LIFIS ONLINE [29.06.10]
www.leibniz-institut.de
ISSN 1864-6972

Falk Peters[1]

Verfassungsgerechter Datenschutz in der digitalen Gesellschaft[2]

Vorbemerkung

Die Dinge drängen einer Entscheidung zu. Immer häufiger wird die Frage nach dem ‚Ich' in der digitalen Welt [3], nach den faktischen Möglichkeiten grundrechtlich garantierter Selbstbestimmung des Menschen in der computergesteuerten Gesellschaft [4], mithin nach der Beherrschbarkeit von Technik durch das Recht [5] zwecks Wahrung der Grundrechte gestellt. Zentraler Begriff ist der Datenschutz, der aus rechtlicher Sicht ein intrinsisches Problem der Dynamik der informationstechnischen Entwicklung ist, diese repräsentiert durch den Computer als des finalen Inbegriffs einer rationalen Welt. Aktuell erhält diese Dynamik einen neuen Schub durch die rasante Entwicklung von Sensoren, d.h. technischer ‚Sinnesorgane', durch die der Computer erst zu einem Automaten im eigentlichen Sinne wird. Schlagworte wie ubiquitäre Elektronik und pervasive Sensorik machen die Runde und signalisieren den Trend hin zum totalen Digitalismus, der ob seiner unverkennbaren gesellschaftlichen Relevanz zwangsläufig auch die Politik auf den Plan ruft.

Nunmehr wird das Problem vom Deutschen Bundestag direkt angegangen, nämlich durch seinen Auftrag an die von ihm eingerichtete Enquete-Kommission „Internet und digitale Gesellschaft", in einer Art Quo-vadis-Mentalität u.a. die Fragen nach

- der Wahrung des Grundrechtsschutzes, insbesondere des Persönlichkeitsrechts;
- der Zukunft des Rechts auf informationelle Selbstbestimmung;
- den rechtlichen und technischen Voraussetzungen für Datenschutz und Datensicherheit;
- den Möglichkeiten und Grenzen der Rechtsdurchsetzung in weltweiten Netzen;
- den soziologischen Auswirkungen der Digitalisierung auf den Einzelnen und die Gesellschaft sowie
- den Möglichkeiten für neue Formen der Teilhabe, der Bürgerbeteiligung und Nutzung neuer Partizipationsformen

zu untersuchen und politische Handlungsempfehlungen dazu zu erarbeiten, die der weiteren Verbesserung der Rahmenbedingungen der Informationsgesellschaft in Deutschland dienen. [6]

1. Gesellschaftspolitische und datenschutzrechtliche Aspekte der informationstechnischen Evolution

Die Quo-vadis-Frage in Zusammenhang mit der informationstechnischen Entwicklung wurde erstmals Mitte der 70er Jahre des vorigen Jahrhunderts gestellt, als sich insbesondere bei mit Computerthemen befassten Juristen, aber auch bei anderen diesbezüglich engagierten Intellektuellen die Befürchtung zu regen begann, durch den Einsatz von Computern könnte die an den verfas-

sungsrechtlich garantierten Grundwerten der individuellen Würde und Freiheit orientierte Gesellschaft künftig zu einem Kollektiv von numerierten Bürgern pervertieren. [7] Als signifikant für die damalige Skepsis soll hier ein Aufsatz des damaligen Rechts- und Rechtsinformatikprofessors Wilhelm Steinmüller mit dem Titel „Quo vadis, Computer?“ in Erinnerung gebracht werden, dessen acht (Hypo-)Thesen wegen ihrer Weitsicht damals und ihrer Aktualität heute im Folgenden zitiert werden. [8]

- *These I*: Datenschutz ist weniger ein Problem einer zu schützenden ‚Privatsphäre‘ (was immer das auch heißen möge), als vielmehr eine Teilfrage aus dem übergreifenden Problem gesellschaftlicher Informationskontrolle angesichts einer im Gefolge der automationsunterstützten Datenverarbeitung (ADV) sich zunehmend verändernden Informationsverteilung in der Gesellschaft.
- *These II*: ADV kann interpretiert werden als eine erstmals gelungene Maschinisierung bestimmter intellektueller Prozesse.
- *These III*: Die sozialen Auswirkungen der ADV entstehen weniger durch die ADV selber (also durch den sogenannten ‚Computer’), als vielmehr durch die mit ihr neu und zusätzlich entstehende Informationsorganisation und durch die sich ihrer bedienenden gesellschaftlichen Kräfte.
- *These IV*: Die Bedeutung bzw. Leistung von Informationssystemen besteht in der Erzeugung und Optimierung dynamischer kybernetischer ‚Modelle’ über gesellschaftliche Objekte zu deren Beherrschung.
- *These V*: Der Auf- und Ausbau von Informationssystemen in Wirtschaft und Staat erzeugt eine globale Verschiebung bisheriger Informationsverteilungen und dadurch mittelbar der Machtstruktur.
- *These VI*: Im wirtschaftlichen Bereich sind allmähliche, aber tiefgreifende und weittragende Gewichtsverlagerungen und Neuentwicklungen im Gefolge der Automation der Information zu erwarten.
- *These VII*: Im staatlichen Bereich einschließlich seiner Wechselwirkung zur übrigen Gesellschaft wird die Tendenz zur Ausweitung des staatlich-exekutiven Sektors bei gleichzeitiger Zurückdrängung partizipatorischer Strukturen und zunehmender ökonomisch-administrativer Verflechtung verstärkt.
- *These VIII*: Gegenläufige Tendenzen sind vorhanden und erweiterungsfähig.

Deutlicher konnte das Misstrauen gegenüber Staat und Wirtschaft, was deren Gebrauch informationeller Macht betrifft, nicht formuliert werden. Bei anderen – ebenfalls als kompetent geltenden – Autoren haben sich die seinerzeit herrschenden Bedenken in teilweise dramatisch, ja nahezu drastisch titulierten Essays wie „Personenkennzeichen –Verwaltungs- vereinfachung oder Jedermann-Steckbrief“, „die stille Gewalt der Computertechnologie“, „Manipulation durch Verhaltensdokumentation“, „Gefährdung der Meinungsfreiheit durch Datenbanken“ und ähnlich lautenden Beiträgen niedergeschlagen, die sich allesamt mit dem „Bürger hinter Datengittern“ und dem Problem seiner Manipulierbarkeit mittels seines Computermodells bzw. mit der Gefahr seiner Objektstellung gleich einer Handelsware befassten. [9]

Erinnern wir uns! Mitte der 1970er Jahre gab es nur Großrechner, deren Hersteller an einer Hand abgezählt werden konnten. Bill Gates hatte gerade seine Firma Microsoft gegründet und war da-

bei, mit dem Betriebssystem MS-DOS den Siegeszug des PC einzuleiten. SAP begann Erfolg zu haben mit einer in COBOL programmierten Unterstützung der betrieblichen Fakturierung. Das Internet war ein nur von amerikanischen Militärs und Wissenschaftlern genutztes Netz, bei dem von einer IT-Infrastruktur etwa gemäß heutigem Verständnis der ICANN (Internet Corporation for Assigned Names and Numbers) keine Rede sein konnte. Ein allgemeines gesellschaftliches Bewußtsein für Datenschutz existierte nicht, einer gar gesetzlichen Regelung des Datenschutzes hatten sich in Europa bis dato lediglich die – ihrer Zeit weit vorauseilenden – Länder Hessen (1970) und Schweden (1972) angenommen.

Umso erstaunlicher erscheint deshalb die Eindringlichkeit, mit der Intellektuelle vor einer demokratisch und rechtsstaatlich bedenklichen Entwicklung der Informationstechnik, repräsentiert durch den Computer, bereits zu einer Zeit gewarnt haben, als diese sich aus heutiger Sicht noch in einem geradezu steinzeitlich anmutenden Zustand befand und die Befürchtung einer massenhaften Überwachung von Bürgern mittels digitaler und Dienste integrierender Telekommunikationsnetze von der IT-Industrie als Horrorvision abgetan wurde. Daß jedoch die damals entworfenen Szenarien sich nicht als Horrorvisionen, sondern sich im Laufe der folgenden Jahrzehnte als real erwiesen haben, davon zeugen verfassungs- widrige Legislative staatlicherseits und Datenskandale in öffentlicher Verwaltung und Wirtschaft mittlerweile unwiderleglich, wie nachstehend an einigen prägnanten Beispielen aufgezeigt wird.

2. Staatliche Vorstöße zur Einschränkung der persönlichen Freiheit und die verfassungsrechtliche Barriere

Von geradezu rechtshistorischer Bedeutung sind diejenigen verfassungsgerichtlichen Entscheidungen, durch die eklatante Vorstöße des Staates, die Privatsphäre seiner Bürger per Gesetz zu kassieren, korrigiert, ja regelrecht gestoppt werden mussten.

2.1 Das Volkszählungsurteil 1983

Angefangen hat alles mit dem Verfahren über die Verfassungsbeschwerden gegen das Gesetz über eine Volks-, Berufs-, Wohnungs- und Arbeitsstättenzählung (Volkszählungsgesetz 1983) vom 25. März 1982 (BGBl. I S. 369). [10] Durch das Volkszählungsurteil wurde die Volkszählung verhindert. Sie hat trotz des großen Zeitablaufs bislang nicht stattgefunden. Mit dieser ‚Jahrhundertentscheidung' erhielt der Datenschutz, verstanden als Grundrecht auf informationelle Selbstbestimmung gemäß Art. 2 Abs.1 GG (Persönliches Freiheitsrecht) i.V.m. Art. 1 Abs. 1 GG (Menschenwürde), Verfassungsrang. Seither müssen alle Gesetze, die eine Beschränkung der informationellen Selbstbestimmung zur Folge haben (können), sich an der Reichweite dieses Grundrechts orientieren.

2.2 Prominente verfassungsrechtswidrige Gesetze der jüngeren Vergangenheit – Beispiele

Beachtlich häufig haben vor allem die sog. Sicherheitsgesetze in den letzten zwei Jahrzehnten wegen befürchteter Freiheitsbedrohung Aufsehen erregt und der bundesverfassungsgerichtlichen Prüfung nicht bzw. nicht in vollem Umfang standgehalten, so z.B.:

- § 31 NWPolG 1990 in der Fassung vom 24. Februar 1990 betr. die Rasterfahndung [11];
- Gesetz zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) und Gesetz zur Verbesserung der Bekämpfung der organisierten Kriminalität vom 04. Mai

1998 (BGBl. I S. 845) betr. die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Großer Lauschangriff) [12];

- Luftsicherheitsgesetz vom 11. Januar 2005 (BGBl. I S. 78) betr. die Ermächtigung der Streitkräfte, ein von Terroristen gekapertes, mit tatunbeteiligten Menschen besetztes Luftfahrzeug, das nunmehr zur Bedrohung von Menschen eingesetzt werden soll, mit Waffengewalt abzuschießen [13];
- HessSOG in der Fassung vom 14. Januar 2005 und SchlHLVwG in der Fassung vom 13. April 2007 betr. die automatisierte Erfassung von Autokennzeichen [14];
- Gesetz zur Änderung des Gesetzes über den Verfassungsschutz in Nordrhein-Westfalen vom 20. Dezember 2006 betr. heimliche Online-Durchsuchungen von Computern [15];
- Gesetz zur Neuregelung der Telekommunikationsüberwachung vom 21. Dezember 2007 betr. die Vorratsdatenspeicherung [16];
- Gesetze zur Änderung des Bayerischen Polizeiaufgabengesetzes (Art. 34 Abs. 2 und 3 BayPAG) und des Bayerischen Verfassungsschutzgesetzes (Art. 6c Abs. 2 BayVSG) vom 8. Juli 2008 betr. die Nutzung der Vorratsdatenspeicherung nach §113a TKG [17].

All diese Gesetze mussten gemäß den jeweiligen bundesverfassungsgerichtlichen Entscheidungen geändert oder gar kassiert werden. Durchaus nachvollziehbar ist daher die Sorge der deutschen Anwaltschaft, der Gesetzgeber habe offenbar gar nicht mehr die Vorstellung, es könne ihm gelingen, Gesetze zu erlassen, die einer verfassungsrechtlichen Prüfung standhalten. [18] Gelindes Entsetzen macht sich gar breit, wenn sie zur Kenntnis nehmen muß, dass „namhafte Vertreter der Ermittlungsbehörden doch allen Ernstes davon ausgehen, dass eine Verfolgung von Straftaten nur noch gegen die und nicht mehr mit der Verfassung möglich ist.“ [19] Kein Wunder also, wenn die Anwaltschaft sich nun fragt, ob die Häufung verfassungsrechtswidriger Gesetzgebung in den letzten Jahren nicht sogar auf ein strukturelles Problem unseres Gesetzgebungsverfahrens zurückzuführen ist. [20] Verstärkt wird diese Sorge noch dadurch, dass der Gesetzgeber in seiner Ratlosigkeit neuerdings offenbar dazu neigt, die Änderung verfassungsgerichtlich gescheiterter Gesetze in der Weise zu bewerkstelligen, dass er ganze Passagen aus der Kritik der jeweiligen Gerichtsentscheidungen wortwörtlich in die Gesetze übernimmt. [21]

Nicht auszudenken, hätte das Bundesverfassungsgericht die vorstehend genannte Gesetzgebung nicht gestoppt. Der personenbezogenen Datenverarbeitungswillkür wären Tür und Tor geöffnet gewesen. Gleichwohl besteht aber auch jetzt kein Grund, sich sicher zu fühlen. Zwar erlangen bundesverfassungsgerichtliche Entscheidungen wie die vorstehend zitierten gemäß § 31 Abs. 2 BVerfGG unmittelbar Gesetzeskraft. Das ist aber nur die verfassungsjuristische Seite. Was de facto mittels gerichtlicher oder administrativer Auslegung aus ihnen gemacht wird, das steht auf einem anderen Blatt. So ist z.B. – das erscheint in Anbetracht der zeitlichen Koinzidenz mit der genannten bundesverfassungsgerichtlichen Rechtsprechung bemerkenswert – im Jahre 2008 die strafgerichtlich bzw. staatsanwaltlich angeordnete Telefonüberwachung gegenüber dem Jahr 2007 bundesweit um 11 % gestiegen, in Bayern um 30 %. [22]

2.3 Eine aktuelle Gesetzesinitiative mit Bedrohungspotential: das Bürgerportal

Nun steht in Deutschland die vielleicht bedeutsamste staatlicherseits verursachte Gefährdung der bürgerlichen Freiheiten bevor: das gesetzliche Vorhaben der Einrichtung von Bürgerportalen, deren Betrieb der Kontrolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI) unter-

liegt, einer Behörde, die ihrerseits der Dienst- und Fachaufsicht des Bundesministers des Innern (BMI) unterstellt ist. [23] Offiziell sind diese Bürgerportale Teil der High-Tech-Strategie der Bundesregierung für ein bürgerfreundliches Deutschland, nämlich einen einheitlichen, staatlich überwachten Kommunikationsraum zu schaffen, dessen Vorteil die hohe Sicherheit ist. Aber wird er – durch die Brille des Datenschutzes besehen – auch vertrauenswürdig sein? Oder ist die gesetzliche Einrichtung von Bürgerportalen so ganz nebenbei ein weiterer staatlicher Vorstoß zur Erlangung möglichst umfassender informationeller Macht über die Bürger, diesmal indes nicht martialisch vorgetragen, sondern versüßt mit der Lockspeise „für ein bürgerfreundliches Deutschland"? Droht das Bürgerportal mithin zum vorläufigen Höhepunkt einer informationstechnischen Entwicklung zu geraten, bei der – in geringer Abwandlung eines in [9] zitierten Autors bzw. Titels – der Bürger auf der Datenbank informationell gleichsam zerlegt und zu beliebigen Zwecken wieder komponiert werden kann?

3. Datenschutzskandale in der Wirtschaft – kleine Lese 2009

Von den allein im Jahre 2009 bekannt gewordenen Datenskandalen haben die im Folgenden genannten besonderes Aufsehen erregt: bei der Handelskette Lidl das Ausforschen von Krankheitsursachen bei krankgeschriebenen Arbeitnehmern [24], bei der Deutschen Bahn die systematische Filterung von emails bei bis zu 80.000 Mitarbeitern zwecks Boykotts eines gewerkschaftlichen Streikaufrufs [25], bei der Deutschen Telekom die jahrelange Bespitzelung von Aufsichtsratsmitgliedern, Journalisten, Mitarbeitern und deren Angehörigen sowie von firmenfremden Personen durch Ausforschen ihrer Bankkonten [26], bei der Innungskrankenkasse Weser-Ems die Weitergabe von Sozialdaten ihrer Versicherten mit den vermarktbaren Vermerken „krebskrank", „keine Zähne" usw. an die Signal Iduna Versicherung [27], bei der Bundesagentur für Arbeit der Einsatz eines Computersystems, über das gut 100.000 Mitarbeiter u.a. Suchtkrankheiten, Verschuldung, Familienprobleme von Hartz IV-Empfängern abrufen konnten [28], bei der Bundesagentur für Arbeit die Zulassung eine Berliner Firma zur Schaltung von mehr als 2.500 unterschiedlichen Stellenangeboten in der Online-Jobbörse der Arbeitsagentur, um die Daten von Bewerbern abgreifen zu können. [29]

Zitat (2009): „Es gibt, und ich habe das in diesem Maße nicht für möglich gehalten, Mängel in der Datenschutzkultur der Unternehmen. Und – das gebe ich zu – die Datenschutzaufsicht ist doch über weite Strecken ein zahnloser oder zumindest ein zahnarmer Tiger." [30]

4. Sicherheit und Vertrauen im Internet – aber gegenüber wem?

Mit der Datenschutzkultur steht es in Deutschland nicht zum Besten, weder im staatlichen noch im nichtstaatlichen Bereich. Das belegen im ersten Fall die bundesverfassungsgerichtlichen Entscheidungen, die den Staat bei dessen Versuchen, die Privatsphäre seiner Bürger durch sog. Sicherheitsgesetze immer weiter zu kappen, allzu oft in die Schranken weisen mussten (siehe 2.), ebenso wie im zweiten Fall die neuerlichen Datenschutzskandale in der Wirtschaft, die gerade auch wegen der sittlichen Verworfenheit ihrer Akteure so großes Aufsehen erregt haben (siehe 3.). Die Normtreue, was das Grundrecht auf informationelle Selbstbestimmung betrifft, ist hier wie da nicht belastbar.

Um aber von vornherein keinerlei Missverständnis hinsichtlich gewisser Bemühungen von Staat und Wirtschaft zur Förderung von Sicherheit und Vertrauen in Informationsnetzen aufkommen zu

lassen, sei Folgendes bemerkt: Die Initiative D21, Europas größte politische Public Private Partnership auf dem Felde der Förderung des gesellschaftlichen Einsatzes der Informationstechnik (IT), hat sich dieses Bestrebens unter dem Slogan „Sicherheit und Vertrauen im Internet“ angenommen. [31] Doch muss folgendes klar sein: Dieses Bemühen betrifft nur das Problem der sog. Computerkriminalität, bezweckt also nur den Schutz der Internetnutzer vor Attacken von außen, also gegenüber Datenkriminellen, durch höchst- mögliche Garantie informationeller Vertraulichkeit, Integrität und Verfügbarkeit im online-Verkehr. Hinsichtlich des Persönlichkeitsschutzes der IT-Nutzer vor unlauterem oder gar gesetzeswidrigem Verhalten der staatlichen bzw. staatlicherseits beauftragten und hoheitlich lizensierten Netzbetreiber oder IT-Dienstleister selbst ist damit noch nichts gesagt, geschweige denn bewirkt.

So sehr also der Slogan „Sicherheit und Vertrauen im Internet“ gerechtfertigt ist, soweit er die Bekämpfung von Computerkriminalität signalisiert, so sehr muß man sich vor seiner suggestiven Kraft hüten, damit sei der Wachsamkeit Genüge getan; denn Wachsamkeit ist gerade auch gegenüber der informationellen Macht von Staat und Wirtschaft jederzeit und überall geboten, wie nicht nur die umfängliche Rechtsprechung betreffend die rechtlichen Grenzen personenbezogener Informationsverarbeitung durch öffentliche und private Stellen deutlich zeigt, sondern auch die Bedenken der Datenschutzbeauftragten belegen. So stellt z.B. der Bundesbeauftragte für den Datenschutz bereits in seinem Bericht betreffend die Jahre 2007 und 2008 – also schon vor Erlass des Bürgerportalgesetzes – die Bürgerportale als elektronischen Königsweg zur Verwaltung aus datenschutzrechtlichen Gründen in Frage. [32] Entwarnung ist also mitnichten in Sicht.

5. Die Folgen rein präskriptiv-normativer Datenschutzregelungen

Bloße präskriptiv-normative Datenschutzkonzepte wurden der heimlich schleichenden und immer stärker werdenden Bedrohung der Privatsphäre als des verfassungsrechtlich geschützten persönlichen Freiheitsraumes durch eine immer perfektere personenbezogene Informationsverarbeitung von Anfang an nicht Herr, wie sich an den im Folgenden beispielhaft aufgeführten ‚Unmöglichkeiten’ zeigt.

5.1 Unmöglichkeit präventiven Datenschutzes

Die von Juristen hier und da immer noch geschürte, alte Vorstellung von der Spezial- bzw. Generalprävention straf- bzw. bußgeldbewehrter Vorschriften ist im Bereich der computergestützten personenbezogenen Informationsverarbeitung vor dem Hintergrund der herrschenden Devise „Kriminell ist, wer sich erwischen lässt“ völlig obsolet; denn kein Betroffener ist wirklich in der Lage, eine ihn treffende Datenschutzrechtsverletzung darzulegen und zu beweisen. Genau das nämlich weiß die datenverarbeitende Stelle durch Organisation zu verhindern. Sollte die Beweisführung aber zufällig doch einmal gelingen, so gibt es im Zeitalter des ubiquitous computing per Internet keine reale Möglichkeit der Naturalrestitution im Falle von Datenschutzrechtsverletzungen. Und eine etwaige Entschädigung in Geld hat allenfalls symbolischen Charakter.

5.2 Unmöglichkeit der Vollstreckung gerichtlicher Datenschutzurteile

Überhaupt zeigt sich in der Internet-Gesellschaft die Ohnmacht der Justiz – an der sie indes unschuldig ist –, dem Informationsrecht allgemein und dem Datenschutzrecht im Besonderen Geltung zu verschaffen. Denn wie z.B. vollstreckt man ein obsiegendes Datenschutzurteil? Doch nur so, dass man der (unterliegenden) datenverarbeitenden Stelle das Urteil zustellt und im Übrigen

darauf hofft, dass sie sich an das Urteil hält. Tut sie dies jedoch nicht, sondern setzt die inkriminierte Datenverarbeitung fort, so wird der Betroffene auch davon höchstens zufällig erfahren und wiederum mangels Darlegungs- und Beweismöglichkeit nichts Wirksames gegen die rechtswidrige Verarbeitung seiner Daten unternehmen können.

5.3 Unmöglichkeit eines compliance managements im Datenschutz

Die Vagheit der natürlichen Sprache und somit der Rechtssprache, die allzu oft unkalkulierbare Auslegungen bei der Rechtsanwendung zulässt, was rechtsstaatlich immer bedenklich ist, ist die Geißel des Rechts hinsichtlich seiner Ordnungsfunktion. Dieser sozusagen genetische Defekt des Rechts hat sich in den letzten Jahrzehnten zu einem besorgnis- erregenden ordnungspolitischen Mißstand ausgewachsen, nämlich seit der Gesetzgeber – in Kapitulation vor der Komplexität insbesondere auch technikbezogener Regelungsmaterien in der modernen Welt – durch übermäßigen Gebrauch von politischer Sprache, unbestimmten Begriffen, Generalklauseln usw. Zuflucht zur sog. symbolischen Gesetzgebung genommen hat, wobei er Gesetzgebung nur noch als politische Zeichensetzung betrachtet.

Der Datenschutz ist ein extremer Fall solch symbolischer Gesetzgebung. Bei ihm ist das Recht nicht mehr als ein Teig, den in journalistischer Manier jeder knetet, wie er die Brote haben will. Seit jeher hat die Datenschutzgesetzgebung die Kritik auf sich gezogen, sie sei schlichtweg zu schwammig, zuletzt noch bei der Öffentlichen Anhörung zum Gesetzentwurf der Bundesregierung zur Regelung des Datenschutzaudits im März 2009. [33] Es liegt auf der Hand, dass bei einer solchen Qualität des Datenschutzrechts eine rationale, d.h. intersubjektiv nachvollziehbare Normbefolgungs- bzw. Normkonkretisierungskontrolle nicht möglich ist; denn wo ein klarer Normbefehl fehlt, kann nicht festgestellt werden, ob er befolgt worden ist oder nicht.

Die seit Langem ausufernde Rechtsprechung zum Datenschutz ist der wohl beste Beleg für die mangelhafte Qualität der Datenschutzgesetzgebung; denn immer wenn Gesetzgebung versagt, müssen die Gerichte versuchen, dieses Versagen auszubügeln, mit der Folge inflationärer und mithin irgendwann inkonsistenter Rechtsprechung.

5.4 Unmöglichkeit der Reduzierung von Übermaßbürokratie im Datenschutz

Nach einer vor wenigen Jahren im BMI von einer großen Unternehmensberatung vorgenommenen Untersuchung der Bürokratiekosten stellte sich heraus, dass die Administration des Datenschutzes die höchsten Bürokratiekosten verursacht. Ein Grund dafür war, dass nahezu jegliche datenschutzrechtliche Maßnahme zunächst personen- und zeitaufwendiger Beratungen, meetings usw. bedarf, eben weil es an einem klaren Normbefehl für den Einzelfall mangelt.

6. Die legislatorische Crux heute und ihre Auswirkungen im Datenschutz

Wie oben unter 5.3 schon angedeutet, wird hierzulande vor allem technikbezogene Gesetzgebung seit Jahrzehnten zunehmend als politische Zeichensetzung verstanden, in der Erwartung, die Gerichte würden die Gesetzesrationalität schon herausfinden. Dieses Verkommen einer traditionell exzellenten deutschen Rechtssetzung, deren Produkte geradezu Exportschlager in vielen anderen Kontinenten der Erde waren, zu rein symbolischer Gesetzgebung mit der Folge der Verschiebung der Rationalitätsverantwortung auf die Einzelfallebene der Gerichte, wird in Justiz und Rechtswissenschaft seit langem ganz allgemein beklagt. Erst kürzlich, nämlich anlässlich des 50.000sten Gerichtsverfahrens in Sachen Hartz IV beim Berliner Sozialgericht im August 2008, hat der Vor-

sitzende des Berliner Anwaltsvereins sich genötigt gesehen festzustellen, heute sei es Aufgabe der Sozialgerichtsbarkeit, als Reparaturbetrieb für die Fehler des Gesetzgebers herzuhalten. [34] Und im Jahr 2007 hat ein Rechtswissenschaftler erstmals alle 698 Gesetze, die die große Koalition in der ersten Hälfte der Legislaturperiode des 16. Deutsche Bundestages (2005-2007) erlassen hat, auf ihre Qualität untersucht. Das Ergebnis: Mehr als dreiviertel der neu erlassenen Gesetze verursachen noch mehr Bürokratiekosten und mehr als die Hälfte aller Gesetze werden nach kurzer Zeit wieder geändert. [35]

In Zusammenhang mit der Verschiebung der Verantwortung für die Gesetzesrationalität auf die Einzelfallebene der Gerichte fällt einem natürlich sofort der Satz ein, mit dem Lenin gerne zitiert wird: „Ich habe nichts gegen Gerichte, solange ich die Personalpolitik mache und die Personalentscheidungen treffe." Was mit diesen Ausführungen gesagt sein soll, ist: Natürlich ist der Richter nicht nur der Mund des Gesetzes. Der Syllogismus, der über Jahrhunderte der Jurisprudenz zum Ansehen einer logischen Wissenschaft verholfen hat, ist längst als Phantasmagorie entlarvt, spätestens durch die mittels beliebiger Umwertung von Begriffen erfolgende Rechtsprechung im Dritten Reich. Gesetze, die seit jeher natürlichsprachlich gefasst sind, sind nun einmal der Auslegung und damit der Irrationalität des persönlichen Vorverständnisses des Auslegenden von der unausweichlich begrifflich gefassten Entscheidungsmaterie ausgeliefert bzw. zugänglich. Gleichwohl darf das im Rechtsstaat nicht dazu führen, daß die exakte (d.h. am Kreis der Normadressaten orientierte und dort intersubjektiv bewährbare) Formulierung eines gesetzlichen Normzwecks auch bei noch so hoher Komplexität des Regelungsgegenstandes gar nicht erst versucht wird, daß statt dessen von vornherein politische Sprache ohne jeglichen terminologischen Fundus benutzt wird und dass dadurch ein Richter bei seiner Entscheidung zu einer objektiv nicht nachvollziehbaren Willkür gezwungen ist, was er selbst natürlich als rechtsstaatswidrig ablehnt und was ihm von den Rechtsunterworfenen auch bei bestem Willen, je nach Betroffenheit, zum Vorwurf gemacht wird. Eine solche Rechtssetzung hat in der Tat nur noch den Zweck der Wahrung rechtsstaatlichen Scheins.

Gerade auch im Datenschutz haben die rechtsnormativen Vorgaben nicht die linguistische Qualität, die erforderlich wäre, um ihre Anwendung kontrollierbar zu machen bzw. sie in IT-gestützte Verfahren, die allein Transparenz und Nachvollziehbarkeit ermöglichen und auf die in der Massengesellschaft ohnehin schon längst nicht mehr verzichtet werden kann, normzweckgerecht und zugleich ökonomisch umzusetzen. Die Folgen dieser mangelhaften Qualität sind – bei den Normadressaten in der öffentlichen Verwaltung ebenso wie in der Wirtschaft – dunkles Orakeln über Normzweck, Interessenlage und Reichweite des Datenschutzes, Sich-Austoben in hermeneutischen Irrationalismen, zahl- und ziellose Methodenstreitereien, endlose Abstimmungs- und Mitzeichnungsrituale zwischen den Einzelfallbeteiligten sowie komplizierte Abstimmungs- und Mitzeichnungsrituale zwischen Datenschutzfachanwendung und IT-Unterstützung. Leider sind all diese negativen Folgen, die schon aus rechtsstaatlichen Gründen hätten beseitigt werden müssen, erst über die Bürokratiekosten ernst genommen worden.

7. Datenschutzrechtliche Informationskontrolle – aber wie?

Liberty dies by inches! Dieser Sterbeprozess ist schon sehr weit fortgeschritten.

7.1 Das Postulat technischen Datenschutzes

Objektiver und höchster Zweck jeglicher Rechtssetzung ist die gesellschaftliche Ordnungsfunktion; denn das gesetzte Recht ist jedenfalls ein Imperativsystem, unabhängig von den gewählten

Rechtsetzungsmethoden und Formulierungen in den einzelnen Gesetzen. [36] Dieses System funktioniert logischerweise nur, wenn der Normbefehl, den jedes Gesetz enthalten muß, rechtssicher ist, wobei Rechtssicherheit als Assoziationssicherheit/Erwartungssicherheit zu verstehen ist, was bedeutet, daß ein jeder Normadressat an den Normbefehl dieselben gedanklichen Assoziationen knüpft wie irgendein anderer Normadressat. In diesem Sinne hat der Bundespräsident in seiner Eröffnungsrede zum 67. Deutsche Juristentag am 23.9.2008 in Erfurt, auf dem es u.a. um die Bewährung der deutschen Rechtsordnung im globalen Wettbewerb der Rechtskulturen ging, thematisiert: Gutes Recht schafft Erwartungssicherheit. [37]

Das o.g. Volkszählungsurteil des Bundesverfassungsgerichts, das den Datenschutzbegriff als Möglichkeit zur informationellen Selbstbestimmung – basierend auf Art. 1 und 2 GG – verfassungsrechtlich höchstrangig etabliert hat, war in der Folgezeit Anknüpfungs- gegenstand für die Überlegungen zu einer verfassungskonformen Informationsordnung, weil das Grundgesetz eben nicht die Freiheit zur Verarbeitung personenbezogener Informationen garantiert, sondern im Gegenteil diesbezügliche Verarbeitungsbarrieren begründet. [38] Und die Anordnung des Bundesverfassungsgerichts, zwecks Garantie des Datenschutzes müssten auch organisatorische und verfahrensrechtliche Vorkehrungen getroffen werden, führte zu ersten Vorschlägen, wie technischer Datenschutz im Rahmen einer verfassungsgerechten Informationsordnung aussehen könnte. [39]

Diese Vorschläge gehen von folgender Prämisse aus: Ein schwerfälliges System aus rechtlichen Wertungen und Begriffen wie der Datenschutz ist mit der Rasanz der informationstechnischen Entwicklung und ihrer beliebigen Nutzung nicht zu synchronisieren. Soll der Datenschutz präventive Wirkungen entfalten, worin im Zeitalter des ‚ubiquitous computing' allein sein Zweck bestehen kann, so darf er nicht der zweifelhaften Normtreue datenverarbeitender Stellen (Normadressaten) anheim gegeben werden bzw. allein überlassen bleiben. Vielmehr müssen bereits Organisation und Funktionsweisen der Datenverarbeitung selbst Ausdruck der formal artikulierten und schließlich programmierten Datenschutzbelange der Betroffenen sein. In der formalen Artikulierung der Datenschutzbelange liegt die Kernaufgabe des technischen Organisationsrechts im Datenschutz. [40]

Daß daraus bisher nichts geworden ist, hat zwar auch politische Gründe, aber nicht nur; denn angenommen, der Gesetzgeber würde eine verfassungsgerechte Informationsordnung einschließlich der oben in *These I* angesprochenen Informationskontrolle wirklich statuieren wollen, so müsste er den Prinzipien der Transparenz und Nachvollziehbarkeit der personenbezogenen Informationsverarbeitung reale Geltung verschaffen. Das aber würde bedeuten, dass er selbst die technische Reglementierung dieser Informationsverarbeitung auf einer abstrakten Ebene eindeutig vorschreiben müsste. Das jedoch ist nur mit den formalwissenschaftlichen Methoden der Rechtsinformatik, auch formale Legistik genannt, zu erreichen, die er aber nicht beherrscht. Leider hat die formale Legistik, deren Zweck in der Erhöhung der Rechtssicherheit (Erwartungssicherheit/Assoziationssicherkeit) und in der Verbesserung der Umsetzung rechtsnormativer Vorgaben in IT-gestützte Verfahren liegt, den deutschen Gesetzgeber noch nicht erreicht.

7.2 Technisches Organisationsrecht im Datenschutz: von der Reaktion zur Prävention

Folgendes ist nach den vorstehend gemachten Ausführungen klar: Das Kernproblem des Datenschutzrechts liegt in seinem mangelhaften natürlichsprachlichen Rechtskode, der selbst für Datenschutzjuristen nur selten eindeutig nachvollziehbar und widerspruchsfrei ausführbar ist. Intransparenz und Mehrdeutigkeit des Datenschutzrechts sind Folgen der Komplexität des Rege-

lungsgegenstandes, bei dem der Gesetzgeber selbst sich von Anfang an nicht darüber klar war, was er eigentlich schützen wollte. Deswegen flüchtete er sich in das oben schon beanstandete symbolische Recht mit seinen vielen unbestimmten Begriffen und Generalklauseln. [41] Gesetzlich klar war eigentlich stets nur eins, nämlich dass personenbezogene Datenverarbeitung nur aufgrund eines Gesetzes oder aufgrund der Einwilligung des Betroffenen zulässig ist. Nachdem das Bundesverfassungsgericht der informationellen Selbstbestimmung, abzusichern durch organisatorische und verfahrensrechtliche Vorkehrungen, den allerhöchsten verfassungsrechtlichen Rang eingeräumt hat [42], stellen sich die Ansatzmöglichkeiten für technisches Organisationsrecht etwa folgendermaßen dar.

7.2.1 Einwilligung des Betroffenen

Wo immer es rechtlich möglich ist, die Einwilligung des Betroffenen als alleinigen oder vorrangigen Zulässigkeitsgrund für die Verarbeitung seiner personenbezogenen Daten gelten zu lassen (und das gilt ganz überwiegend im privatwirtschaftlichen Bereich), ist die informationelle Selbstbestimmung durch eine partizipatorische Informationsorganisation in Form einer gesetzlich und zwar formallegistisch geregelten Public Key Infrastructure (PKI) zu gewährleisten; denn „das Grundrecht auf informationelle Selbstbestimmung verpflichtet den Staat, im Ausgleich mit konkurrierenden Freiheitsrechten ein angemessenes Schutzregime zu schaffen. Dabei wird der Staat häufig eine verbindliche Ordnung konstituieren müssen, um der grundrechtlichen Werteordnung auch im Privatrechtsverkehr Geltung zu verschaffen. Die nun von der Bundesregierung geplante Einführung des Einwilligungsprinzips (sog. Opt-in-Verfahren; der Verf.) für den Datenhandel sowie eines – allerdings freiwilligen – Datenschutzauditverfahrens mit Gütesiegel scheinen daher nahezu geboten zu sein, um dem objektiven Gehalt des Rechts auf informationelle Selbstbestimmung endlich auch im privaten Bereich hinreichend Rechnung zu tragen.“ [43] Damit steht das Opt-in-Verfahren – in Anbetracht der oben unter 2. und 3. geschilderten Situation – dringend zu einer gesetzgeberischen Befassung an. [44]

7.2.2 Informatische Ontologie

Wo das Opt-in-Verfahren rechtlich nicht möglich ist (z.B. bei der personenbezogenen Datenverarbeitung zwecks Strafverfolgung, zwecks Bekämpfung des Terrorismus usw.), da ist – zur Verhinderung beliebiger Auslegbarkeit der Reichweite des Datenschutzes im Einzelfall – sein Normzweck abstrakt unter Verwendung informatischer Ontologien gesetzlich zu fixieren.

7.3 Zur rechtlichen Modellierung des Datenschutzes

Die formallegistische Präzisierung von Rechtstexten erfolgt wissenschaftlich gemäß den folgenden linguistischen Stufungen:

- *Natürlichsprachliche Fassung*. Das ist z.B. ein Gesetzestext.
- *Verbale Spezifikation*. Sie ist die aussagen- und prädikatenlogisch und ggfls. mittels deontischer Logik geprüfte Version des Rechtstextes.
- *Semiformale Spezifikation*. Sie ist die strukturprachliche Fassung des Rechtstextes, entweder in Form einer logikorientierten oder in der Form einer graphikorientierten Strukturprache.
- *Formale Spezifikation*. Sie ist die mathematische bzw. bewiesene mathematische Version des Rechtstextes.

Ein 1969 erstmals formuliertes, rechtssoziologisches Postulat geht dahin, bei jeglicher Rechtsetzung den Anteil des Verfahrensrechts so groß wie möglich und den Anteil des materiellen Rechts so gering wie möglich zu halten. [45] Die Begründung dafür ist, dass das Verfahren ein raumzeitliches Phänomen ist, sich deswegen formal, also eindeutig beschreiben läßt und aufgrund dieser Unauslegbarkeit erwartungssicher ist und das Aufkommen von Komplexität verhindert bzw. reduziert, wohingegen das materielle Recht, das unausweichlich wertausfüllungsbedürftig und folglich meinungsabhängig ist, Komplexität produziert.

Die Ratio dieser Begründung ist zwingend, weil es Wahrheit im naturwissenschaftlichen Sinne im Recht nicht gibt, sondern diese im Recht per Abstimmung ermittelt und aufgrund eines vorgeschriebenen und korrekt eingehaltenen Verfahrens gültig wird. Die Korrektheit des Verfahrens kann nun rational, also intersubjektiv einhellig, überprüft werden, weil der Verfahrensbegriff sich an den Kriterien von ‚richtig' oder ‚falsch' bzw. ‚wahr' oder ‚unwahr', also an binären Kriterien im formalwissenschaftlichen Sinne orientiert. Dieser Ratio folgt z.B. das anglo-amerikanische Recht, bei dem der professionelle Jurist nur auf die korrekte Einhaltung des Verfahrens achtet und die materiellrechtliche Entscheidung einer Jury von Geschworenen (juristischen Laien) überlassen bleibt.

Mithin ist rationaler Grund für die Bevorzugung einer semiformalen Rechtssetzungsmethode bei der gesetzlichen Regelung des Datenschutzes, dass durch sie das Problem der – aufgrund der erwähnten mangelhaften linguistischen Qualität gegebenen – Unzuverlässigkeit rein präskriptivnormativ gehaltener Datenschutzregelungen gemildert oder gar behoben werden kann, weil eine durchgehend strukturierte und IT-gestützte Datenschutzorganisation, die allein Transparenz und Nachvollziehbarkeit verspricht, als endliche Menge semiformal beschriebener Verfahren dargestellt und so a priori datenschutzgerecht im Sinne der vorstehend unter 1. und 2. beschriebenen Forderungen und Grundsätze gestaltet werden kann. Der Einsatz von z.B. grafisch-logischen Modellierungswerkzeugen der Rechtsinformatik zwecks datenschutzgerechter Reglementierung der personenbezogenen Datenverarbeitung würde es – etwa nach dem Vorbild der Geschäftsprozessmodellierung – ermöglichen, den normativ konzipierten Normzweck des Datenschutzes in Form von Aufbau- und Ablauf- strukturen transparent darzustellen bzw. konsistent zu entwickeln, somit unkalkulierbare Auslegungen zu verhindern und eine weit höhere Rechtssicherheit (Erwartungssicherheit/ Assoziationssicherheit) bei der Anwendung des Datenschutzrechts zu garantieren und schließlich bedeutende Vereinfachungen bei jeglicher Rechtsänderung zu erzielen. Doch dafür ist es unumgänglich, zunächst die rechtsinformatischen Anforderungen an die rechtliche Modellierung der Datenschutzrechts unter Bevorzugung des Verfahrensrechts gegenüber dem materiellen Recht zu erarbeiten und darauf basierend rechtsinformatische Ontologien zu entwickeln, aufgrund derer sodann

- die logische Darstellung der einschlägigen *Rechtsnormen* im Einzelnen und insgesamt;
- die Erstellung eines *Rechtsmetamodell*s, in welchem die rechtlichen Entitäten (Rechtsbegriffe, Rechtsnormen, Rechtssubjekte, Rechtsobjekte, Rechtsregeln usw.) hierarchisch geordnet und untereinander vernetzt werden;
- der Aufbau einer *Rechtsdatenbank*, in denen Rechtsinformationen vernetzt werden und Rechtsauswertungen erfolgen können sowie
- die Ableitung allgemeingültiger (d.h. für die Regelung technikbezogener Regelungs-materien allgemein geeigneter) semiformaler Methoden, darzustellen in einem *Handbuch der formallegistischen Rechtsetzung,*

möglich wird.

Literatur

[1] Der Autor ist Rechtsanwalt in Berlin, Lehrbeauftragter für Rechtsinformatik an der Brandenburgischen Technischen Universität Cottbus und Verfasser zahlreicher Veröffentlichungen zum Datenschutz
[2] dargestellt anhand der Situation in Deutschland
[3] www.initiatived21.de/veranstaltungen/veranstaltungsarchiv/digitalewelt
[4] www.datenschutzgeschichte.de/Interviews Simitis und Steinmüller
[5] vgl. aaO, Interview Roßnagel
[6] vgl. BT-Drucksache 17/950 vom 03.03.2010, Rubriken „Recht und Innen“ und „Gesellschaft und Demokratie“
[7] vgl. Hoffmann/Tietze/Podlech (Hrsg.): Numerierte Bürger, Technologie und Gesellschaft, Band 1, Peter Hammer Verlag, Wuppertal 1975
[8] vgl. Steinmüller: Quo vadis, Computer? –Vermutungen über Alternativen künftiger sozioökonomischer Entwicklungen, in: Numerierte Bürger (s.o.), Seite 139ff
[9] vgl. [7]; aus der unüberschaubaren Fülle der damaligen Publikationen seien hier als ebenfalls besonders markant noch genannt: Krauch (Hrsg.): Erfassungsschutz. Der Bürger in der Datenbank: Zwischen Planung und Manipulation, Deutsche Verlags-Anstalt, Stuttgart 1975; Hoffmann: Computer, Macht und Menschenwürde, R. Piper und Co. Verlag, München 1976; ders., Bürger hinter Datengittern, aus Politik und Zeitgeschichte – Beilage zur Wochenzeitung Das Parlament, Bonn 1977 - B 25/77 -, S. 3ff
[10] vgl. dazu 1 BvR 209/83 u.a. – Urteil vom 15. Dezember 1983
[11] vgl. dazu 1 BvR 518/02 – Beschluss vom 04. April 2006
[12] vgl. dazu 1 BvR 2378/98 und 1 BvR 1084/99 – Urteil vom 3. März 2004
[13] vgl. dazu BverfG, NJW 2006, S. 751
[14] vgl. dazu 1 BvR 2074/05 und 1 BvR 1254/07 – Urteil vom 11. März 2008
[15] vgl. dazu 1BvR 370/07 und 1BvR 595/07 – Urteil vom 27. Februar 2008
[16] vgl. dazu 1BvR 256/08, 1BvR 263/08 und 1 BvR 586/08 – Urteil vom 2. März 2010
[17] vgl. dazu 1 BvR 256/08 – Beschluss vom 28. Oktober 2008
[18] vgl. Heussen: Netze ausspannen oder Betonböden gießen?, Berliner Anwaltsblatt 9/2009, S. 297ff, 298
[19] vgl. Berliner Anwaltsblatt 3/2010, S. 49
[20] vgl. Berliner Anwaltsblatt 4/2010, S. 97
[21] als Beispiel vgl. BKA – Gesetz vom 25. Dezember 2008 (BGBl. I, S. 3083) als Konsequenz des bundesverfassungsgerichtlichen Urteils vom 27. Februar 2008, vgl. [15]
[22] vgl. Bundesamt für Justiz v. 23.09.2009
[23] Entwurf eines Gesetzes zur Regelung von Bürgerportalen und zur Änderung weiterer Vorschriften, BT-Drucksache 16/12598 vom 08.04.2009; Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes, BT-Drucksache 16/11967 vom 16.02.2009, hier: Artikel 1: Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)
[24] vgl. Berliner Morgenpost v. 07.04.2009
[25] vgl. DIE WELT v. 31.03.2009
[26] vgl. Berliner Morgenpost v. 18.05.2009
[27] vgl. Berliner Morgenpost v. 15 05.2009
[28] vgl. Spiegel Online v. 30.10.2009
[29] vgl. AFP v. 10.11.2009

[30] so der Bundesbeauftragte für den Datenschutz, vgl. Innenausschuss des 16. Deutschen Bundestages, 88. Sitzung am 23.03.2009, Protokoll Nr. 16/88, S. 17
[31] vgl. E-Government Roadmap. Ein Projekt der Lenkungsgruppe E-Government und Vertrauen im Internet; Hrsg. Initiative D21 e.V., Berlin 2006
[32] vgl. BT-Drucksache 16/12600 v. 21.04.2009, S. 87
[33] so die Repräsentantin der Deutschen Vereinigung für Datenschutz e.V., vgl. Innenausschuss des 16. Deutschen Bundestages, 88. Sitzung am 23.03.2009, Protokoll Nr. 16/88, S. 17
[34] Berliner Anwaltsblatt 10/2008, S. 349
[35] www.insm.de/Umfragen_Studien/INSM-Studie_Gesetzescheck
[36] vgl. Engisch: Einführung in das juristische Denken, Verlag W. Kohlhammer, Stuttgart-Berlin-Köln, 10. Auflage 2005, S. 8ff, 20
[37] vgl. BRAK-Mitteilungen/2008, S. 242f
[38] vgl. Simitis: Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, S. 398ff
[39] vgl. Peters: Technischer Datenschutz, CR 12/1986, S. 790ff; Peters/Kersten: Technisches Organisationsrecht im Datenschutz – Bedarf und Möglichkeiten, CR 9/2001, S. 576ff
[40] vgl. Peters: Arbeitnehmerdatenschutz, Diss. Frankfurt a. M., 1982, S. 249
[41] vgl. www.datenschutzgeschichte.de/interviews Simitis
[42] vgl. [10]
[43] so der Präsident des Bundesverfassungsgerichts, zitiert vom Bundesbeauftragten für den Datenschutz, vgl. Innenausschuss des Deutschen Bundestages, Protokoll 88. Sitzung v. 23.03.2009, S. 17f
[44] so auch das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein, vgl. aaO, S. 30
[45] vgl. Luhmann: Legitimation durch Verfahren, 6. Aufl., Suhrkamp, Frankfurt am Main 2001

[29.06.10]

Anschrift des Autors:

RA Dr. jur. Falk Peters
Artemisstr. 9A
D – 13469 Berlin
ra.dr.falk.peters@t-online.de