkgebühren, die heimliche Datenerfassung im Internet sowie der gesamte und riesige Bereich des Verbraucherdatenschutzes – also überall dort, wo personenbezogene Daten der Verbraucherinnen und Verbraucher erhoben und verarbeitet werden.

Die Fälle sind gekennzeichnet durch eine individuelle Betroffenheit von Menschen, deren Daten in bestimmten sozialen Situationen für sie nicht nachvollziehbar erhoben und verarbeitet werden. Der Datenschutzbeauftragte ist mit seinen Möglichkeiten in dieser Situation eine Art „Bürgeranwalt", der versucht Sachverhalte aufzuklären und die datenschutzrechtliche Rechtsposition der Betroffenen zu stützen.

Die **individuelle Betroffenheit der Menschen ist die Basis des Datenschutzes:** Sie reicht vom ALG II-Empfänger über den Steuerzahler, den Internetnutzer bis hin zu den Landfrauen in Schleswig-Holstein. Das ist Datenschutz **mit kleiner Münze**. Hier spielt die Musik der Grundrechtsverwirklichung.

1.2 Datenschutz ist technikfeindlich.

Die Wurzel für diese These liegt in den 70er / 80er Jahren. Komplementär zum Verhältnis von „Atomkraft versus Solarstrom" bzw. zentrale Großtechnik versus dezentraler Kleintechnik steht auch die Kritik an einer zentralen automatisierten Datenverarbeitung, die die betroffenen Grundrechtssubjekte mit ihren gleichförmigen Rechenoperationen gleichsam vermachtet.

Die Gegenüberstellung von Rechentechnik versus Grundrechtsfreiheit hat unglaublich viel Schaden angerichtet: Hierzu zähle ich die starke Juridifizierung des Datenschutzes, die die Technik zum technisch-organisatorischen Erfüllungsgehilfen degradiert hat. Die Idiotie dieser Sichtweise findet sich in der Form der Anlage zu § 9 BDSG wieder: Technischer Datenschutz als Anlage zum rechtlichen Datenschutz.

Eine weitere Folge ist die Beherrschung der Datenschutzbeauftragten des Bundes und der Länder durch Juristen. Datenschutz wurde und wird seit Jahrzehnten vorrangig über Gesetze betrieben. Erst § 3a BDSG – technische Gestaltung für Datensparsamkeit und Datenvermeidung – hat zumindest eine symbolische Wende eingeleitet. Immerhin stützt diese Norm die konzeptionelle Entwicklung von PET – Privacy Enhanced Technologies – allerdings fehlt es noch immer an einer systematischen Entwicklung derartiger Technologien.

Datenschutz darf nicht technikfeindlich sein, er muss vielmehr technikkritisch und technikkonstruktiv sein. Datenschutz ist eine **Aufgabe der technischen Gestaltung**. Mit dieser Sichtweise ist die Wende zu einer prä-

ventiven Datenschutzkonzeption eingeleitet. Vermeidung des Personenbezuges an der technischen Quelle der Entstehung ihrer Daten durch Gestaltung der technischen Systeme. Wer sich dieser Herausforderung stellen will, muss anders ticken als nur kritisch-destruktiv. Er muss sich verabschieden von der bequemen Denkweisen, hinter jeder technischen Anwendung stünde der Teufel.

Gefordert ist eine fundierte Analyse des technischen Systems, aber eben auch Kompetenz und Mut, ein technisches System so zu gestalten, damit es zum Schutz der informationellen Selbstbestimmung der Betroffenen datenschutzkonform eingesetzt werden kann. Datenschutzkonforme Gestaltung technischer Informationssysteme ist aus dieser Sicht vor allem auch eine konzeptionelle Herausforderung.

1.3 Datenschutz ist wirtschaftsfeindlich.

Wer informationstechnische Systeme betreibt, mit deren Hilfe personenbezogene Daten der Verbraucherinnen und Verbraucher erhoben und verarbeitet werden, ist nicht nur im Sinne des Datenschutzrechts verantwortlich für Datenschutzkonformität dieser Prozesse. Die wirtschaftlichen Verwertungsinteressen einer solchen Datenverarbeitung sind evident. Wir alle wissen, dass der Einsatz der Informationstechnik in der Regel zu einer Unterstützung von Prozessen erfolgt, bei denen nicht selten auch Lohnkosten und damit Arbeitsplätze eingespart werden und werden sollen.

Ist der Datenschutz – insbesondere in seinen Ausprägungen des Verbraucher- oder des Arbeitsnehmerdatenschutzes deswegen wirtschaftsfeindlich?

Wenn man die eben beschriebene Gestaltungsaufgabe ernst nimmt, dann ist dies nicht der Fall: Datenschutz ist unter dieser Voraussetzung allenfalls kritisch gegenüber bestimmten wirtschaftlichen Prozessen und Mechanismen, die durch Informationstechnik unterstützt werden, bspw. der heimlichen Überwachung und der Verhaltenssteuerung der Betroffenen.

Datenschutz ist aber nicht wirtschaftsfeindlich. Tatsächlich gibt es sogar eine ganze Reihe von parallelen Interessenslagen zwischen dem Interesse des Betroffenen auf Wahrung seiner informationellen Selbstbestimmung und dem Interesse eines Wirtschaftsunternehmens, das personenbezogene Daten erhebt und verarbeitet:

- Unternehmen mit Endkundengeschäft haben in der Regel ein Interesse, dass ihre Kundendaten vertraulich und sicher verarbeitet werden. Kundendaten sind Kapital, das man nicht mit anderen Unternehmen teilt.

- Unternehmen mit Endkundengeschäft haben in der Regel ein Interesse an der Wahrung der Datenschutzinteressen ihrer Kunden, weil sie im eigenen wohlverstandenen Interesse nicht wollen, dass sie sich unzufrieden von dem Unternehmen abwenden.

- Unternehmen haben ein wirt schaftliches Interesse, nicht durch Datenschutzskandale einen Imageschaden zu erleiden.

Ein Unternehmen, das im eignen Interesse einen systematischen Informationsschutz leistet, leistet damit auch einen Beitrag für den Datenschutz. Allerdings nur „einen“ Beitrag und dieser ist häufig auch nicht ausreichend.

Allzu oft haben wir es mit Unternehmen zu tun,

- die ihre Beschäftigten exzessiv bspw. mit Videokameras am Arbeitsplatz überwachen,

- die Kunden- oder Beschäftigtendaten durch Dienstleister außerhalb der vorgeschriebenen Regularien verarbeiten lassen,

- Kundendaten durch automatisierte Verfahren mit Daten aus anderen Quellen zusammenspielen oder automatisiert bewerten (Scoring),

- Kundendaten ohne Zustimmung der Betroffenen zu Werbezwecken verwenden oder

- Daten aus unterschiedlichen Quellen sammeln und wirtschaftlich verwerten (Adresshandel).

Der Umstand, dass sich Unternehmen nicht an die datenschutzrechtlichen Vorgaben halten oder halten wollen, bedeutet aber nicht, dass der Datenschutz wirtschaftsfeindlich ist. Er bedeutet nur, dass es Unternehmen gibt, die sich nicht an die einschlägigen Rechtsvorschriften halten oder im Managementdeutsch formuliert nicht „compliance“ sind.

Eine moderne Datenschutzpolitik unterstützt und belohnt Unternehmen, wenn sie sich in Übereinstimmung mit den Datenschutzanforderungen verhalten.

Das Datenschutz-Gütesiegel aus Schleswig-Holstein ist ein herausragender Beleg, dass der Datenschutz auch **positive Anreize** setzen kann, die gesetzlichen Anforderungen einzuhalten:

- Das ULD konnte seit 2003 über 40 Gütesiegelverfahren mit der Verleihung eines Zertifikates abschließen. Die Nachfrager kommen aus allen Gebieten der

Bundesrepublik, obwohl das Gütesiegel aus Rechtsgründen nur für Produkte verliehen werden kann, die in der Schleswig-Holsteinischen Landesverwaltung eingesetzt wer den können.

- Das Gütesiegel Schleswig-Holstein ist mittlerweile international aner kannt: Belege sind,
  - ein Innovationspreis der Europäischen Kommission für dieses Konzept im Jahr 2004,
  - zwei Zertifizierungsverfahren eines großen Softwareherstellers aus den USA (Microsoft) 2007
  - der Auftrag der Europäischen Kommission vom Juni 2007 an ein internationales europäisches Konsortium unter Führung des ULD, das Konzept des Gütesiegels aus Schleswig-Holstein europaweit auszurollen (EuroPriSe).

- Die Tatsache der Initiative der Großen Koalition für ein Bundesauditgesetz nach § 9a BDSG (selbst wenn der Referentenentwurf des BMI in der vorliegenden Fassung konzeptionell mehr Fragen als Antworten bietet, so ist allein die Tatsache dieser Initiative eine Anerkennung dieser Datenschutzpolitik).

2. Entwicklungen

Ich bin nun gebeten worden, zu neueren Entwicklungen in der Datenschutzpolitik zu sprechen.

Da die Bedrohung der informationellen Selbstbestimmung durch staatliche Überwachung bereits im Mittelpunkt anderer Beiträgen stand, greife ich nur einen Aspekt heraus und setze ansonsten meinen Schwerpunkt auf die Bedeutung einer präventiven Datenschutzpolitik als Reaktion auf die Herausforderungen einer exzessiven Datenverarbeitung.

2.1 Indienstnahme Privater

Das bisherige Bedrohungsszenario der informationellen Selbstbestimmung, dass die Sicherheitsbehörden selbst personenbezogene Daten erheben und verarbeiten, wird überlagert – nicht aber abgelöst – durch die zunehmende Indienstnahme privater Dienstanbieter für Zwecke der Inneren Sicherheit.

Vielleicht wäre dies allein noch nicht dramatisch, wenn sich die rechtsstaatlichen Grenzen einer zielgerichteten Fahndung nach Straftätern (Strafprozessrecht) oder Störern (Polizeirecht) nicht seit Jahren zu präventiven Vorfeldstrategien auflösen würden:

Die moderne Sicherheitspolitik will präventiv tätig sein, indem sie Netzwerke möglicher Täter oder Störer identifiziert und aufklärt.

Die moderne Sicherheitspolitik will präventiv tätig sein, weil sie das kriminelle Potenzial eines Menschen am liebsten in einem Stadium erkennen will, in dem er selbst noch nicht einmal an die Planung gedacht hat.

Das Kennzeichen diser Sicherheitspolitik ist Verdachtsgewinnung und Vorfelderfassung.

Wer so denkt und ausgerichtet ist, muss „seine Netze“ zwangsläufig weit auswerfen. Gleichzeitig werden damit eine Vielzahl an Personen aus dem Umfeld von möglichen Tätern oder Störern erfasst, die noch nicht einmal als Kontakt- und Begleitpersonen in Frage kommen. Wer kommunikative Netzwerke aufklären will, kennt keine Grenzen.

Vor dem Hintergrund einer solchen der Sicherheitspolitik ist der zunehmende und exzessive Zugriff auf die Kundendaten privater Dienstleistungen zu sehen und zu würdigen. Unabhängig von der Frage, ob diese Zugriffe verfassungsmäßig sind oder nicht: Im Fokus der Sicherheitsbehörden sind die Datenbestände der privaten Dienstanbieter wie Telekommuni-kationsunternehmen, Postdienstleister. Reisedienstleister oder Finanzdienstleister.

Dies bedeutet im Umkehrschluss, dass die privaten Dienstanbieter zum Büttel (Erfüllungsgehilfen) der staatlichen Sicherheitsbehörden geworden sind. Die Vertraulichkeit der Kundenbeziehung wird durch den Staat zunehmend entwertet. Die Situation ist dramatisch, weil die Zugriffe auf einzelne Datenbestände nicht zielgerichtet erfolgen, sondern Kennzeichen einer Schleppnetzfahndung tragen.

Die Dienstanbieter könnten ihre Kundenbeziehungen schützen, wenn sie sich datenvermeidend und datensparsam verhalten würden. Das Interesse des Betroffenen auf Wahrung einer auf das erforderliche Maß beschränkten Verarbeitung seiner Daten ist konvergent mit dem Interesse der Unternehmen, seine Kundenbeziehung zu schützen.

Sie wäre konvergent, wenn sich die Unternehmen datenschutzkonform verhalten: In einzelnen Fällen ist dies durchaus der Fall. Es ist immerhin im Bereich der Telekommunikation insoweit der Fall, dass der Staat durch die Verpflichtung zur Vorratsdatenspeicherung eine datensparsame Datenverarbeitung für einen definierten Zeithorizont verbietet.

Die Indienstnahme Privater hat noch einen weiteren Aspekt: Die Verpflichtung der Dienstanbieter zur Vorratsspeicherung weckt Begehrlichkeiten Dritter: Das beste Beispiel sind die urheberrechtlichen Auskunftsansprüche nach § 101a Urhebergesetz. Die Gewinner der Vorratsdatenspeicherung werden vor allem die Plattenfirmen, die Labels sein, also eine in der Internetwirtschaft sterbende Industrie die ihre Interessen nun noch großzügiger durchsetzen kann, weil sie nicht willens ist, die Nutzung virtueller Güter datenschutzkonform zu gestalten.

Dies ist ein völlig absurdes Ergebnis: **Verfassungsschutz und Musikindustrie** werden in einem Atemzug berechtigt, exklusiven Zugriff auf Verkehrsdaten der Nutzer zu bekommen. Dieser Regelungsvorschlag ist erstens dreist und trägt zweitens das Kainsmal der Verfassungswidrigkeit.

2.2 Präventiver Datenschutz

Im Folgenden möchte ich den Blick von der staatlichen repressiven Datenschutzpolitik auf die Herausforderungen einer präventiven

Datenschutzpolitik wenden: Ich setze den Schwerpunkt hier vor der DVD nicht grundlos, sondern mit Bedacht. Wir haben fast 30 Jahre Datenschutzpolitik als Rechtspolitik begriffen und damit reaktiv betrieben: Neue technische Phänomene wurden mit dem Ruf nach dem Gesetzgeber beantwortet.

Das Ergebnis ist eine Flut an bereichsspezifischen Datenschutzregelungen und - gemessen an diesem Maßstab der Durchregulierung - viele Regelungslücken.

Die Juridifizierung des Datenschutzes hat uns Datenschutz-Kontrollstellen beschert, in denen vorwiegend Juristen reaktiv im Sinne einer Ordnungsbehörde handeln. Technische Kompetenz im institutionellen Datenschutz ist selten.

Die Juridifizierung des Datenschutzes hat das Thema in den Parlamenten bei den Innen- und Rechtspolitikern verortet, aber nicht bei den Wirtschafts- und Verbraucherpolitikern.

Die Schlussfolgerung lautet: Wer den Datenschutz voran bringen will, muss eine **präventive Datenschutzpolitik** betreiben:

Präventive Datenschutzpolitik bedeutet eine technisch-organisatorische und rechtliche **Gestaltungskompetenz**.

Präventive Datenschutzpolitik setzt auf **Beratung**: Wer aber beraten will, muss über die entsprechende fachlichen Kompetenzen verfügen, auch helfen zu können.

Und schließlich: Die Investition in den Datenschutz muss sich für den Nachfrager auch lohnen, d.h. ihm muss ein Anreiz geboten werden, mit seiner Leistung gegenüber seinen Kunden in Abgrenzung zu Dritten auch werben zu können. Datenschutzinvestitionen müssen sich als **Wettbewerbsvorteil** auszahlen. Vor diesem Hintergrund sind das Datenschutzaudit für Produkte sowie das Datenschutzaudit für Verfahren zentrale Elemente einer präventiven Datenschutzstrategie.

Wir im ULD haben uns diesen Herausforderungen gestellt und dabei eine Reihe von wichtigen Erfahrungen gemacht, über die ich im Folgenden berichten will.

2.3 Gestaltungs - kompetenz

Gestaltungskompetenz müssen wir bei der Durchführung von unseren Drittmittelprojekten beweisen, um von Partnern aus Wirtschaft und Wissenschaft akzeptiert zu werden. Wir verknüpfen unser technisches und datenschutzrechtliches Know how, um die datenschutzfreundliche Gestaltung von Technologien voranzutreiben: Ein zentraler Schwerpunkt ist dabei die datenschutzfreundliche Gestaltung des **Identitäts-Managements**. ID-Managenent nicht fremdgesteuert, sondern User-Controlled. Unsere konzeptionellen Überlegungen über eine hard- und softwargestützte Unterstützung des ID-Managements zusammen mit Partnern aus Wirtschaft und Wissenschaft in Europa sind immerhin so erfolgversprechend, dass das EU-Projekt Prime ab März 2008 verlängert wird.

Gestaltungskompetenz ist aber auch bei der **Entwicklung des E-Government** gefragt: Elektronische Anwendungen müssen und sollen gestaltet werden: Dies reicht von der Gestaltung von Anwendungen, Authentifizierungsverfahren von Behörden und Bürgern, der Umsetzung der Anforderung an die Mandantenfähigkeit bis hin zur revisionsicheren Administration der entsprechenden Verfahren.

In Schleswig-Holstein sind wir vom ULD deswegen gefragte Gesprächspartner, weil wir mit den konzeptionellen Anforderungen des Datenschutzes in Form eines IT-Konzeptes und eines Sicher-heitskonzeptes nicht nur konzeptionelle Defizite aufdecken, sondern sie durch die unsere Anregungen, Hinweise, Zuarbeiten zu Sicherheitsfragen und schließlich auch den Entwurf entsprechender Templates auch schließen können.

2.4 Konzeptionierung

Die Grunderfahrung ist, dass mit der Komplexität der Verfahren die Bedeutung einer stringenten **Konzeptionierung der Verfahren** wächst.

Konzeptionierung ist das Gegenteil, von „einfach mal anfangen“. Es setzt voraus, dass das Verfahren geplant wird, bevor es gebaut und implementiert wird. Insbesondere die Phase der Planung setzt voraus, dass die Bedürfnisse an das Verfahren unter funktionalen Gesichtspunkten ebenso wie die Anforderungen aus Datenschutz und Datensicherheit analysiert und präzisiert werden. Die gegebenenfalls bestehenden Zielkonflikte sind in der Planungsphase zu lösen, aber nicht erst im Produktivbetrieb.

In der Praxis zeigt sich, dass zahlreiche automatisierte Verfahren bereits in dieser Phase der Konzeptionierung erhebliche Mängel aufweisen, die sich dann später im produktiven Betrieb negativ auswirken: Anforderungen sind nicht definiert, Sicherheitsmaßnahmen sind unzureichend und Abläufe sind nicht definiert. Häufig zeigt sich auch, dass Verfahren in Hinblick auf die genutzten personenbezogenen Daten überdimensioniert sind, d.h. die beabsichtigte Unterstützung der Aufgabe hätte auch mit einem geringeren Aufwand an Informationen und Daten erledigt werden können. Mängel aus der Phase der Konzeptionierung erzeugen zudem in aller Regel einen erheblichen Aufwand, weil die erforderlichen Maßnahmen nun im laufenden Betrieb zu erheblich höheren Kosten mühsam nachgezogen, d.h. nachgebessert werden müssen. Kurz zusammengefasst: Ein im Sinne des Datenschutzes gut konzeptioniertes System spart Kosten. Weil wir in diese Richtung beraten, werden wir auch um unseren Rat gefragt.

Konzeption bedeutet Denkarbeit – sie mündet aber auch in **Dokumentationsarbeit**, damit Vertreter und Nachfolger die Arbeit an den Systemen übernehmen oder fortsetzen können, sowie die erforderlichen Revisionsarbeiten übernommen werden können. Wir haben gelernt, dass unsere Partner in Wirtschaft und Verwaltungen häufiger denken als schreiben können: Die Konsequenz ist ein für Zwecke der öffentlichen Verwaltung entwickeltes Architekturschema zur Dokumentation von Verfahren mit entsprechenden Templates. Das Konzept lässt sich auf Wirtschaftsunternehmen übertragen. Gleichzeitig bieten wir über

unsere Datenschutzakademie Kurse an, um das Erstellen einer schlanken, aber aussagekräftigen Dokumentation zu unterstützen. Auch dies ist ein Baustein des präventiven Datenschutzes.

Von nicht geringerer Bedeutung ist die Vorgabe, **Verfahren zu testen** und vor einem produktiven Betrieb in einem förmlichen Verfahren durch die verantwortlichen Personen der Organisation **freigeben** zu lassen. Es ist evident, dass nicht ausreichend getestete Verfahren einen höheren Korrekturaufwand produzieren als getestete. Hierfür müssen aber auch die entsprechenden Ressourcen bereitgestellt werden. Bei Standardprodukten lassen sich Test- und Freigabeverfahren zentralisieren. Bei neuen Verfahren bedarf es entsprechender Testumgebungen sowie Testdaten. In der öffentlichen Verwaltung haben wir durch gezielte Inspektionen erstens Mängel aufdecken können und zweitens – viel wichtiger – zeigen können, dass sich durch eine Umorganisation im Patchmanagement erheblicher Aufwand reduzieren lässt.

Ich will Sie nicht mit Details langweilen, sondern will mit diesen Beispielen eindringlich illustrieren, dass die Einstellung der Datenschützer in Richtung Konstruktion gehen muss. Diese Konstruktion setzt voraus, dass man eine Situation antizipiert und einen entsprechenden technisch-organisatorischen Gestaltungsvorschlag entwickelt.

Der Datenschutzbeauftragte darf nicht „Moserkopp“ sein, sondern er muss sich als „Konstrukteur“ verstehen. Umso schneller wird es uns gelingen, technische Systeme datenschutzkonform zu gestalten.

2.5 Prozessmanagement: Rollen und Aufgaben

Was bedeutet dies für die betriebliche Praxis: Natürlich weiß auch ich, dass betriebliche Datenschutzbeauftragte häufig einen schweren Stand haben, natürlich weiß auch ich, dass betriebliche Datenschutzbeauftragte häufig auch als ein Hindernis im Unternehmen gesehen werden. Aber gerade deswegen sind selbstkritische Hinweise notwendig:

Da ist zum Beispiel die Fixierung auf das Beauftragtenwesen:

Wir wissen genau, dass es nicht der **Datenschutz*beauftragte*** an sich ist, an dem die Welt datenschutzfreundlich genesen wird. Wir wissen auch alle, dass die Frage ab welcher Größe ein Unternehmen einen Datenschutzbeauftragten benötigt, zwar wichtig, aber sekundär ist. Die datenschutzfreundliche Gestaltung der Verarbeitungsprozesse hängt nicht am Beauftragten an sich, sondern letztlich an dem Gestaltungswillen und der Gestaltungskompetenz im Unternehmen ab. Der Datenschutzbeauftragte kann hierzu einen wichtigen Beitrag leisten. Dazu muss er sich richtig einbringen und aufstellen.

Insbesondere bei KMU ist weniger häufiger mehr: Mehr als ein Programm für die ersten 100 Tage kann ein durchschnittlicher Datenschutzbeauftragter im Nebenamt in einem durchschnittlichen Unternehmen mittlerer Größe in einem ganzen Berufsleben nicht bewältigen. Also müssen wir bspw. das Programm für die ersten 100 Tage perfektionieren.

Unsere Erfahrung ist, weniger über Beauftragte und mehr über die **Managementprozesse** nachzudenken, in und mit denen die Datenflüsse im Unternehmen gestaltet werden. Der Datenschutz darf nicht als „fremde Dritte“ über das Unternehmen als gesetzliche Verpflichtung kommen, sondern muss sich als logischer Baustein im Sicherheitsmanagement eines Unternehmens zwangsläufig ergeben: Der Datenschutzbeauftragte als Ergänzung des Sicherheitsmanagements.

Nun werden die Praktiker im Saal sagen, schön, wenn wenigstens das IT-Sicherheitsmanagement flächendekkend in Unternehmen verbreitet wäre. Dass dies nicht der Fall ist, räume ich ein: Aber ich weise darauf hin, dass wir hier einen wichtigen **Bündnispartner** haben. Die Errichtung eines IT-Sicherheitsmanagements wird auch von anderen als nur den Datenschützern gefordert und betrieben, insbesondere aus Gründen des Risikomanagements von Wirtschaftsprüfern und Versicherern.

2.6 Standardisierung

Diese Überlegungen „stechen“ aber nur, wenn es auch eine entsprechende Unterstützung von außen gibt. Wenn in Wirtschaft und Verwaltung Standardsysteme eingesetzt werden – wie bspw. **SAP HR** – dann sollten sich doch auch diese und andere Systeme standardmäßig datenschutzkonform gestalten lassen. Natürlich ist dies der Fall, man muss es nur wollen. Gerade SAP ist ja ein Beispiel, an dem man sehen kann, dass sich eine kleine Community an Datenschützern sogar ohne eine angemessene Unterstützung durch den Hersteller um eine datenschutzkonforme Gestaltung dieser Systeme durch die Entwicklung von Guidelines bemühen kann.

Das Problem ist nur, dass die Aufsichtsbehörden diese und andere Bemühungen zu wenig unterstützen (können) bzw. nicht oder zu wenig rezipieren. Die Juristen denken in Einzelfällen, obwohl sich die Effekte in der Fläche nur durch **Standardisierung** erreichen lassen. Hier liegen die Herausforderungen der Zukunft. Wir stellen uns dieser Herausforderung wo immer wir können: Derzeit durch einen Kollegen im ULD, der mit einem Teil seiner Arbeitskraft im Rahmen eines Projektes die Datenschutzüberlegungen im Rahmen der ISO begleitet.

Ein Beispiel für derartige Bemühungen sind die von uns mit anderen Kollegen bspw. aus Rheinland-Pfalz und Mecklenburg-Vorpommern vorangetriebenen Bemühungen, um eine **revisionssichere Protokollierung der Aktivitäten von IT-Administratoren**. Es geht um die Begrenzung und Kontrolle der Macht der Administratoren (also nicht der Anwender oder Nutzer).

Wir stellen uns vor, dass die Protokolldaten automatisiert auf einen

separierten Server geschrieben und dort als eigenes Verfahren behandelt werden.

Wir stellen uns vor, dass diese Protokolldaten durch gesonderte Tools nach vorgegebenen Auffälligkeiten automatisiert ausgewertet werden (Datenschutzkonsole) und entsprechende Warnhinweise in ein Ticketsystem zur weiteren Bearbeitung im Sicherheitsmanagement gegeben werden (Leitstand).

Natürlich ist die Kontrolle der Administratoren unter Gesichtspunkten einer Leistungs- und Verhaltenskontrolle ein Problem. Auf eine Kontrolle zu verzichten ist aber unter Gesichtspunkten der IT-Sicherheit und des Datenschutzes auch ein Problem: Eine solche Datenschutzkonsole ist bislang nur das Label für eine Lösung, an der für unterschiedliche Verfahren die Community zur Hebung des Datenschutzniveaus beitragen könnte und meiner Überzeugung nach auch muss.

Ein anderes Beispiel für eine Standardisierung ist der Brückenschlag oder Schulterschluss zwischen Datenschutz und IT-Grundschutz des BSI. Wir vertreten mit anderen Kollegen, dass die Maßnahmen des **IT-Grundschutzes den Stand der Technik** für die organisatorisch-technischen Maßnahmen im Sinne des Datenschutzrechtes wiedergeben. Dies ist uns um so leichter gefallen, als das BSI den IT-Grundschutz nun auch um Managementkomponenten geöffnet hat und damit eine Anschlussfähigkeit für das Datenschutzmanagement bietet.

Wir im ULD zertifizieren übrigens mittlerweile auch im Rahmen unseres Datenschutzaudits für Behörden auch nach IT-Grundschutz. Zwei meiner Kollegen haben sich vom BSI zum lizensierten Auditor schulen lassen. Weitere werden folgen.

2.7 Datenschutz-Zertifizierungen

Zur Standardisierung gehört schließlich auch ihre Zertifizierung. Im Grund steckt in jedem Datenschutz-Gütesiegel auch ein kleines **Protection Profile eines Produkttyps** in einer bestimmten Ausprägung. Entsprechendes gilt für die von uns in Schleswig-Holstein auditierten Behördenverfahren und die ihnen zugrunde liegenden Datenschutz- und Sicherheitskonzepte.

Nimmt man also die ca. 40 Gütesiegel und die 20 Auditierungen, so hat man reichlich Stoff für produkt- und anwendungsbezogene Datenschutzstandards.

Über die Bedeutung der Zertifizierung als Angebot an die Wirtschaft habe ich bereits zu Beginn gesprochen. Ich habe auch deutlich gemacht, dass wir in Schleswig-Holstein mit unserem zweistufigen Verfahren sehr gute Erfahrungen gemacht haben.

Die nun vorliegende Konzeption eines einstufigen Auditschemas geht an der Realität leider völlig vorbei: Unsere Erfahrungen zeigen, dass die Qualität der uns vorgelegten Gutachten sehr unterschiedlich ist. Die Aussagekraft der Zertifizierungen hängt letztlich an der Qualitätssicherung durch die Zertifizierungsstelle. Sie ist auch gleichzeitig der Vertrauensanker gegenüber den Betroffenen. Entsprechend verlaufen auch die Diskussionen im europäischen Kontext. Auch EuroPriSe wird ein Netzwerk an europäischen Zertifizierungsstellen vorsehen, die ihre Tätigkeit untereinander koordinieren.

Schlusswort

Ich bin mir bewusst, dass ich Sie als Auditorium aus den Höhen der großen Datenschutzpolitik in die Niederungen der strategischen Datenschutzarbeit geführt habe.

Ich mache dies, weil wir fest davon überzeugt sind, dass die Musik in diesen Niederungen spielt.

Ich habe den Akzent auf den präventiven Datenschutz gesetzt, weil wir Datenschutzkonformität in der Fläche erreichen wollen. Präventiver Datenschutz bedeutet, den rechtlichen Datenschutz durch die Politik „Datenschutz durch Technik“, „Datenschutz als Wettbewerbsvorteil“ sowie „Datenschutz durch Prozessmanagement“ zu ergänzen.

Um dies konkret zu machen, habe ich vor dem Hintergrund unserer Erfahrungen den Aspekt der Gestaltung in den Vordergrund gestellt und dies an den Elementen der Konzeptionierung, der Standardisierung sowie der Zertifizierung verdeutlicht.

Unsere Grundintention ist, uns aus der defensiven Rolle des Jammerns und Klagens in die einer optimistischen Konstruktion zu bringen. Dies bedarf noch einiger Arbeit – also noch weiterer 30 Jahre !

Vielen Dank !

Reinhard Fraenkel

Datenschutz auf dem heißen Stuhl Zur Halbwertzeit der Zweckbindung

Meine sehr geehrten Damen und Herren,

„Datenschutz auf dem heißen Stuhl Zur Halbwertzeit der Zweckbindung“,

Das Oberthema erinnert an eine Fernsehsendung aus den Kindertagen des privaten Fernsehens. Wenn ich mich recht erinnere lief die Sendung bei RTL. Jeweils ein Protagonist musste auf dem heißen Stuhl Platz nehmen und wurde hochnotpeinlich von verschiedenen Menschen über seine Thesen befragt. So möchte ich es heute auch mit dem Datenschutz halten. Es geht mir um eine höchst subjektive Sicht auf den Zustand des Datenschutzes heute. Aus diesem thematischen Zugriff folgt, dass das nachfolgende Thema „Zur Halbwertzeit der Zweckbindung“ nur ein Unterpunkt sein wird. Um gleichwohl das Thema einzugrenzen, werde ich im Rahmen dieses Referates eine gründliche Auseinandersetzung mit der grundrechtlichen Verortung und den damit verbundenen Problemen, die sie dem Datenschutz bereiten, verzichten. Zum Einen haben wir heute Vormittag bereits zur Grundrechtsgebundenheit des Datenschutzes schon einiges gehört, einiges das uns sicherlich nachdenklich stimmt. Andererseits sind meine diesbezüglichen Überlegungen noch nicht endgültig ausgereift und auch sehr theoretischer Natur. Insoweit bitte ich Sie um Verständnis, wenn ich diese grundsätzlichen Überlegungen zur dogmatischen Verortung des Datenschutzes einem gesonderten Referat vorbehalte.

Demgegenüber möchte ich Ihnen heute einen sehr praxisorientierten Werkstattbericht eines in der privaten Wirtschaft tätigen Datenschutzbeauftragten geben, um einmal aus dieser Perspektive den Datenschutz zu beleuchten. Datenschutz und Privatwirtschaft – das scheint ja a priori etwas zu sein, was nicht so recht zusammen passt. Die Vorbehalte, die der Privatwirtschaft entgegen schlagen sind mannigfaltig. Dass beispielsweise die ULD bzw. ihre Protagonisten kaum eine Gelegenheit auslassen, der Privatwirtschaft datenschutzrechtliche Defizite nachzusagen, davon durfte ich mich gerade jüngst wieder im von Ihnen, Herr Bizer, verfassten Editorial von DuD Heft 8/2007 überzeugen.[1] Ich werde darauf gleich noch einmal zurückkommen. Es schwimmt sich ja so gut im Mainstream der Gleichgesinnten. Aber Sie, lieber Herr Bizer, haben ja nur einer weit verbreiteten Meinung, sozusagen der herrschenden Meinung, Ausdruck verliehen. Ich zitiere beispielhaft den ideologisch ja doch weitgehend unverdächtigen Wolfgang Hoffmann-Riem, der 1998 wie folgt formulierte:

„Je stärker der Aufbau der Kommunikationsnetze und die in ihn gestalteten Verkehrsregeln aus der staatlichen Obhut genommen und privater Gestaltung überlassen werden, desto größer ist das von privater Seite ausgehende Gefährdungspotential. Da private Machtträger anders als staatliche nicht den spezifischen rechtsstaatlichen und demokratischen Vorkehrungen der Missbrauchsabwehr unterliegen, ist hier häufig ein gesteigerter Schutzbedarf gegeben, der weitgehend und nur durch positive Schutzvorkehrungen gesichert werden kann.“[2]

Dieses Zitat stammt zwar noch aus der vor Schily/Schäuble-Ära, aber doch schon aus einer Zeit, in der die Innenminister der Bundesrepublik Deutschland vergessen hatten, dass sie auch und in erster Linie Verfassungsminister sind. Die Dignität der gesetzesgebundenen Verwaltung, das sollte man nicht vergessen, hängt ja zunächst und in erster Linie von den Gesetzen ab, die den Aufgabenkanon der Verwaltungen beschreiben und wenn diese Gesetze problematisch sind, ist es natürlich deren Vollzug durch die gesetzesgebundene Verwaltung auch. Unabhängig aber davon bedient Hoffmann-Riem ein Klischee, das auf seine Stichhaltigkeit dringend geprüft werden muss. Nämlich das Klischee, dass Datenschutz im öffentlichen Bereich gesicherter ist als in der Privatwirtschaft.

Insofern ist es also seitens der Veranstalter schon beachtlich, dass sie mich gebeten haben, zu diesem Thema zu referieren. Ich berate ja in meiner Funktion als Rechtsanwalt in Datenschutzfragen nicht einfach nur irgendwelche Unternehmen. Nein, im Jahre 2002 war ich der betriebliche Datenschutzbeauftragte eines Unternehmens, dem der Big Brother Award zumindest mittelbar umgehängt worden ist, ein Sachverhalt, der mich bis heute mit Verbitterung erfüllt, den ich aber, um die sich ausbreitende Feststimmung hier und heute nicht mehr als notwendig zu trüben, auf sich beruhen lassen will. Aktuell bin ich Datenschutzbeauftragter eines Unternehmens, das 2002 ebenfalls den Big Brother Award bekommen hat. Darüber allerdings wird hier noch zu reden sein, weil die Auswirkungen dieser Preisverleihung bis heute spürbar sind.

Ich bin also formal betrachtet in der Reihe der heutigen Referenten eher das schwarze Schaf. Ich kann weder für mich die unbestreitbare Seriosität eines Burkhard Hirsch in Anspruch nehmen, noch mit einem durchaus verdienten Amtsbonus der von den jeweiligen Parlamenten berufenen Datenschutzbeauftragten glänzen. Auch

1 DUD 2007 S. 558

2 Wolfgang Hoffmann-Riem Informationelle Selbsbestimmung in der Informationsgesellschaft – Auf dem Wege zu einem neuen Konzept des Datenschutzes in AöR 1998 S. 513 ff., 525

mit akademischen Ehren kann ich mich nicht schmücken. Dass meine Sicht auf den Datenschutz also eine etwas andere ist als die vieler anderer, dürfte nach diesem kleinen aber aus meiner Sicht notwenigen Vorspann deutlich geworden sein.

Datenschutz auf dem heißen Stuhl – das ist für mich natürlich die Halbwertzeit der Zweckbindung oder, um es anders zu sagen, der Umgang des Gesetzgebers mit Datenschutz. Datenschutz auf dem heißen Stuhl ist aber auch aus meiner Sicht die Infragestellung des Paradigmas, dass die Gefährdungen des Datenschutzes mehr von der Privatwirtschaft und weniger von der staatlichen Verwaltung ausgehen. Wer über Datenschutz auf dem heißen Stuhl heute referiert, kann natürlich, auch wenn Sie, meine sehr geehrten Damen und Herren, das heute schon mehrfach gehört haben, zu dem Skandal der Vorratsdatenspeicherung nicht schweigen. Schließlich muss auch die Arbeit der Aufsichtsbehörden selber thematisiert werden, die in ihrer Qualität und in der Wahrnehmung ihrer Aufgaben, bei der Vielzahl der Behörden auch keine große Überraschung, schon erhebliche Unterschiede aufweisen und so zumindest teilweise auch an der Legitimitätskrise des Datenschutzes mit Schuld tragen. Zu guter letzt heißt Datenschutz auf dem heißen Stuhl für mich auch zu konstatieren, dass die Fortsetzung der alten Grabenkämpfe, wie sie in der Neuformulierung des § 28 BDSG peinlichen Ausdruck finden, den Blick verstellt auf ganz neue Herausforderungen, die im Schema der Vermachtungen von öffentlichem Sektor einerseits und Privatwirtschaft andererseits nur noch unzureichend beschrieben sind.

I. Zur Halbwertzeit der Zweckbindung

Durch die eben vorgestellten Themenfelder zieht sich wie ein roter Faden meine Generalthese. Sie lautet: Der Datenschutz wird abgeschafft. Wo er nicht abgeschafft wird, ist er drauf und dran sich selber abzuschaffen. Als betrieblicher Datenschutzbeauftragter der Firma Toll Collect bin ich in das Gesetzgebungsverfahren um eine Novellierung des Autobahnmautgesetzes (ABMG) zumindest am Rande mit involviert. Worum geht es bei dieser Novelle? Der Gesetzgeber hat mit der Verabschiedung des ABMG eine strikte Zweckbindung der unmittelbar mautrelevanten Daten verbunden. Fahr- und Kontrolldaten sollten ausschließlich für Zwecke des Mautgesetzes genutzt werden dürfen. Diese Regelung erwies sich als brüchig, als nämlich das Amtsgericht Gummersbach 2003 im Rahmen einer teleologischen Reduktion zu dem Ergebnis kam, dass trotz des eindeutiges Wortlautes des Gesetzes es Fälle gäbe, in denen Daten auch für andere Zwecke, hier für Zwecke der Strafverfolgung, übermittelt und genutzt werden dürften.

Daraufhin hat der Gesetzgeber erstaunlich schnell reagiert. Im Dezember 2004 wurden die §§ 4 Abs. 2 und 7 Abs. 2 ABMG, in denen die Nutzung und Übermittlung der Maut- und Kontrolldaten geregelt sind, um einen Satz erweitert. Der Satz lautet: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig." Durch diese Klarstellung wurde endgültig festgelegt, dass Mautdaten selbst im Falle eines richterlichen Beschlusses nicht herauszugeben sind.

Diese Ergänzung ist 2004 immerhin nahezu einstimmig im Deutschen Bundestag verabschiedet worden, also nicht nur mit den Stimmen der damals regierenden rot-grünen Koalition, sondern auch mit den Stimmen der CDU/CSU-Fraktion.

Seitens der Polizeibehörden ist diese Verschärfung der Zweckbindung nie akzeptiert worden und auch Amtsgerichte haben trotz des nun eindeutigen Wortlautes weiterhin Beschlagnahmeverfügungen erlassen. Das Mautsystem startete am 1. Januar 2005, die erste Beschlagnahmeverfügung des Amtsgerichts Frankfurt am Main erfolgte am 7. Januar 2005. Die Beschlagnahme konnte durch ein kurzes Telefonat mit dem Richter abgewendet werden, indem der Richter freimütig zugab, er kenne das Gesetz gar nicht. Er sei davon ausgegangen, dass hier dem Telekommunikationsrecht vergleichbare Regelungen zur Anwendung kämen. Wenn mir als Anwalt ein ähnlicher Fehler unterlaufen wäre, wäre ich wahrscheinlich auch noch vom gleichen Richter zu einer hohen Schadensersatzzahlung verurteilt worden, weil ich meine Pflichten als Rechtsanwalt grob fahrlässig verletzt hätte, denn der Rechtsanwalt hat ja das Recht zu kennen. Nehmen Sie dies, meine Damen und Herren, auch als einen ersten kleinen Hinweis darauf, dass es mit dem Datenschutz in den Behörden, zu denen ja auch die Gerichte gehören, auch nicht immer zum Besten bestellt ist.

Erlauben Sie mir noch zwei Beispiele aus der täglichen Praxis: Ein Kriminaldirektor des bayrischen LKA, natürlich des bayrischen LKA möchte man meinen, aber es hätte genau so gut das LKA Hamburg sein können, wollte für Ermittlungszwecke Mautdaten. Dies habe ich unter Verweis auf die Rechtslage verweigert. Daraufhin sagte er: „Wir haben andere Mittel und Möglichkeiten, uns die Daten zu be-

schaffen.“ Dies sei aber rechtswidrig, erklärte ich, woraufhin ich belehrt wurde, über die Rechtsmäßigkeit einer Maßnahme entscheide immer noch die Polizei. Da kann ich nur sagen: Danke!

In einer ähnlichen Situation teilte mir ein Polizeibeamter mit, wenn er die gewünschten Daten von der Toll Collect GmbH nicht erhalten könne, dann gäbe es ja immer noch das BAG. Er sei davon überzeugt, dass die beamteten Kollegen schon bereitwilliger mit der Hergabe von Daten für Strafverfolgungszwecke seien. Hier, meine Damen und Herren, ist nicht der Ort, über das Verhältnis des BAG und Toll Collect viele Worte zu machen. Eines aber wird man nicht sagen können: Die Strafverfolgungsbehörden haben es beim BAG sicherlich keinen Deut leichter als bei der Toll Collect GmbH, an Mautdaten im engeren Sinne heranzukommen. Sie sind noch tabu, ganz unabhängig davon, an welche Stelle, die Toll Collect GmbH oder das BAG, sich Polizeidienststellen wenden. Immerhin war ja die Erwartung des Polizeibeamten ganz offenbar erfahrungsgesättigt, was ich durchaus als weiteres Indiz für meine These werte, dass der Datenschutz in Behörden auch verbesserungsbedürftig ist.

Die strikte Zweckbindung im Mautgesetz soll allerdings aufgehoben werden und Daten auch für Zwecke der Strafverfolgung nutzbar gemacht werden. Ich persönlich halte eine moderate, auf eng begrenzte Tatbestände reduzierte Öffnung der Zweckbindung für sinnvoll und geboten. Als Datenschutzbeauftragter kommen Sie in ein unausweichliches moralisches Dilemma, wenn Sie an der Aufklärung eines Tötungsdeliktes durch Hergabe von Daten mitwirken könnten. Das gilt insbesondere dann, wenn es sich, wie im vergangenen Jahr, um einen Fall von Vergewaltigung mit anschließender Tötung handelte und ganz offensichtlich der Täter ein Wiederholungstäter war. In dieser Situation gegen alle Pressionen, die es auch seitens der Politik konkret gegeben hat, der Linie des Rechts zu folgen, verwischt die Grenzen von Gesinnungs- und Verantwortungsethik. Zurück bleibt einmal mehr die Erkenntnis, dass Handeln sich schuldig machen heißt, aber Nicht-Handeln eben auch.

Insofern bekenne ich mich persönlich dazu, die strikte Zweckbindung im Mautgesetz für begrenzte Fälle schwerster Kriminalität, insbesondere gegen Leib und Leben und gegen die sexuelle Selbstbestimmung zu lockern. Vielleicht wäre es sinnvoll gewesen, eine entsprechende Öffnungsklausel von vornherein in die §§ 4, 7 ABMG aufzunehmen. Dass es sich der Gesetzgeber nicht leicht macht, sieht man allein daran, dass das Verfahren einer Änderung des Mautgesetzes an dieser Stelle schon etwa 24 Monate in Anspruch nimmt. Wäre es allein nach dem Innenministerium gegangen, gäbe es die entsprechende Rechtsänderung schon lange. Eine entsprechende Änderung wird kommen und sie wird wahrscheinlich sehr viel weitergehend sein, als ich es für wünschenswert halte.

Zwar wird es einen Richtervorbehalt geben, aber, meine Damen und Herren, der Richtervorbehalt ist kein allein selig machendes Mittel. Ganz unabhängig davon, wie die endgültige gesetzliche Regelung aussehen wird, es bleibt natürlich ein verheerender Eindruck zurück. Die Bundesregierung hat sich entschlossen, die anonyme Vignettenlösung durch ein komplexes, den fließenden Verkehr weitgehend nicht behinderndes System einer nutzungsabhängigen Maut abzulösen. Dass bei einem solchen System zwangsläufig Streckendaten mautpflichtiger Fahrzeuge anfallen, ist systembedingt. Dies gilt auch für die Maßnahmen der automatischen Kontrolle der Mautpflicht die in ihrer realisierten Variante als Musterbeispiel eines in die Technik integrierten Systemdatenschutzes gelten darf.

Die Verankerung der strikten Zweckbindung der Mautdaten im ABMG sollte eventuelle Bedenken des BfDI ebenso ausräumen, wie vergleichbare Bedenken des ADAC oder der Verbände des Speditionsgewerbes. Wenn sie jetzt wieder durch die geplante Novelle des ABMG zur Disposition gestellt wird, riskiert der Gesetzgeber einen weiteren Vertrauensverlust der Bürger bzw. der in solche Gesetzgebungsverfahren involvierten Behörden wie den BfDI. Die Auswirkungen auf das bestehende System sind schon jetzt, vor der Änderung des ABMG, spürbar.

In seinem letzten Tätigkeitsbericht hat der Bundesbeauftragte für Datenschutz und Informationssicherheit sich des Mautthemas noch einmal angenommen und sich ganz ähnlich wie seinerzeit Frank Rosengarth in seiner Begründung für die Verleihung des Big Brother Awards an Toll Collect geäußert: „Ich“, so heißt es im 21. Tätigkeitsbericht auf Seite 124, „hielte es für keineswegs akzeptabel, das jetzige, auf schwere Lkw beschränkte Verfahren, bei dem eine Vielzahl von Daten über jeden zurückgelegten Kilometer erfasst werden, unverändert auf Pkw zu übertragen. Vielmehr muss frühzeitig über Alternativen nachgedacht werden, bei denen es nicht zu einer fahrzeugbezogenen Vollüberwachung kommt.“

Ich lade den Bundesbeauftragten für Datenschutz und Informationssicherheit hiermit gerne ein und bin diesbezüglich auch vom Sprecher der Geschäftsführung der Toll Collect GmbH ausdrücklich bevollmächtigt, zu einer intensiven Diskussion mit allen Verantwortlichen zu der Frage, ob angesichts der gesetzlich vorgegebenen Aufgaben die Toll Collect GmbH zu viele Daten erhebt. Auch die unterstellte Vollüberwachung findet nicht statt. Diese Begrifflichkeit hat mich, das will ich offen sagen, angesichts der Intensität des Informationsaustausches zwischen der Toll Collect GmbH und dem BfDI etwas überrascht. Der Begriff der Vollüberwachung ist negativ besetzt und trifft auch nicht das, was die Toll Collect GmbH macht. Die Toll Collect GmbH erhebt von den Nutzern des Mautsystems die Maut und legt anhand der gefahrenen Kilometer den Mautpflichtigen gegenüber Rechnung. Das Mautsystem ist kein Instrument zur Verkehrsüberwachung und lässt sich auch nicht ohne massive Eingriffe in die Programme in ein entsprechendes System transformieren. Ich kann die Äußerungen des BfDI nur als bereits an die Politik adressiert verstehen und auch als Ausdruck einer gewissen Enttäuschung gegenüber dem Gesetzgeber einmal ja auch dem BfDI gegenüber abgegebene Zusicherungen alsbald über Bord zu werfen. Leider entsteht dabei auch in der Öffentlichkeit der fatale Eindruck, Toll Collect erhebe mehr als unbedingt notwendig

Bewegungsdaten und betreibe zumindest für den LKW-Verkehr eine flächendeckende Verkehrsüberwachung.

Aber zurück zum Gesetzgeber. Ob ihn angesichts viel weitergehender Gesetzesvorhaben, die den Datenschutz elementar aushöhlen, ein eventueller Vertrauensverlust wirklich interessiert, erscheint mir fraglich. Es dürfte ihm letztlich egal sein. Die Halbwertzeit der Zweckbindung, bezogen auf das Mautgesetz, beträgt also voraussichtlich vier Jahre. Ob sich allerdings das schwindende Vertrauen in die Zuverlässigkeit der Gesetzgebung auf eine mögliche Ausweitung der Mautpflicht auf Fahrzeuge unter 12 t zulässiges Gesamtgewicht auswirken wird, steht in den Sternen, obwohl ich persönlich glaube, dass selbst eine PKW-Maut jedenfalls nicht an der jetzt zu erwartenden Aufweichung der Zweckbindung scheitern würde.

II. Exkurs Zur datenschutzrechtlichen Zuverlässigkeit der öffentlichen Verwaltung

Ich muss noch einmal auf den 2002 an Toll Collect vergebenen Big Brother Award zurückkommen. In den Gründen für die Preisverleihung heißt es unter anderem: „Die Zusicherung der Betreiber, dem Datenschutz Sorge zu tragen, erscheint bei der Größenordnung der Erfassung und den Möglichkeiten der Auswertung nicht angemessen." In diesem Satz drückt sich einmal mehr das Misstrauen aus, das Privatunternehmen entgegen schlägt, wenn es um Datenschutz geht. Ich hatte eingangs bereits beispielhaft Wolfgang Hoffmann-Riem zitiert und auf entsprechende Äußerungen von Herrn Bizer verwiesen. Diesem Misstrauen gegenüber privaten Unternehmen einerseits und dem damit zugleich verbundenen Vertrauen gegenüber der staatlichen Verwaltung tragen auch die Überrmittlungsregelungen des BDSG selber Rechnung. Dies wird exemplarisch durch einen Vergleich der §§ 15,16 BDSG deutlich. § 15 BDSG regelt die Datenübermittlung an öffentliche Stellen. In § 15 Abs. 2 Satz 2 BDSG heißt es: „Erfolgt die Übermittlung auf Ersuchen des Dritten an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt. …".

Fordert also eine öffentliche Stelle, beispielsweise die Polizei, von einer anderen öffentlichen Stelle Daten an, trägt die Verantwortung für die Rechtmäßigkeit der Datenübermittlung nicht die übermittelnde Stelle, sondern die anfordernde Stelle. Die anfordernde Stelle müsste also in jedem Einzelfall prüfen, ob sie die Daten überhaupt anfordern darf oder ob es möglicherweise Übermittlungshemmnisse gäbe. Übermittlungshemmnisse, wie wir sie gegenwärtig noch im ABMG haben. Der Datenschutzbeauftragte der anfordernden Polizeibehörde müsste, so mein Verständnis, im Vorfeld prüfen, ob die Polizeibehörde auf Mautdaten zugreifen darf. In diesem Zusammenhang müsste er auf das ABMG stoßen und den Ermittlungsbeamten mitteilen, dass ein Zugriff auf Mautdaten unzulässig sei. Von einem derartigen Datenschutzbeauftragten habe ich aber bis jetzt nichts gehört.

Erfolgt andererseits die Datenübermittlung an nicht-öffentliche Stellen, trägt ohne Wenn und Aber die Verantwortung für die Zulässigkeit der Übermittlung die übermittelnde Stelle. Gegenüber privaten Institutionen muss also eine Daten übermittelnde Behörde in jedem Fall die Zulässigkeit der Übermittlung überprüfen. In der unterschiedlichen Behandlung drückt sich die Hoffnung des Gesetzgebers aus, dass die Verwaltung strikt gesetzesgebunden arbeitet. Zugleich drückt sich ein quasi institutionalisiertes Misstrauen gegenüber Privatunternehmen aus. Ob diese unterschiedliche Behandlung tatsächlich gerechtfertigt ist, darüber kann man durchaus geteilter Meinung sein. Ich halte in jedem Falle die doppelte Kontrolle, wie sie für die Privatwirtschaft selbstverständlich ist, auch für Datenübermittlungsvorgänge in der Verwaltung für angemessen und richtig. Im privaten Bereich ist es ja so: Will eine private verantwortliche Stelle von einer anderen verantwortlichen Stelle Daten erheben, muss natürlich zunächst die die Daten begehrende Stelle prüfen, ob sie die Daten erheben darf. Andererseits aber muss die Daten abgebende Stelle selbstverständlich prüfen, ob sie die Daten übermitteln darf. Ich halte, wie gesagt, meine Damen und Herren, diese Regelung für sinnvoll und geboten. Sie mag gelegentlich den Prozess des Datenaustausches verzögern, dies ist aber im Interesse der Sache hinzunehmen.

Die datenschutzrechtliche Sensibilität öffentlicher Verwaltungen ist im Übrigen nicht so überragend, als dass es gerechtfertigt wäre, immer nur in der ja angeblich permanent Daten sammelnden Privatwirtschaft den bösen Buben zu sehen. Ich bin betrieblicher Datenschutzbeauftragter eines Unternehmens, das im Rahmen der A uftragsdatenverarbeitung Jahr für Jahr im siebenstelligen Bereich Einwohner meldeamtsanfragen stellt. Dabei handelt es sich in aller Regel um einfache Einwohnermeldeamtsanfragen. Welche Daten im Rahmen der einfachen Einw ohnermeldeamtsanfrage tatsächlich übermittelt werden dürfen, ist aber sehr vielen Einwohnermeldeämtern nicht bekannt. Jedenfalls enthalten ca. 10 % der Auskünfte auch Daten, die nur im Rahmen einer erweiterten EMA mitgeteilt werden dürften. Gott sei Dank gibt es in diesem Zusammenhang einmal kein Nord-Süd-Gefälle. Einwohnermeldeämter also in Schleswig-Holstein sind genauso betroffen, wie vergleichbare Ämter in Bayern oder Baden- Württemberg. Insoweit erweist sich jedenfalls für mich das Urteil, Verwaltungen seien a priori datenschutzsensibler als die freie Wirtschaft, als durchaus überprüfenswertes Vorurteil. Dieses Problem aber scheint hier in diesem Rahmen durchaus bekannt zu sein, denn immerhin werden ja auch Behörden mit dem Big Brother Award ausgezeichnet. Ich kann allerdings nach den von mir gemachten Erfahrungen nur hoffen, dass diese Auszeichnungen auch zu Recht erfolgen.

III. Zur Vorratsdatenspeicherung

Meine Kernthese, dies nur zur Erinnerung, lautet: Der Datenschutz wird abgeschafft. Die

Vorratsdatenspeicherung ist ein gutes Fallbeispiel. Sie trägt zur Fortentwicklung des Datenschutzes nichts bei. Im Gegenteil! Durch die Vorratsdatenspeicherung wird der Datenschutz geschleift. Er steht trotz aller Sonntags- oder Demonstrationsreden generell zur Disposition. Tragende Säulen des Datenschutzrechts sind mit den Begriffen „Erforderlichkeit“ und Zweckbindung“ umschrieben. Jede Art der Verarbeitung personenbezogener Daten hat sich an diesen Rechtskategorien zu messen. Sie sind, gemeinsam mit dem Gebot, Daten zu löschen, wenn sie nicht mehr erforderlich sind, der Gratmesser der Zulässigkeit von Datenverarbeitung schlechthin. Ein datenschutzrechtlich einwandfreier Prozess kann durch Subsumtion dieser Begriffe auf den Einzelfall hin konstruiert und verwirklicht werden. Der Prozess der Datenverarbeitung ist also von seinem Ende her zu denken. Diese Herangehensweise, Datenschutzprozesse über ein Löschkonzept zu strukturieren, vermag dem Unternehmen, das sich dieser Prozedur aussetzt, Geschäftsprozesse selber transparenter zu machen als dies ohne eine entsprechende Herangehensweise der Fall wäre. Wie dies im Einzelnen aussehen kann, ist Gegenstand zweier Aufsätze, an denen Dr. Hammer von der Secorvo Consulting GmbH und ich aktuell arbeiten. Natürlich ist ein solches Konzept in Unternehmen und Verwaltung nur durchsetzbar, wenn Zweckbindung und Erforderlichkeit den Stellenwert in der datenschutzrechtlichen Gesetzgebung erhalten bzw. behalten, die sie als tragende Säulen eines datenschutzrechtlich einwandfrei organisierten Prozesses ausweisen. Genau diese Funktionen werden aber durch die Richtlinie zur Vorratsdatenspeicherung bei Verbindungsdaten für die die Leistungen erbringenden Unternehmen außer Kraft gesetzt. Die diesbezüglichen Vorschriften des TMG bzw. TKG werden geschleift. Der Gesetzgeber selber unterminiert damit die entscheidenden Säulen jeder datenschutzrechtlich konformen Verarbeitung von Daten. Flatrates in der TK-Branche entheben die leistungserbringenden Unternehmen von der Notwendigkeit, Verbindungsdaten eines Kunden zu speichern. Damit werden Datensparsamkeit ermöglichende Tarifmodelle initiiert. Weil dies aber einem unbestimmten A ufklärungsinteresse des Staates zuwider läuft, werden durch die Vorratsdatensp eicherungsrichtlinie derartige Prozesse außer Kraft gesetzt. Weil dies gerade nicht mehr anlassbezogen geschieht, sondern prophylaktisch und sich auf alle Formen elektronischer bzw. digitaler Verbindungsdaten erstreckt, entwertet der Gesetzgeber selber seine diesbezüglichen rechtlichen Grundlagen im BDSG.

Über die inhaltlichen Konsequenzen der Vorratsdatenspeicherung haben wir heute schon einiges gehört. Deswegen kann ich mich an dieser Stelle kurz fassen. Die Vorratsdatenspeicherung der TK-Verbindungsdaten hat im Gegensatz zur Erstellung von Bewegungsprofilen noch ganz andere Auswirkungen. Bewegungsprofile geben immer „nur“ Auskunft über die Bewegungen einer einzelnen Person oder einer Personengruppe. Eine systematische Auswertung aber der TK-Verbindungsdaten gibt Auskunft über soziale Beziehungen und Beziehungsnetzwerke. Dies ist eine ganz andere Qualität. In der Anhörung vor dem entsprechenden Bundestagsausschuss hat ein als Experte geladener Mitarbeiter eines Landeskriminalamtes diese spezifische Qualität so auf den Punkt gebracht: „Wenn wir alle TK- bzw. digitalen Verbindungsdaten eines Bürgers für sechs Monate gespeichert haben, haben wir seine elektronische DNA.“ Es wird plötzlich sichtbar, wie verschiedene Menschen auf bestimmte Nachrichten reagieren. Wer plötzlich wen anruft. Ob plötzlich bei einem vermehrt Anrufe eingehen und ähnliches mehr. Es bedarf gar nicht mehr der Gesprächsinhalte, wenn man in derartiger Dichte über Verbindungsdaten verfügt. Es gibt genügend andere Anknüpfungspunkte, aufgrund derer dann auf Inhalte rück geschlossen werden kann.

Insoweit ist also die Regelung zur Vorratsdatenspeicherung in doppelter Weise katastrophal. Sie höhlt zentrale Begriffe aller datenschutzrechtlichen Regelungen aus und entwertet sie damit. Darüber hinaus wird das gesamtgesellschaftliche Beziehungsgeflecht jedes einzelnen Bürgers zu allen anderen mittelbar und unmittelbar transparent.

Keiner, meine Damen und Herren, kann ernsthaft behaupten, die Bundesrepublik Deutschland sei ein Polizeistaat. Aber da wo Datentöpfe angelegt werden, werden auch Begehrlichkeiten geweckt. Das prinzipielle Unbehagen, das mich angesichts dieser neuen Möglichkeiten der Analyse privater Beziehungsgeflechte beschleicht, wird eben gerade dadurch bestärkt, dass die Ermittlungsprozesse der Strafverfolgungsbehörden, die unmittelbar in Grundrechtspositionen der Bürger eingreifen, auch im Nachhinein viel zu wenig transparent gemacht werden.

Der präventiv wirken sollende viel beschworene Richtervorbehalt ist auch nur ein bedingt taugliches Abwehrmittel. Nicht immer kennen die Richter das Recht. Oft werden sie mit Sachverhalten konfrontiert, die ausschließlich aus der Brille ermittelnder Polizeibeamter dargestellt werden. Oft sind Richter auch schlicht überfordert von beispielsweise einem stressigen Notdienst. Natürlich gibt es unbestreitbar eine große Nähe zwischen Staatsanwaltschaften und Gerichten. All dies nährt durchaus berechtigte Zweifel, dass ausgerechnet der Richtervorbehalt die Schutzschwelle darstellen soll, die die Bürger in jedem Falle vor unzulässigen Übergriffen des Staates schützen. Erst jüngst hatte das Bundesverfassungsgericht durch Kammerbeschlüsse vom 4. Juli 2006, 18. April 2007 und 30. April 2007 drei Verfassungsbeschwerden, in diesem Falle von Rechtsanwälten, gegen die Überwachung ihrer TKAnschlüsse stattgegeben.[3] Ich erlaube mir nur ein Zitat aus einem der entsprechenden Beschlüsse: „Das Amtsgericht ist weder den Anforderungen des verfassungsrechtlichen Richtervorbehalts aus Art. 13 Abs. 2 GG gerecht geworden, noch den besonderen Sorgfaltsanforderungen, die sich aus Art. 12 Abs. 1 GG bei der Anwendung des einfach gesetzlichen Richtervorbehalts aus § 100d Abs. 1 StPO ergeben.“[4]

Das Amtsgericht Friedberg, um noch einmal auf das Mautgesetz zurück zu kommen, ist in seinem der Herausgabe von Mautdaten stattgebenden Beschluss aus dem Jahre 2006 vom ABMG in der

3 Vgl. DUD 2007 S. 616 ff.

4 a.a.O., S. 623

Fassung des Jahres 2002 und nicht von der aktuellen Fassung des ABMG vom 7. Dezember 2004 ausgegangen. Auch dem Amtsgericht Oschersleben war im Jahr 2005 nicht bekannt, dass das ABMG novelliert worden sei und auch das Landgericht Magdeburg ist seinem Beschluss vom 03.02.2006 ganz offenbar davon ausgegangen, dass das ABMG in der Fassung von 2002 gelte.[5]

Eine kriminologische Untersuchung von Prof. Pfeiffer aus Hannover hat gezeigt, dass 1/3 aller Verfahren, die als Morduntersuchungen beginnen, tatsächlich nur zu Verurteilungen wegen Mordes führen. Gleichwohl liegt natürlich zu Beginn einer Untersuchung das Definitionsmonopol der vermuteten Straftat bei den Ermittlungsbehörden. Unter Zugrundelegung des von den Ermittlungsbehörden unterbreiteten Sachverhalts trifft der Richter seine Entscheidung. Dass die Entscheidungen nicht immer richtig sind, habe ich eben kurz belegt. Durch die Definitionsmacht der Ermittlungsbehörden wird das Problem aber noch verschärft. Es entzieht sich unserer Kenntnis, in wie vielen Fällen völlig zu Unrecht eine TKÜberwachung angeordnet wurde. Ebenso entzieht es sich unserer Kenntnis, in wie vielen Fällen denn eine TK-Überwachung tatsächlich ermittlungstechnisch zu einem Erfolg geführt hat. Es stärkt eben nicht das Vertrauen in den Rechtsstaat, wenn derartige Statistiken nicht vorgelegt werden müssen. Das Risiko von Bürgern, in strafrechtliche Ermittlungen hineingezogen zu werden, steigt aber durch die Auswertung der Vorratsdatenspeicherung noch um ein Vielfaches, weil, wie gesagt, durch die Zusammenschau dieser Daten Netzstrukturen sichtbar werden, die Auskunft über das komplexe soziale Geflecht, in das jeder einzelne eingebunden ist, geben. Da spielt es dann eben keine Rolle mehr, ob das Kind eines Verdächtigen den gleichen Kindergarten besucht wie das eigene Kind. Durch die verabredete Telefonkette zur Benachrichtigung bei besonderen Vorkommnissen im Kindergarten gehört man eben auch zum sozialen Umfeld des Verdächtigen. Breiter, auch von großen Teilen der Bevölkerung getragener Protest gegen die Vorratsdatenspeicherung ist gleichwohl nicht in Sicht.

Es hat ganz offensichtlich auf breiter Basis einen Abstumpfungsprozess in der Bevölkerung gegeben. Wir haben uns daran gewöhnt, dass staatliche Stellen auf private Lebensdaten zugreifen. Ich nenne beispielhaft das Recht der Steuerbehörden, auf Bankdaten zuzugreifen. Wir gewöhnen uns an biometrische Vermessungen in Ausweis und Pass. Die Polizeigesetze einzelner Bundesländer lassen das flächendeckende Screening von Kfz-Kennzeichen zu. So findet ein schleichender Aushöhlungsprozess statt, der, gepaart mit dem Argument, „Wer nichts zu verbergen hat, hat auch nichts zu befürchten“, die datenschutzrechtliche Sensibilität der Bürger immer weiter herabsetzt. Es gibt eben im Jahre 2007 keine dem Volkszählungsurteil des Bundesverfassungsgerichts 1983 vorausgehende breite Bürgerbewegung gegen staatlich organisierte Datensammlungen. Weder die einheitliche Steuernummer, die auf der Tagesordnung steht, noch die Online-Durchsuchung von PCs wird daran etwas ändern. Die Situation von 1983 wird heute als einmalige, nicht wiederholbare Sondersituation eingeschätzt. Ich zitiere aus der Süddeutschen Zeitung vom 9.10.2007: „Nicht wiederholbar scheint die kollektive Hysterie anlässlich der Volkszählung in der Bundesrepublik von 1983, eine Überwachungshysterie die damals mit der apokalyptischen Untergangsgier angesichts von Waldsterben und Atomraketen einher ging und die sich auch in dem nachfolgenden Urteil des Bundesverfassungsgerichts nieder schlug.“ So bösartig also wird der Bürgerprotest von 1983 heute gesehen.[6] Selbstverständlich weisen die Aufsichtsbehörden in ihren Tätigkeitsberichten pflichtschuldig auf ihre verfassungsrechtlichen Bedenken gegenüber der staatlichen Sammelwut hin. Diese wird auch breit vom BfDI Peter Schaar in seinem Buch: „Das Ende der Privatsphäre“ thematisiert. Auf spezifische verfassungsrechtliche Bedenken bei der geplanten Vorratsdatenspeicherung hat jüngst auch Herr Bizer hingewiesen.[7]

Dass Sie, lieber Herr Bizer, Ihren Aufsatz im Editorial des gleichen Heftes zum Anlass nehmen, gegen private Dienstleister nachzutreten, hilft der Sache wenig[8], öffnet aber einen Sandkasten, in dem die gegenüber staatlichen Datensammlungen weitgehend ohnmächtigen Datenschutzbeauftragten spielen können und an Gesetzen mitbasteln dürfen, die die eigennützige Datenverarbeitung gemäß § 28 BDSG durch Einzelfallregelungen weiter kompliziert und den Datenschutz zur lex specialis eines Verbraucherschutzgesetzes mutieren lässt. Auf diesen Skandal werde ich gleich noch zurückkommen.

Thilo Weichert übt sich derweil als Volkstribun. Seine Rede anlässlich der Zwischenkundgebungen der Demonstration „Freiheit statt Angst – Stoppt den Überwachungswahn“ erinnert streckenweise an die Diktion der frühen 68er. Zitat: „Sie wollen uns einsperren. Sie wollen uns nicht hinter Mauern und Gittern einsperren, sondern in einen informationellen Käfig.“ Der bewusste Verzicht auf Konkretion suggeriert, dass hier dunkle Mächte am Werke sind. Es sind aber keine dunklen Mächte am Werke. Es ist der Deutsche Bundestag, der auf Vorschlag von Innen- und Justizministerium derartige Gesetze erlässt. Am Schluss seiner Rede wird Weichert eschatologisch wenn er sagt: „Es gibt aber keinen Anlass zur Resignation:

Übermäßige Überwachung muss nämlich nicht Aggression und Depression auslösen, sie kann auch Kritik und Widerstand auslösen. Und genau diesen Effekt haben die jüngsten verfassungsfeindlichen Überwachungsbestrebungen .“ Für die Zukunft ist er optimistisch und leitet seinen Optimismus einmal mehr von dem Vertrauen in die Judikatur des

5 Vgl. dazu näher Fraenkel/ Hammer „Keine Mautdaten für Ermittlungsverfahren“ in: DUD 2006 S. 497 ff.

6 Siehe Johann Schloemann „Der Staat ist nicht dein Freund“, Süddeutsche Zeitung 9.10.2007

7 Bizer, Vorratsdatenspeicherung – Ein fundametaler Verfassungsverstoß in DUD 2007 S. 586 ff.

8 Bizer, a.a.O, S. 558

Bundesverfassungsgerichts ab.[9]

Da wird die Hoffnung also auf acht Personen fokussiert. Wieder einmal soll es das Bundesverfassungsgericht richten. Der Glaube an diese Institution ist groß. Ein mythologischer Heilsbringer ist das Gericht auch für den Berliner Beauftragten für Datenschutz und Datensicherheit, Herrn Dr. Dix. Am 10. November 2006 hielt er einen Vortrag zum Neuro-Screening, Hirndoping, Cyborgs.[10] In diesem Zusammenhang ging Dix auch auf die Entscheidung des Bundesverfassungsgerichts zum großen Lauschangriff vom März 2004 ein, in dem festgestellt wurde, dass zur Unantastbarkeit der Menschenwürde die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung gehöre, in dem der Staat auch zu Zwecken der Strafverfolgung nicht eingreifen dürfe.[11] Den Satz: „Eine Abwägung nach Maßgabe des Verhältnismäßigkeitgrundsatzes zwischen der Unverletzlichkeit der Wohnung und dem Strafverfolgungsinteresse des Staates findet insoweit nicht statt“, bejubelt Dix mit den Worten: „Mit dieser kategorischen, geradezu befreiend wirkenden Aussage wird ein explizites Abwägungsverbot ausgesprochen.“[12]

Was wirkt befreiend? Offensichtlich das Abwägungsverbot. Hier ist endlich ein Grund von Klarheit, auf den sich aufbauen lässt. Kein abwägungstechnischer Treibsand mehr, sondern eine klare, unverrückbare Aussage. Dies ist der Fels, auf dem Dix seinen Rechtsstaat gründen will. Schade nur, dass Dix acht Zeilen später auch darauf hinweist, dass diese kategorische Aussage so doch nicht stehen bleibt: „Das Gericht hat eine Ausnahme von dieser kategorischen Aussage für den Fall gemacht, dass jemand in seiner Wohnung mit Familienangehörigen über seine Beteiligung an einer schweren Straftat spricht.“[13]

Das ist eben das Elend an der Abwägung, dass sich die Gewichte immer verschieben können. Insofern ist Kritik am Paradigma der Abwägung dringend geboten.[14]

Darauf zu hoffen also, dass „Rettung“ vom Bundesverfassungsgericht kommt, erscheint mir eine trügerische Hoffnung, zumal natürlich auch das Bundesverfassungsgericht bei allem Bemühen um Objektivität eben auch Einflüssen aus Politik und Gesellschaft ausgesetzt und in seiner Rechtsprechung durchaus unkalkulierbar ist.

Nein, meine Damen und Herren, ich teile weder den Optimismus von Herrn Weichert, noch das Vertrauen in das Bundesverfassungsgericht, wie es sich in den Äußerungen von Herrn Dix manifestiert. Ich glaube vielmehr, dass das Datenschutzrecht einem Zersetzungsprozess ausgesetzt ist, das primär vom Gesetzgeber selber initiiert wird. Aber es ist eben der Gesetzgeber nicht allein. Teilweise zumindest wird der Zersetzungsprozess durch die Aufsichtsbehörden selber mit befördert. Zugleich schwindet die datenschutzrechtliche Sensibilität in der Bevölkerung. 30 Millionen Pay Back Karten sprechen eine deutliche Sprache

IV. Zu den Aufsichtsbehörden

Wieso tragen die Aufsichtsbehörden einen Teil der Verantwortung? Ich könnte Sie relativ lange mit Erfahrungen unterhalten, die ich persönlich mit Aufsichtsbehörden gesammelt habe. Die Qualität und die Bereitschaft, sich für Belange Betroffener einzusetzen, ist doch von Aufsichtsbehörde zu Aufsichtsbehörde sehr unterschiedlich. Teilweise habe ich den Eindruck, dass man als Petent oder Hinweisgeber nur als lästig empfunden wird. Nur ein Beispiel: Ein Unternehmen, für das ich betrieblicher Datenschutzbeauftragter war, musste mit einem Dienstleister das Auftragsverhältnis beenden, weil der Dienstleister unter anderem Zahlungsverpflichtungen nicht nachgekommen war. Vertraglich war vereinbart, dass der Dienstleister alle ihm übergebenen personenbezogene Daten im Falle derVertragsbeendigung, gleich aus welchem Grunde, an das Unternehmen herausgeben musste. Die Herausgabe der Daten hat der Dienstleister verweigert. Zugleich wusste ich, dass der Dienstleister auch Sozialdaten für Krankenkassen verarbeitet. Da dem Dienstleister offenbar die Insolvenz drohte, bestand die reale Gefahr, dass er die Daten Dritter, die er im Auftrag verarbeiten sollte, veräußern würde. Über diese Vermutung und die Tatsache der Verweigerung der Herausgabe von Daten habe ich die zuständige Aufsichtsbehörde informiert und angeregt, man möge doch insbesondere vor dem Hintergrund der Sozialdaten eine Anlassprüfung bei dem Unternehmen durchführen. Die Antwort der Datenschutzaufsicht sbehörde lautete: „Wir bestätigen den Eingang Ihres Schreibens vom … . Wir weisen Sie darauf hin, dass es nicht Aufgabe unserer Behörde ist, Ihnen bei der Durchsetzung Ihrer zivilrechtlichen Ansprüche behilflich zu sein. Mit freundlichen Grüßen“ Nicht einmal richtig gelesen wurde mein Hinweis.

In einem anderen Fall ging es um § 18 KWG, dem mit Billigung des BAFIN weit geöffneten Einfallstors der Banken zur Ausforschung ihrer Kunden. Von der Aufsichtsbehörde bekam ich relativ schnell einen Zwischenbescheid. Man nehme die Angelegenheit ernst und sei mit der Bankenaufsicht zur Klärung des Sachverhaltes in weiteren Gesprächen. Das Schreiben endete mit dem Satz: „Nach Eingang des Ergebnisses werde ich Sie über den Fortgang der Angelegenheit unterrichten.“ Das war im Jahre 2001. Seitdem habe ich nichts mehr gehört.

Ich gebe zu, beide Anfragen waren komplexer als eine Anfrage wegen möglicherweise unrechtmäßiger Nutzung von Adressdaten für Werbezwecke. Es mag auch sein, dass es sich dabei um Einzelfälle handelt und die Praxis vieler Aufsichtsbehörden im Umgang mit Datenschutzanfragen anders ist. Man sollte sich also davor hüten, Einzelfälle zu verallgemeinern. Was

9 Zitate stammen aus dem Internet, HTTPS: //www.Datenschutzzentrum.de /Vortraege20070922-weichert

10 Dix in: Die Gedanken sind frei, 2007, S. 28 ff.

11 Dix, a.a.O., S. 31

12 Dix, a.a.O., S. 32

13 Dix, a.a.O.

14 Vgl. dazu: Ladeur, Kritik der Abwägung in der Grundrechtsdogmatik, Tübingen 2004

mich allerdings wirklich irritiert: Es besteht bei allen die am Datenschutz interessiert sind, ein Konsens. Das Datenschutzrecht muss modernisiert werden. Diese Forderung wird regelmäßig auch in den Datenschutzberichten der Aufsichtsbehörden gefordert. So zuletzt auch durchaus leidenschaftlich im Tätigkeitsbericht 2005/2006 des Bundesbeauftragten für Datenschutz und Informationsfreiheit (BfDI).[15]

Schon Hoffmann-Riem in dem eingangs zitierten Aufsatz plädiert für eine umfassende Novellierung des Datenschutzes hin zu einem Infrastrukturschutz, den er als Systemschutz versteht.[16] So unterschiedlich die dogmatischen Ansatzpunkte verschiedener Autoren sind, in der Notwendigkeit einer Fortentwicklung des Datenschutzes in diese Richtung hin sind sich alle einig, ganz gleich ob sie stärker aus der grundrechtsorientierten Fraktion kommen, ich nenne beispielhaft Spyros Simitis und natürlich Roßnagel mit seinen beiden großen Gutachten aus dem Jahr 2001 und 2006, oder ob sie einer grundrechtlichen Verortung des Datenschutzes eher skeptisch gegenüber stehen, beispielsweise Bull oder Ladeur,[17] einig sind sie sich darin, dass der Datenschutz in die Systeme hinein verlagert werden muss. Das was jetzt allerdings der Gesetzgeber vorgelegt hat, ist die Absage an eine grundsätzliche Reform des Datenschutzrechts. § 28 BDSG wird geöffnet und um mehrere Tatbestände erweitert. Warum? Weil die Auslegungs- und Wertungsspielräume des § 28 BDSG in der Praxis zu divergierenden Rechtsauffassungen der Dat enschutzaufsichtsbehörden der Länder hinsichtlich der Zulässigkeitsvoraussetz ung für bestimmte Datenverwendungen geführt hat. So die Begründung. Nunmehr soll durch die Einführung spezieller Erlaubnistatbestände mehr Rechtssicherheit sowohl für die Betroffenen als auch für die Wirtschaft geschaffen werden. Vielen Dank!

Zunächst erlauben Sie mir den Hinweis: Wieso ist der Bundesgesetzgeber gewissermaßen Schiedsrichter, weil sich 16 Aufsichtsbehörden nicht zu einer einheitlichen Rechtsauffassung durchringen können? Den Aufsichtsbehörden fehlt etwas: Zu selten stehen sie in der Pflicht, bestimmte Aufsichtsmaßnahmen gerichtlich verantworten zu müssen. Worin liegt denn die Dignität beispielsweise des Bundeskartellamtes? Diese Dignität liegt gerade darin, dass beispielsweise eine Untersagungsverfügung des Bundeskartellamtes regelmäßig richterlicher Überprüfung unterliegt und das Kartellamt auch oft genug in entsprechende Gerichtsverfahren hineingezogen wird.

Es gibt Rechtsauffassungen einzelner Aufsichtsbehörden, beispielsweise zur Auftragsdatenverarbeitung, die vielleicht eine Stütze finden können in Aufsätzen der Mitarbeiter dieser Aufsichtsbehörde, keinesfalls aber im Gesetz. Ich finde es von der Rechtskultur her problematisch, wenn man nicht auch lernt, streitig miteinander umzugehen. Natürlich suche auch ich das Gespräch mit den Aufsichtsbehörden. Und nicht nur das Gespräch, sondern nach Möglichkeit auch ein Übereinkommen. Das darf aber zu keinem faulen Kompromiss führen. Wenn ich als Datenschutzbeauftragter oder als hinzugezogener Rechtsanwalt eine Verarbeitung datenschutzrechtlich für zulässig halte, die Aufsichtsbehörde aber eine vergleichbare Verarbeitung für nicht zulässig hält, und es nicht gelingt, die Aufsichtsbehörde zu überzeugen, dann soll so etwas auch streitig ausgetragen werden. Dass es aber tatsächlich zu streitigen Auseinandersetzungen kommt, darüber höre ich sehr wenig. Ein eigentümlicher Schonraum wird da kreiert. Umso unverständlicher ist es mir dann, dass einzelne Aufsichtsbehörden lustvoll auf die Privatwirtschaft einschlagen. Wenn sie konkrete Hinweise auf Datenschutzverletzungen haben, dann sollen sie gefälligst für Abhilfe sorgen im Zweifel eben streitig.

Wozu aber führt jetzt die Uneinigkeit in den Rechtsauffassungen der einzelnen Aufsichtsbehörden? Sie führt, wenn das Gesetz wird, was jetzt auf dem Tisch liegt, zur Zersetzung und Dekonstruktion des Datenschutzes. Die geplante Novelle des § 28 BDSG ist die Preisgabe des Anspruchs des Gesetzgebers, abstrakt allgemeine Regelungen zu etablieren. Ich zitiere beispielhaft aus dem Vorschlag für den neuen § 28 Abs. 3a BDSG:

„Die Übermittlung oder Nutzung von Angaben über eine untitulierte vom Betroffenen nicht bestrittene Forderung ist zulässig, soweit es

1. zur Wahrung berechtigter Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist,

2. dem Betroffenen vier Mahnungen nachweisbar zugestellt wurden,

3. die erste Mahnung nach dem Eintritt der Fälligkeit der Forderung und

4. die vierte Mahnung frühestens sechs Wochen nach Zugang der ersten Mahnung zugestellt wurde und

5. der Betroffene rechtzeitig vor der Übermittlung oder Nutzung der Angaben, jedoch nach der ersten Mahnung von der bevorstehenden Übermittlung oder Nutzung unterrichtet wurde.

Soweit die Forderung von Betroffenen bestritten wird, ist die Übermittlung oder Nutzung nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass das Bestreiten offensichtlich rechtsmissbräuchlich ist.“

Was ist das für ein Gesetzgeber? Wie verhält sich diese Regelung beispielsweise mit § 286 BGB? § 286 BGB wurde gerade novelliert, um Unternehmen, auch kleinen Unternehmen, Handwerksbetrieben und ähnlichem mehr, die Beitreibung ihrer Forderungen zu erleichtern. Und jetzt diese Regelung? Kommt das raus, wenn 16 Aufsichtsbehörden sich nicht einigen können? Heißt diese Regelung beispielsweise, dass z. B. die Einleitung des gerichtlichen Mahnverfahrens, zu deren Zweck ja notwendigerweise Daten

15 Siehe 21. Tätigkeitsbericht 2005 /2006, S 16

16 Hoffmann-Riem, a.a.O., S. 534 ff.

17 Vgl. beispielhaft: Ladeur, Datenschutz – Vom Abwehrrecht zur planerischen Optimierung von Wissensnetzwerken in: DUD 2000, S. 24 ff. und Bull, Datenschutz als Datenaskese?, NJW 2006, S. 1617 ff.

eines Schuldners übermittelt werden müssen, erst nach der vierten Mahnung zulässig ist? Hat der Gesetzgeber eigentlich bedacht, dass ein Unternehmen natürlich berechtigt ist, seine vorgerichtlichen Kosten im Falle des Verzugs des Schuldners ebenfalls geltend zu machen. Und das natürlich die Kosten für vier Mahnungen, die mit Einschreiben/Rückschein verschickt werden müssen, deutlich höher sind als die Kosten vielleicht nur einer Mahnung.

Das Ärgerliche ist eben, dass der Anspruch auf abstrakt generelle Formulierungen im Gesetz preisgegeben wird. Dies sind Sandkastenspiele, die den Datenschutz in keiner Weise voran bringen, aber, ich muss es so sagen, Scheinaktivitäten der Aufsichtsbehörden vortäuschen und dem Gesetzgeber zugleich das gute Gefühl gibt, den Aufsichtsbehörden Brocken hinzuwerfen, ohne eine tatsächliche Strukturreform des Datenschutzes in Angriff zu nehmen.

Dass sich datenschutzrechtliche Belange mit so einer oder einer ähnlichen Regelung bei der Privatwirtschaft lächerlich machen, muss ich nicht betonen. Im Jahr 2006 haben über 7 Mio. Versandhandelskunden ihre Ware nicht fristgerecht gezahlt. Bin ich froh, dass ich nicht Datenschutzbeauftragter eines Versandhandelsunternehmens bin. Eine solche gesetzliche Regelung dem Debitorenmanagement zu verkaufen dürfte äußerst schwer fallen.

Dies ist Alibi-Gesetzgebung, die eher der Abschaffung des Datenschutzes als seiner Stärkung dient. Diese Form der Gesetzgebung ist auch nicht geeignet, ein höheres Maß an Datenschutzsensibilität in der Bevölkerung zu evozieren.

Was wirklich Not tut, sind ganz andere Regelungen. Wenn Sie als Datenschutzbeauftragter eines Unternehmens, das mit komplexen Systemen arbeitet, einigermaßen verantwortungsvoll tätig sein wollen, dann brauchen Sie zwingend Werkzeuge, die es Ihnen erlauben, die immer komplexeren Anwendungsprogramme daraufhin zu überprüfen, wo überall personenbezogene Daten gespeichert sind. Nehmen wir eine so einfache Software wie People Soft.

Ein Standardmodul für CRM-Systeme. Diese Software enthält 21.003 Tabellen mit über 37.000 jeweils wechselnden Feldinhalten. Ich könnte an dieser Stelle auch SAP nennen. Ohne technische Hilfsmittel ist es völlig ausgeschlossen, Programme derartiger Komplexität daraufhin zu überprüfen, ob beispielsweise einmal festgelegte Löschroutinen in allen Tabellen in denen personenbezogene Daten verarbeitet werden, greifen oder ob einmal festgelegte Anonymisierungsparameter in allen Tabellen greifen. Mit anderen Worten: Eine gesetzliche Regelung, die die Hersteller von komplexer Anwendungssoftware verpflichten, Tools zur Überprüfung datenschutzrechtlicher Vorgaben mitzuliefern, würde dem Datenschutz weitaus mehr helfen als derart konkrete Regelungen wie ich sie gerade, bezogen auf § 28 BDSG, vorgestellt habe. Insofern bin ich schon gespannt, welche Möglichkeiten uns Kollege Schwab gleich aufzeigen wird.

V. Überholte Frontstellungen

Und noch etwas lassen Sie mich zum Schluss sagen: Die auch in der Novelle zum § 28 BDSG wieder einmal deutlich werdende Frontstellung von öffentlichen und privaten Datenvermachtungen ist letztendlich überholt. Die Herausforderungen denen sich der Datenschutz zu stellen hat, sind in absehbarer Zeit ganz andere. Ein Menetekel, das auf die neuen Herausforderungen hinweist, sehen wir bereits an der Wand. Es wird aber, wie es Feuerschriften so an sich haben, nicht nur in Babylon übersehen, sondern auch bei uns. Datenschutzrechtsverstöße die auch unmittelbar negative Auswirkungen auf einzelne haben oder hatten, wurden bisher im Schema privater und öffentlicher Vermachtung wahrgenommen. Die Gefahren der einzelnen Bürger über große Datensammlungen der Privatwirtschaft werden an die Wand gemalt. Die Gefahren eines heraufdämmernden Überwachungsstaates werden beschworen. Aber, meine Damen und Herren, eine dritte Gefährdergruppe taucht am Horizont auf. Die Gefährdergruppe ist jedermann. Die Vorboten sehen wir im Internet dadurch, dass beispielsweise über Lehrer verunglimpfende Äußerungen publiziert werden. Die Bildzeitung kreiert den Jedermann-Reporter.

Ich kann mich noch lebhaft an das Jahr 1991 erinnern, als auf dem Arbeitskreis Presserecht und Pressefreiheit wir leidenschaftlich um die Frage des Presseprivilegs im Datenschutz gestritten haben. Simitis wollte es damals schon eingeengt bzw. aufgehoben wissen. Die Frage des Presseprivilegs stellt sich heute völlig neu. Die Bildzeitung bereitet ein großes Internetportal vor, in dem alle Leser aufgefordert werden, zu schreiben und/oder Bilder zu veröffentlichen. Wir werden ein Heer rasender Reporter. Das Multifunktionshandy macht nicht nur Fotos, sondern lässt auch mittlerweile leistungsstarke Videosequenzen zu. Man freut sich über den gelungenen Schnappschuss eines Prominenten im Urlaub oder über das gerade im Video festgehaltene Missgeschick des Nachbarn. Oder man dreht eben mal schnell sein eigenes Gewaltvideo um es auf You Tube ins Internet zu stellen. Und wenn es dann noch auf unterschiedlichen Plattformen Geld für derartige Aufnahmen gibt, deren Veröffentlichung ohne Genehmigung des Abgelichteten ja immer auch eine Persönlichkeitsrechtsverletzung darstellen, die viel unmittelbarer wirken kann als eine Schufa-Mitteilung, dann müssen wir plötzlich erschreckt zur Kenntnis nehmen, dass es praktisch kein entwickeltes Datenschutzbewusstsein in der Bevölkerung gibt. Anders beispielsweise als im Verkehrsrecht, wo man von klein auf lernt, rechts zu fahren, fehlt bei Bloggern und Jedermann-Redakteuren jedes Unrechtsbewusstsein. Man denkt sich nichts dabei. Man realisiert auch gar nicht, dass man personenbezogene

Daten eines Dritten übermittelt und dass es dafür möglicherweise keine Rechtsgrundlage gibt. Was ist denn letztlich schon an dem Foto dabei? Gegenwärtig schwappt durch das Internet die Welle von Lehrerbeurteilungen. Der Versuch einzelner Lehrer, sich gegen die Veröffentlichung einer Benotung zu wehren ist gescheitert. So gab das LG Köln dem Antrag auf Erlass einer einstweiligen Verfügung einer Lehrerin nicht statt. (Vgl. LG Köln Az.: 28 O 333/07).“ Die Pädagogin wollte verhindern, im Internet von ihren Schülern bewertet zu werden - unter anderem in Kategorien wie „sexy“, „cool“, „witzig“, heißt es in Spiegel online.

Die Richter sahen die Benotung von Lehrern vom Grundrecht auf Meinungsäußerung gedeckt. Bei den Benotungen handele es sich „nicht um Tatsachenbehauptungen, sondern um Werturteile“. Und die seien zulässig, solange die Grenze zur Schmähkritik nicht überschritten werde. Ob andere die Kritik für falsch oder ungerecht hielten, sei nicht von Bedeutung.

Die bruchlose Übertragung der aus dem Presserecht entwickelten Grundsätze der Schmähkritik sind mehr als problematisch. Die Presse berichtet in aller Regel über Personen, die sich bewusst in der Öffentlichkeit bewegen, die vielfach auch die Öffentlichkeit suchen. Das ist aber bei den Lehrern, die von den Schülern im Internet beurteilt werden, gerade anders. Hinzu kommt, dass einmal ins Internet gestellte Informationen faktisch nicht rückholbar sind. Es gibt keinerlei verobjektivierte Maßstäbe zur Lehrerbeurteilung, so wichtig und geboten die Überprüfung von Lehrerleistungen sicherlich auch ist. Natürlich sind die Lehrerbeurteilungen erst ein aller erster Schritt in die Richtung einer die Privatheit negierenden Medienzukunft. Hier aber stellen sich zwingend die Zukunftsaufgaben des Datenschutzes. Ein in die Zukunft weisender Datenschutz muss sich dieser Probleme bewusst werden. Es ist schlechthin eine Erziehungsaufgabe. Wenn diese Erziehungsaufgabe erfolgreich ist, dann mag sich vielleicht die von Weichert beschworene Datenschutzsensibilität einstellen. Aber nur dann. Mein Optimismus hält sich diesbezüglich sehr in Grenzen.

DVD Deutsche Vereinigung für Datenschutz e. V.

Bonner Talweg 33-35
53113 Bonn

Telefon: 0228/22 24 98
Telefax: 0228/24 38 470

dvd@datenschutzverein.de
www.datenschutzverein.de

Presseerklärung
Bonn, 19.3.2008

Bundesverfassungsgericht entschärft Vorratsdatenspeicherung

Das Bundesverfassungsgericht hat heute, am 19. März 2008, per einstweiliger Anordnung das Gesetz zur Vorratsdatenspeicherung teilweise gestoppt. Die Deutsche Vereinigung für Datenschutz (DVD) erklärt dazu:

Mit der einstweiligen Anordnung hat das Verfassungsgericht den datenhungrigen Staat erneut in seine Schranken verwiesen. Zwar dürfen die Telekommunikationsdaten zunächst weiter gespeichert werden. Die Weitergabe der gespeicherten Daten an staatliche Stellen ist jedoch ab sofort nur noch bei besonders schweren Straftaten möglich.

Die allgemeine Überwachung des Telekommunikationsverhaltens von 82 Millionen Menschen in Deutschland ist damit zunächst eingeschränkt worden. Die Deutsche Vereinigung für Datenschutz begrüßt diese Entscheidung aus Karlsruhe. Die acht Richter haben klar zu erkennen gegeben, dass sie die Sorgen der mehr als 30.000 Beschwerdeführer als berechtigt ansehen. „Gesetze werden nur in ganz seltenen Ausnahmefällen vom Bundesverfassungsgericht vorläufig außer Kraft gesetzt“, erläutert Sören Jungjohann, Mitglied im Vorstand der DVD. „Dies gilt insbesondere dann, wenn es wie hier mittelbar auch um eine Richtlinie der Europäischen Union geht. Vor diesem Hintergrund ist bereits die teilweise Suspendierung der Vorratsdatenspeicherung ein beachtlicher Erfolg für die Bürgerrechte.“

Darüber hinaus hat das Bundesverfassungsgericht mit seiner Entscheidung aber auch die Weichen für das endgültige Urteil über die Vorratsdatenspeicherung gestellt. Die DVD geht davon aus, dass das Gesetz über die Vorratsdatenspeicherung schon bald als verfassungswidrig aufgehoben werden wird. Denn schon einmal, im Jahr 1983, hat das Bundesverfassungsgericht ein verfassungswidriges Gesetz zunächst durch einstweilige Anordnung aufgehalten und einige Monate später für nichtig erklärt. Die damalige Entscheidung ging als „Volkszählungsurteil“ in die Geschichte der Grundrechte ein. Das für 2008 erwartete „Vorratsdatenurteil“ könnte ein vergleichbarer Meilenstein des Datenschutzes werden.

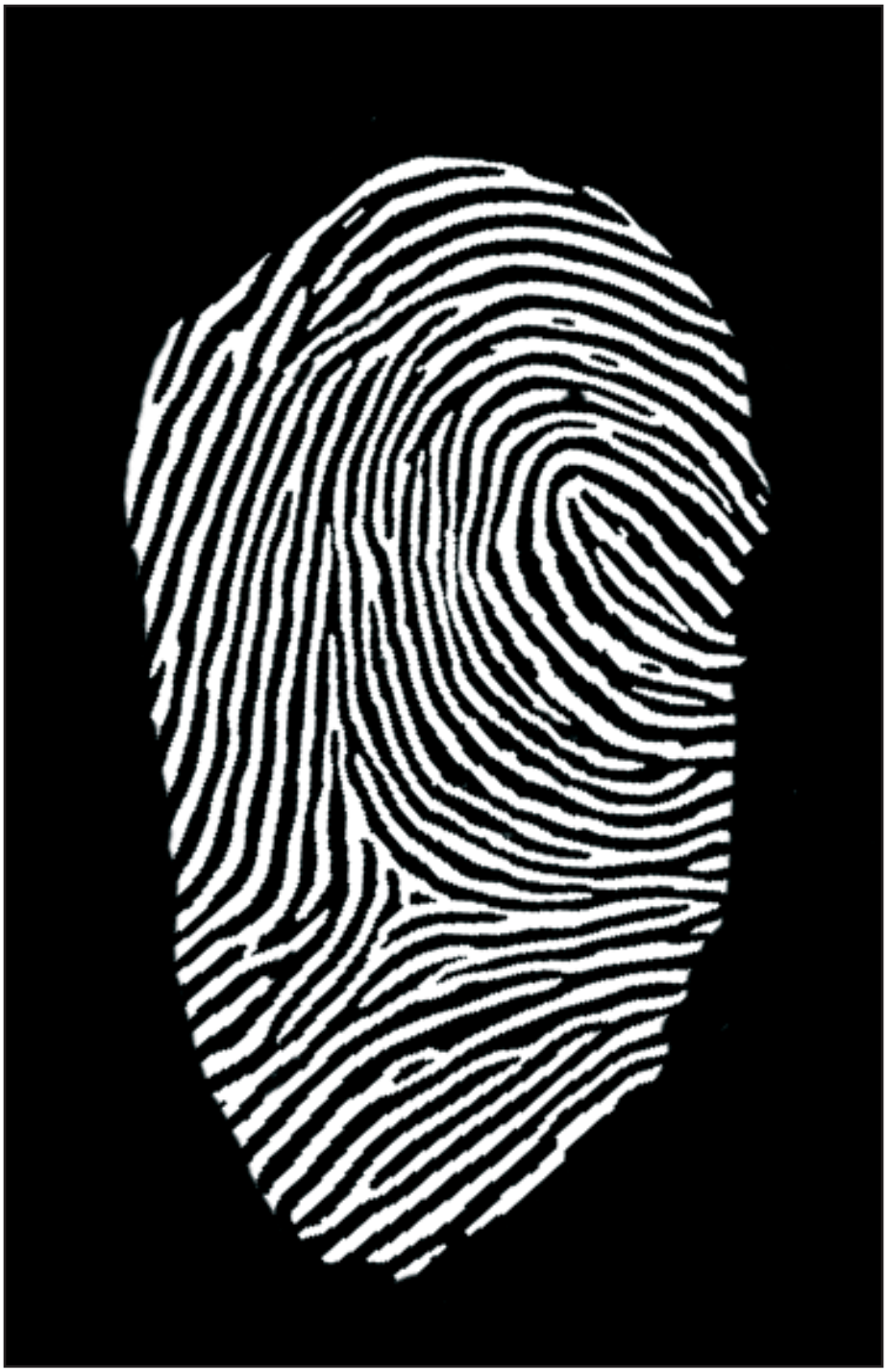
Hintergrund:
Die Verfassungsbeschwerden richten sich gegen das „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“, das am 1. Januar 2008 in Kraft trat. Das Gesetz verpflichtet Telekommunikations- und Internetprovider, die Telefon-, E-Mail- und Internetdaten aller Menschen in Deutschland für sechs Monate zu speichern. Zugriff auf diese Daten haben diverse Sicherheitsbehörden.

Die Deutsche Vereinigung für Datenschutz (DVD) nimmt seit mehr als dreißig Jahren die Interessen der verdateten Bürger und Bürgerinnen wahr. Sie sieht die Vorratsdatenspeicherung als einen weiteren Schritt auf dem Weg zum Präventionsstaat, den es zu verhindern gilt.

Weitere Auskünfte erteilen:
Sören Jungjohann
Mitglied im Vorstand der Deutschen Vereinigung für Datenschutz
Telefon: (01 51) 12 52 94 71

Geschäftsstelle
Telefon: (02 28) 22 24 98

Von wem ist dieser Fingerabdruck?



Auflösung:

www.ccc.de

Bielefelder Erklärung wider Überwachungs- und Datensammelwahn

Am 12. und 13. Oktober 2007 wurde Bielefeld zur deutschen Hauptstadt des Datenschutzes. Die Deutsche Vereinigung für Datenschutz (DVD) veranstaltete anlässlich ihres 30-jährigen Bestehens den Datenschutztag 2007. Am Abend desselben Tages verlieh der Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs (FoeBuD) die BigBrotherAwards 2007, die Oskars für Datenkraken. Tags darauf veranstaltete schließlich das Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) seine Jahrestagung unter dem Motto „Datensammelwut“. Die drei Nichtregierungsorganisationen geben aus diesem Anlass die folgende gemeinsame öffentliche Erklärung gegen den Datensammelwahn und die immer stärkeren Überwachungstendenzen von Staat und Wirtschaft heraus.

Beim Telefonieren und beim Verschicken von SMS und E-Mail, mit jeder Überweisung und mit jedem Gebrauch von Kreditkarten, EC-Karten und Kundenkarten aller Art sowie durch Ausfüllen von ungezählten Online-Formularen hinterlassen die Menschen in Deutschland breite Datenspuren. Viele dieser Datenspuren lassen sich nicht mehr vermeiden, wenn man am politischen, wirtschaftlichen und sozialen Leben teilnehmen will. Das weckt Begehrlichkeiten: Staat und Wirtschaft gehen immer ungenierter mit diesen Daten um, erstellen Kunden-, Bewegungs- und Persönlichkeitsprofile, überwachen, kontrollieren, spähen aus und manipulieren. Die Privatsphäre und das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Persönlichkeitsrechts werden zunehmend eingeschränkt und missachtet.

In der Europäischen Union werden schon heute in vielen Ländern (und bald flächendeckend) die durch Telekommunikation entstehenden Verkehrsdaten mindestens sechs Monate gespeichert. Dies stellt Hunderte von Millionen Menschen unter den Generalverdacht, Telekommunikationseinrichtungen für kriminelle Zwecke zu nutzen.

Die US-amerikanischen Einwanderungsbehörden verlangen umfangreiche Datensammlungen über alle europäischen Fluggäste, bevor sie in den USA landen dürfen. Viele staatliche Einrichtungen in Deutschland, allen voran der Innenminister, tun es ihnen gleich und wünschen sich zweckverändernde Zugriffe z. B. auf Fluggastdaten, Autobahnmautdaten und private Videoaufzeichnungen. Sie gieren nach Überwachungskameras und heimlichen Online-Durchsuchungen, sie vermessen und katalogisieren uns mithilfe biometrischer Daten wie Fingerabdrücken, Gesichtsmerkmalen und DNS-Profil. Da erscheint es zur Erschließung der umfangreichen Datenbanken nur folgerichtig, dass uns eine Personenkennziffer verordnet wird, die uns von der Geburt bis zum Tod eindeutig identifiziert. Unter dem Vorwand, terroristische Gefahren abzuwehren, werden von staatlicher Seite immer neue Ideen zu Datensammlungen entwickelt und dabei die Einschränkung der Grundrechte systematisch und absichtsvoll betrieben. Ob solche Maßnahmen zu mehr Sicherheit führen, ist völlig ungewiss; dass sie die Freiheit beeinträchtigen, ist dagegen offensichtlich.

Die DVD, das FIfF und der FoeBuD fordern alle politisch Verantwortlichen auf, sich für die Erhaltung der Grundrechte einzusetzen, statt ständig zu versuchen, mithilfe angstschürender Schreckensszenarien den schleichenden Abbau wesentlicher demokratischer Errungenschaften zu rechtfertigen.