Rainer Hamm

Datenschutz in Hessen in den 90er Jahren des 20. Jahrhunderts

Der Nachfolger von Herrn Simitis im Amt des HDSB, Winfried Hassemer, hat mir ausdrücklich erlaubt, das hochsensible personenbezogene (um nicht zu sagen: „schmerzhafte“) Datum bekannt zu geben, dass er an den Folgen eines kleinen Unfalls leidet und deshalb hier nicht selbst über seine Ära berichten kann. Und er hat mir erlaubt, dies, so gut es eben geht, an seiner Stelle zu tun. Nachdem wir inzwischen in einer Weise beruflich verbunden sind, die es immer mal wieder notwendig und möglich macht, dass wir uns gegenseitig vertreten, habe ich die Aufgabe auch gerne übernommen.

Die Zeit von 1991 - 1996, in der Hassemer das Amt innehatte, und der Rest jenes Jahrzehnts, als ich - darin bis dahin völlig ungeübt - auch einmal Behördenleiter spielen durfte, diese Jahre waren insgesamt davon geprägt, dass wir von dem guten Ruf zehren konnten, den die Dienststelle und der Datenschutz in Hessen in den 17 Simitis-Jahren erworben hatte. Hassemer und ich als sein Nachfolger hatten gemeinsam, dass unsere fachlichen Vorverständnisse nicht im öffentlichen Recht, sondern im Strafrecht und dem Strafverfahrensrecht mit den dort geltenden Grundrechtsbezügen wurzelten. Kein Grundrechtseingriff durch Strafverfolgungsbehörden ohne ausdrückliche gesetzliche Ermächtigung. Zweckbindung der Informationserhebung, Verhältnismäßigkeit, ultima ratio - waren uns vertraute Regeln und sie fanden wir nun in leicht gewandelter Form im Datenschutzrecht wieder. Strafrecht und Datenschutz! Hassemer und ich haben gelernt, wie viel die beiden Gebiete gemeinsam haben, aber auch mit welch hoher elektrischer Spannung der Grenzzaun aufgeladen ist, der die beiden Gebiete trennt. Aber davon später mehr.
Am Tage seiner Wahl, nannte Hassemer in der Antrittsrede als Ziel seiner bevorstehenden Amtszeit, dass das Recht auf informationelle Selbstbestimmung mit allem Nachdruck als Grundrecht allgemein verständlich gemacht werden solle. Bürgerinnen und Bürger müssten verstehen, dass es beim Datenschutz um ihre eigenen Interessen geht. Und ganz so, als habe er prophetisch die beinahe 2 Jahrzehnte später aufgekommenen Datenschutzskandale in der Privatwirtschaft vorausgesehen, hat Hassemer auch bereits in seiner Antrittsrede die Bedrohung des Rechts auf informationelle Selbstbestimmung durch eben die Privaten angesprochen. Er sagte wörtlich: *“Man darf … annehmen, dass die normalen alltäglichen Gefährdungen der informationellen Selbstbestimmung eher auf den leisen Sohlen des Privatrechts daherkommen als in den schweren Schuhen des Öffentlichen.“* [1]

Auf den leisen Sohlen des Privatrechts! Privatrecht, Gesellschaftsrecht, Medienrecht. Und heute sprechen wir auch noch von einem Rechtsgebiet, das wir „Compliance“ nennen. Wenn Compliance funktioniert, kann das auch an Datenschutzverstößen liegen. Wenn sie versagt, schiebt man das vielleicht auf die durch Datenschutz bestehenden Erkenntnisschranken für eine effiziente Prävention.

Da gibt es ein Leck in dem zur Geheimhaltung verpflichteten Aufsichtsrat eines börsennotierten großen Telekommunikationskonzern. Und die Sicherheitsabteilung erhält den Auftrag, herauszufinden, wer in strafbarer Weise immer einen bestimmten Journalisten über kurserhebliche Tatsachen vorab informiert. Dann wird ein externes sog. "Dienstleistungsunternehmen" beauftragt, Recherchen anzustellen, und dem fällt möglicherweise (der Prozess darum läuft gerade in Bonn) nichts Besseres ein, als bei seinem Kunden (das T-Unternehmen) illegal die Verbindungsdaten zu erheben, aus denen sich ergeben sollte, welches Aufsichtsrats-Mitglied wann mit welchem Journalisten telefoniert hat. Dies ist nur ein Beispiel dafür, wie wichtig das Datenschutzrecht in der Privatwirtschaft geworden ist. Andere Fälle, in denen um Korruptionsprävention unter Ausrasterung von Arbeitnehmerdaten ging, könnten hinzugefügt werden.

[1] Hassemer, Datenschutz und Datenverarbeitung heute, 1995, S. 54

Dabei müssten wir auch reden über konkurrierende Ermittlungen von Staatsanwaltschaften, parlamentarischen Untersuchungsausschüssen und privaten externen oder internen "forensic services" sowie dem heiklen Thema des Informationstransfers zwischen den verschiedenen Einheiten.
Dass Hassemer auf solche Gefahren schon damals hinwies, war nicht selbstverständlich. War er doch - ebenso wie seine Vorgänger und bis heute alle seine Nachfolger für den Datenschutz bei Privaten gar nicht zuständig, weil in unserem Bundesland eisern daran festgehalten wird, dass die Datenschutzkontrolle für den öffentlichen und den privaten Bereich getrennt organisiert ist. Die Vor- und Nachteile dieser Trennung waren ein Dauerthema in Hassemers und meiner Zeit und auch in den regelmäßigen Konferenzen der Datenschutzbeauftragten des Bundes und der Länder. Hassemer wollte die Trennung überwinden, weil er erkannte, *"dass die Anhäufung von Informationen außerhalb des staatlichen Bereichs für die Interessen der Menschen an Privatheit nicht weniger gefährlich ist als innerhalb".* [2]

Aber er forderte auch massiv eine Veränderung der allgemeinen Bewusstseinslage, die er so kennzeichnete: *"Die private Datenverarbeitung liegt noch immer am Rande unserer Wahrnehmung und die wirtschaftlichen Interessen an ungestörter privater Datenverarbeitung sind durchsetzungsfähig..... Von einem abgestimmten, differenzierten und funktionierenden Datenschutzrecht für Private sind wir noch weit entfernt."*

Vieles sprach und spricht dafür, die Datenschutzkontrolle für den öffentlichen und privaten Bereich in die Hand einer Behörde zu legen. Manche Bundesländer sind diesen Weg auch gegangen und haben damit - wie es heißt - auch gute Erfahrungen gemacht. Auf der anderen Seite hat sich einer solchen Regelung aber auch immer ein Problem in den Weg gestellt, dessen Lösung der Suche nach der Quadratur des Kreises gleicht: Hessen hat mit guten Gründen die Institution des Datenschutzbeauftragten mit völliger Unabhängigkeit ausgestattet. Der Amtsinhaber wird vom Landtag gewählt und ich bin einigermaßen stolz darauf, dass es in meiner Amtszeit gelungen ist, im Rahmen der Umsetzung der Europäischen Datenschutzrichtlinie (wir waren nach ziemlich langer Zeit das erste Bundesland, das dies geschafft hat) ein Datenschutzgesetz verabschieden zu lassen, in dessen § 22 es klipp und klar heißt:

„Der Hessische Datenschutzbeauftragte ist als oberste Landesbehörde in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen."

Oberste Landesbehörde, also keinem Ministerium gegenüber zur Rechenschaft verpflichtet und völlig unabhängig! Davon können die Datenschutzbeauftragten anderer Bundesländer nur träumen. Und das gilt insbesondere für diejenigen, die auch bereits über exekutive Befugnisse gegenüber Privaten verfügen - sei es zur Durchsetzung des Datenschutzes, sei es zur Entscheidung von Streitfragen im Zusammenhang mit dem wachsenden Rechtsgebiet der Informationszugangsrechte. Hier wird man ohne eine Dienstaufsicht zumindest i.S. einer Rechtsaufsicht nicht auskommen. Die Erhaltung der völligen Unabhängigkeit ist der Kreis, die Zuständigkeit für die Privatwirtschaft ist die Quadratur.

Wenn man dann auch noch an die Konstellation denkt (was für mich in meiner merkwürdigen Doppelrolle als praktizierender RA und HDSB natürlich besonders nahe lag), dass eine Datenschutzkontrollbehörde auch noch Einblick in die Akten, Unterlagen und Dateien der von einer spezifischen strafbewehrten Schweigepflicht und Zeugnisverweigerungsrecht getragenen Berufsgruppen erhalten soll, liegt der Konflikt auf der Hand. Ich habe im Rahmen der damaligen Diskussionen manchmal überspitzt formuliert: „Nur über meine Leiche würde ich als Rechtsanwalt einer staatliche Stelle ausgerechnet für die Zwecke des Datenschutzes in meiner Kanzlei Zugang zu den Informationen verschaffen, die meiner Schweigepflicht unterliegen.“

[2] Hassemer, aaO, S. 55

Dafür haben auch manche Datenschützer Verständnis, solange es um die Daten und anvertrauten Informationen des Mandanten geht. Aber wie halten wir es mit den Daten von Dritten und Prozessgegnern? Kürzlich hat das Kammergericht den Konflikt zwischen dem Anwaltsgeheimnis eines Strafverteidigers und dem Einsichts- und Auskunftsanspruch des auch für den nicht-öffentlichen Bereich zuständigen Berliner Datenschutzbeauftragten in der Weise gelöst, dass Anwaltskanzleien zwar nicht wegen der Subsidiaritätsklausel des BDSG mit Blick auf die Regelungen der BRAO völlig der Kontrolle entzogen sind, dass aber der Auskunftsanspruch des DSB noch keine Rechtfertigung dafür bietet, dem RA bußgeldbewehrt einen Bruch seines Anwaltsgeheimnisses abzuverlangen.[3]

Das Beispiel zeigt, wie wichtig es wäre, ein konsistentes und den jeweiligen Datenverarbeitungszusammenhängen gerecht werdendes Datenschutzrecht und eine dazu passende differenzierte Datenschutzkontrolle zu schaffen, bei der weniger die Unterscheidung öffentlich vs. privat als vielmehr die Vertraulichkeitsinteressen der beteiligten Grundrechtsträger maßgeblich dafür sind, dass nicht das Recht auf informationelle Selbstbestimmung ausgerechnet durch die Datenschutzkontrollstelle verletzt wird.

Zurück zur Ära Hassemer: Er übte – ebenso wie ich danach - das Amt in einer Zeit aus, in der das Parlament und die Landesregierung in Hessen sehr viel Verständnis und Engagement für den Datenschutzgedanken aufbrachten, während in der Bundespolitik die Skepsis und die Kritik an dem Beharren auf die Sicherheitsstrategien begrenzende informationelle Selbstbestimmung vorherrschte. Im Spannungsfeld zwischen Sicherheit und Freiheit, zwischen Rechtsstaat und Gefahrenabwehr, zwischen Grundrechtsdenken und Bekämpfungsrhetorik entwickelte Hassemer eine großartige Idee:

Er erfand und begründete das **Wiesbadener Forum Datenschutz**, das wir heute nun schon zum 18. Mal gestalten dürfen. Die Veranstaltungsreihe zeichnet sich dadurch aus, dass es durch Meinungsaustausch und Diskussion die Anliegen unseres Rechtsgebietes Datenschutz in das öffentliche Bewusstsein der Bevölkerung und ihrer Vertreter in den Gesetzgebungsorganen rücken soll. Im Vorwort zum Tagungsbändchen Nr. 1 heißt es:

"Es ist der Versuch, den Datenschutz als ein Menschenrecht zu zeigen. Einer breiten Öffentlichkeit soll an aktuellen Fragestellungen vermittelt werden, welche besonderen Facetten, Antworten und Konsequenzen das Recht auf Schutz der persönlichen Daten heute haben kann."

Die Idee, dass der Hessische Datenschutzbeauftragte jährlich einmal in Zusammenarbeit mit dem Landtagspräsidenten einen Diskussionsrahmen schafft, in dem – ursprünglich noch live vom Hessischen Fernsehen übertragen - aktuelle Themen zwischen Wissenschaftlern und Praktikern diskutiert werden, um dann anschließend die Wortprotokolle als Buch zu veröffentlichen, hat in ihrer praktischen Umsetzung den Datenschutz erheblich vorangebracht. Alle Nachfolger Hassemers haben Wert darauf gelegt, die Reihe der Foren fortzuführen, auch wenn Veränderungen im Verlagswesen und vielleicht auch in den öffentlichen Haushalten es offenbar irgendwann nicht mehr möglich gemacht haben, auch die verlegerisch betreute Buchreihe für den Buchhandel fortzuführen. Ich finde das schade, auch wenn mit der gefundenen Lösung, die Vortragstexte im Internet anzubieten und die Broschüren auf Anforderung kostenlos zu versenden, ein verbraucherfreundlicher Ersatz geschaffen wurde.

[3] KG – 2 Ss 23/07 - Beschl. v. 20. August 2010. Der 3. Leitsatz lautet: "Der Rechtsanwalt ist wegen § 38 Abs. 3 Satz 2 BDSG im Hinblick auf § 203 Abs. 1 Nr. 3 StGB nicht verpflichtet, dem Datenschutzbeauftragten mandatsbezogene Informationen zu geben, die seiner Verschwiegenheitspflicht unterliegen. Denn die Vorschrift des § 38 Abs. 3 Satz 1 BDSG enthält keine dem § 24 Abs. 2 Satz 1 Nr. 2 BDSG entsprechende Bestimmung, nach der sich auch bei nicht-öffentlichen Stellen die Kontrollbefugnis des Datenschutzbeauftragten auf diejenigen personenbezogenen Daten erstreckt, die der beruflichen Geheimhaltung unterliegen."

Die Titel der ersten sieben Tagungsbände und damit Themen der von Hassemer und mir jeweils zusammen mit dem Landtagspräsidenten veranstalteten ersten Foren werfen ein durchaus repräsentatives Licht auf die im Berichtszeitraum brisanten Reizthemen, die jeweils auch vor und nach den Veranstaltungen weit über die datenschutzrechtliche Fachwelt hinaus kontrovers diskutiert wurden.

Es begann 1992 mit dem Thema **„Datenschutz und Stasiunterlagen – Verdrängen oder Bewältigen?“**

Die beiden Hauptreferate wurden von Joachim Gauck und Spiros Simitis gehalten. Gauck schaffte etwas, was wohl seitdem nie wieder einem Redner in der Veranstaltungsreihe gelungen ist: Er hielt einen spannenden Vortrag, ohne dass das Wort „Datenschutz“ auch nur ein einziges Mal darin vorkam. Nicht etwa, dass der Redner sein Thema verfehlt hätte, sondern er führte seinen Zuhörern in der ihm eigenen Eindringlichkeit die Vorgeschichte und die politisch-moralischen Hintergründe des kurz vorher in Kraft getretenen Stasi-Unterlagengesetzes vor Augen. Daran konnte Simitis anknüpfen, bei dem natürlich die datenschutzrechtliche Perspektive vorherrschte. Er bescheinigte dem Gesetzgeber des Stasiunterlagengesetzes, die größtmögliche Nähe zum Datenschutz gesucht zu haben, warnte aber davor, dass der öffentliche Umgang mit den Unterlagen des MfS eine gegenläufige Entwicklung nehmen könnte, indem die Konzentration ihrer Verwendung auf individuelle Stigmatisierung die Aufarbeitung der politischen und historischen Rahmenbedingungen in den Hintergrund treten lassen könnte.

Es folgte 1993 das Forum, dessen Thematik den Strafrechtler Hassemer erkennen ließ: **„Organisierte Kriminalität – geschützt vom Datenschutz?“**

Hassemer hatte ein Jahr vorher noch als Motto des 1. Forums vorgegeben, Datenschutz müsse den Geruch verlieren, auf „Kriminelle“ und „Spinner“ konzentriert zu sein. Nun war es an der Zeit, das blöde aber verbreitete Wortspiel vom „Datenschutz = Tatenschutz“ anhand der damals als neu erlebten Form der Begehung von Straftaten durch „OK“ auf seine Berechtigung hin zu diskutieren. Bundesanwalt Schoreit und RiBVerfG Grimm hielten die Referate, Strafrechtslehrer Polizeipräsidenten, Strafverteidiger, Generalstaatsanwälte, Verfassungsschützer, Innenstaatssekretäre und Richter diskutierten kontrovers. Hassemer konnte aber am Ende resümieren, dass sich mit den Merkmalen Abschottung, Heimlichkeit, Informationsbedarf und Vernetzung immer mehr Übereinstimmungen zwischen den neuen Formen der Kriminalität und den daran angepassten neuen Methoden der Kriminalitätsbekämpfung einstellen und er glaubte aus der Veranstaltung auch eine Warnung vor einem zunehmenden Ineinanderwachsen von Strafverfolgung, Politik und Justiz auf der einen Seite und Kriminellen auf der anderen Seite, also auch Korruption, herausgehört zu haben.[4]
Auch das Forum 1994 mit dem Thema „**Datenschutz - auch für Ausländer?“** war aus einer aktuellen und bis heute nicht ganz überwundenen Problemlage gewählt. Die Schwierigkeit bestand freilich darin, dass das Verhältnis zwischen der deutschen Bevölkerung und dem Staat einerseits und den (heute sagen wir) deutschen und nichtdeutschen Menschen mit Migrationshintergrund andererseits in rechtlicher Hinsicht viel weiter greift, als es in den datenschutzrechtlichen Aspekten zum Ausdruck kommt. Wohl auch deshalb brachte jenes Forum als Novum, dass es mehr Referate (nämlich 10) gab als Diskussionsbeiträge (9) und dass am Ende von dem damaligen Schleswig-Holsteinischen DSB Bäumler und von Herrn von Plottnitz verhaltene Kritik daran angebracht wurde, das Thema Datenschutz sei eigentlich zu kurz gekommen.[5] Aber immerhin wurde auch darüber gestritten, ob man bei Kriminalstatistik, die in

[4] Tagungsband 2, S. 93
[5] Tagungsband 3, S. 66, 74.

der Veranstaltung durch Alexis Albrecht vorgestellt und gewürdigt worden war, ausländische Beschuldigte und Täter überhaupt gesondert ausweisen dürfe.[6]

1995 befasste sich das Forum ähnlich wie das heutige mit der Selbstreflektion aus Anlass eines Jubiläums **„25 Jahre Datenschutz“**. Übrigens hieß es damals nicht wie heute „Datenschutz in Hessen“, sondern schlicht „25 Jahre Datenschutz“. Damals konnte noch als allgemein bekannt vorausgesetzt werden, dass der Datenschutz weltweit ebenso alt war wie der Datenschutz in Hessen, weil die Krippe, in der das uns allen heilige Kindlein dereinst geboren wurde, nun einmal in Wiesbaden gestanden hatte. Und wie der Geburtsvorgang vonstatten gegangen war, durfte in jenem 4. Forum, noch bevor der damals amtierende HDSB und Mitveranstalter das Wort ergriff, aus eigenem Erleben der erste Datenschutzbeauftragte, den es weltweit jemals gegeben hatte, Wilhelm Birkelbach, schildern. Das ist heute noch lesenswert, zumal wir alle tief bedauern und betrauern, dass er nicht mehr unter uns weilt.

Das nächste (5.) Forum durfte ich am 28.11.1996 veranstalten. Das Thema **„Strafrecht und Datenschutz - ein Widerspruch in sich?“** war natürlich eine persönliche Verlegenheitslösung. Als ich ohne jedes Zögern die Frage bejahte, ob ich denn überhaupt die Reihe fortsetzen wolle, war ich noch keine 100 Tage im Amt und noch in der Lern- und Einarbeitungsphase. Aber ich hatte schon die Erfahrung gemacht, dass alles, was im Datenschutzrecht galt, in meinem anderen angestammten Tätigkeitsfeld alltäglich auf eine harte Probe gestellt wird. Beschuldigte in Strafverfahren hätten sich schon immer gewünscht, dass die Staatsanwaltschaft ihnen beim Nachweis ihrer Straftaten mehr informationelle Selbstbestimmung einräumen würde. Dieser Wunsch kann natürlich nur begrenzt erfüllt werden. Aber dass Zeugen und Opferzeugen, Beschuldigte mit ihrer Unschuldsvermutung sich Einsichtnahme von Dritten in Akten gefallen lassen müssen, in denen hochsensible auch Gesundheits- und Psychodaten gespeichert oder auch nur abgeheftet sind, verstand sich unter Datenschutzaspekten nicht von selbst. Das StVÄG 1999, das uns die §§ 474 ff. StPO brachte, sollte nach langjährigen immer wieder verschobenen Entwürfen erst im Jahre 2000 in Kraft treten. Und wie verhält sich die Öffentlichkeit der Hauptverhandlung zu den Werten des Datenschutzrechts? Zumal in einer Zeit, in der gerade auch wieder einmal über die Einführung eines Court-TV für Strafverhandlungen diskutiert wurde? Und überhaupt: Wie verhält sich die Staatsanwaltschaft zum Datenschutz bei ihrer Pressearbeit während des eigentlich nicht öffentlichen Ermittlungsverfahren?

Dies alles waren Fragen, bei denen gerade ich mich in meiner neuen Rolle vor übereilten Antworten schützen wollte. Also habe ich aus der Not eine Tugend gemacht und habe mit Hilfe der Vernetzung meine Behörde in der Datenschützerszene und meinen mitgebrachten „Beziehungen“ zur Strafrechtsszene beide Fachgebiete mit einer ebenso prominenten wie sachkundigen Schar von Fachleuten aus beiden Gebieten und auch noch aus der Welt der Medien zusammengebracht. Das Ergebnis war erhellend und für alle lehrreich. Unter den hochkarätigen Referenten möchte ich – ohne die anderen damit abzuwerten – insbesondere den Strafrechtsprofessor Detlef Krauß nennen, der leider vor wenigen Wochen gestorben ist. Sein damaliges Referat über die „Wirrnisse der Gesetzgebung im Strafrecht“, über die zunehmende Entformalisierung des Strafverfahrensrechts und sein Appell an den Gesetzgeber am Ende seines Vortrages sollten zur Pflichtlektüre eines jeden Strafrechtlers und Datenschutzrechtlers gehören. Seine Ausführungen mündeten in die Worte:

„Die datenschutzrechtliche Neuordnung des Strafverfahrens … ist ein Grundrechtsgebot; sie hat das Rechtsstaatsprinzip auf ihrer Seite. Die anstehende Gesetzgebung könnte dem Strafprozess in der Wirrnis gegenwärtiger Kriminalpolitik wieder einmal Konturen verleihen.“[7]

[6] Tagungsband 3, S. 74 (Plottnitz: nein [„Ostfriesen werden auch nicht gesondert ausgewiesen“]); 86 (Hassemer: ja [dient der Korrektur einer selektiven Wahrnehmung in der Öffentlichkeit und der Politik])

[7] Tagungsband 5, S. 47

Das StVÄG 1999 zur datenschutzrechtlichen Anreicherung der StPO hat leider diese Erwartung nicht erfüllt. Und Fälle wie die als Reality-TV veranstaltete Verhaftung von Klaus Zumwinkel, die öffentliche Verbreitung von Sexualpraktiken und Krankheitsdaten der beschuldigten Pop-Sängerin Benaisa und die Verbreitung von intimen Aktenteilen im Falle Kachelmann schreien auch heute noch danach, dass die Werte des Datenschutzrechts auch beim Herumfuchteln mit dem schärften Schwert des Staates, dem Strafrecht, mehr Beachtung finden.

Die letzten beiden von mir veranstalteten Foren befassten sich 1997 mit **„Datenschutz durch Kryptografie – ein Sicherheitsrisiko?“** und 1998 mit **„Datenschutz und Forschung“.**

Unser Beitrag zur sog. Kryptokontroverse: Inzwischen hatte ich gelernt, dass der besten Datenschutz in den Zeiten des Internet im technischen Selbstschutz besteht. E-Mails und gespeicherte Daten auf Festplatten und Servern galten als frei zugänglich für Hacker und halbwegs technisch versierte Spione oder private Schlüssellochgucker. Und ich hatte erfahren, dass es kostenlose Software gibt, mit der man alle Inhalte von Computern und von Telekommunikation so verschlüsseln kann, dass (so hieß es damals) selbst die IT-Leute und Hochleistungsrechner des Pentagon 100 Jahre benötigen würden, um den Schlüssel zu knacken. Aber da begann natürlich das Problem. Wenn das Pentagon das nicht schafft, dann schaffen es auch die Sicherheits- und Strafverfolgungsbehörden nicht, die mit mehr oder weniger hohen rechtsstaatlichen Voraussetzungen wie Richtervorbehalt, Zweckbindung und Verhältnismäßigkeitsgrundsatz das Recht haben, im Rahmen von Hausdurchsuchungen oder auch heimlicher Telekommunikationsüberwachung solche Eingriffshandlungen vorzunehmen.

Also gab es die politische Forderung, entweder die Entwicklung, den Export und die Anwendung hochwirksamer Kryptographie ganz zu verbieten, oder ihren Einsatz nur unter der Bedingung zu erlauben, dass sozusagen ein Zweitschlüssel für die legale hoheitliche Verwendung unter den Kautelen des Rechtsstaates zu hinterlegen sei. Das Forum, in dem wir dies unter dem Aspekt "Kryptografie als Mittel des Daten(selbst)schutzes – ein Sicherheitsrisiko?" behandelten, hatte z.B. durch das Referat von Prof. Pfitzmann sehr informative Passagen, die den Teilnehmern der anschließenden Podiumsdiskussion vor Augen führten, worum es technisch ging. Es gab aus Nachdenkliches, wie der Beitrag des damaligen Bundesjustizministers Schmidt-Jortzig. Und es gab auch Heiteres, wie der Beitrag des späteren Bundesinnenministers Otto Schily, der über seine persönlichen ersten Versuche berichtete, eine E-Mail zu verschicken:

„Ich versuche mich auch manchmal in Internet und E-Mail und allem, was es da so gibt, zu betätigen. Es ist mir einmal so ergangen, daß ich ein E-Mail zustande gebracht habe. Dann

ist es irgendwie mit einem schönen Vögelchen verschwunden - aber es kam nie an. (Heiterkeit)

Es kam auch nicht zurück. (Heiterkeit - Zuruf des Ministers Bökel)

Man weiß es nicht, vielleicht ist es bei Herrn Bökel angekommen. - Aber insofern, muss

ich sagen, habe ich ein instinktives Bedürfnis nach Kryptographie verspürt.

(Heiterkeit)“[8]

Das ist erst 13 Jahre her. Damals hatte noch niemand – wie viele wohl auch hier im Saal - ein kleines Gerät in der Tasche, mit dem er wie selbstverständlich beinahe von jedem Ort und bei jeder Gelegenheit Twittern, E-Mails und SMSe verschicken und empfangen kann, ohne dass die Provider noch wie damals AOL den Vorgang mit Vögelchen veranschaulichen müssen. Und seien wir ehrlich. Wir tun dies weitgehend auch mit personenbezogen Informationen und

[8] Tagungsband 6 Nr. 104

allein im Vertrauen darauf, dass die Verschlüsselungen, die uns die Provider voreinstellen, schon genügend Datenschutz mitliefern.

Offen gesagt, weiß ich nicht, wie die Kryptokontroverse letztlich ausgegangen ist. Ich weiß nur so viel aus dem persönlichen Erleben: Gleich nach dem Forum 1997 habe ich dafür gesorgt, dass in der Homepage meiner Anwaltspraxis allen Besuchern an der Stelle, wo sie die E-Mail-Adressen erfahren konnten, das Herunterladen eines PGP-Schlüssels angeboten wurde. Nachdem der Schlüssel 10 Jahre lang unangetastet dort gelegen hatte (es gab nicht einen einzigen Download), haben wir das Projekt beendet, zumal wir inzwischen längst auch selbst dazu übergegangen waren, Anwaltspost mit vertraulichem Inhalt in der Weise zu versenden, dass wir passwortgeschützte Pdf-Dateien verschicken. Sollte jemals ein Geheimdienst oder eine Strafverfolgungsbehörde und der zuständige Richter der Auffassung sein, dass die Voraussetzungen einer Überwachung unseres E-Mailsverkehrs gegeben seien, so wird weder uns noch den Briefpartnern das Passwort noch etwas nützen. So ähnlich wird die Sache mit der Kryptografie als Sicherheitsrisiko über weite Strecken und auf dem weiten Feld des modernen Informationsaustauschs auch sonst ausgegangen sein.

Aber das Thema Kryptografie taucht auch noch einmal in dem nächsten und meinem letzten Forum Datenschutz im Jahr 1998 auf, wo wir über die Frage diskutierten, ob und unter welchen Voraussetzungen nicht der Datenschutz die Forschung behindert. Der Vorwurf stand im Raum, u.a. weil die Forderung, zum Schutz des Grundrechts auf informationelle Selbstbestimmung müssten z.B. in der Medizinforschung personenbezogene Patientendaten stets alsbald anonymisiert oder pseudonymisiert werden, mit internationalen Wissenschaftsstandards kollidierten, die einer Forschungsstudie die Validität absprachen, wenn sie nicht auch personenbezogen reproduzierbar und jedenfalls kontrollierbar ist. Hierzu hat einer der Referenten (der Medizininformatiker Prof. Rienhoff) als Lösung vorgeschlagen, die Patientendaten mit einer Personal Identity-Technik unter Anwendung kryptografischer Verfahren zu versehen. Und als ob er ein Jahr vorher dabei gewesen wäre, hat er hinzugefügt:

„Nun wissen Sie, dass in der Kryptographiedebatte etliche Länder Vorbehalte seitens der Ermittlungsbehörden angemeldet haben. Besonders prononciert ist dies in Frankreich und in den USA formuliert worden, aber auch in anderen Ländern. Es ist auch interessant …, dass Frankreich und die USA die beiden Länder sind, die sich möglicherweise am zielstrebigsten auf diese bevorstehende und so oft apostrophierte Informationsgesellschaft vorbereiten und auch meiner Meinung nach deshalb konsequenterweise die beiden Länder sind, die ihren Geheimdienst einsetzen, um in dieser Informationsgesellschaft Informationen zu beschaffen. Wir in Deutschland tendieren in unserer angestammten Biederheit dazu, das nicht für möglich zu halten. Es ist aber eben so, dass der französische Geheimdienst auch in der Bundesrepublik Deutschland, im Nachbarland, versucht, medizinische Forschungsgeheimnisse auszuspionieren.[9]

Mit diesen Worten aus dem Munde eines Datenschutzverantwortlichen einer hessischen Universitätsklinik war der Bogen gespannt zwischen dem Thema technischer Datenschutz und Forschung. Aber darin erschöpfte sich das Thema des 7. Forums natürlich nicht. Ich muss sagen, dass ich den damaligen Dialog zwischen den Forschern aus verschiedensten Disziplinen auf der einen Seite und uns Datenschützern auf der anderen als besonders angenehm und fruchtbar in Erinnerung habe, zumal ich vorher vor einer solchen Begegnung zweier Lager mit bis dahin weitgehend praktizierter Bunkermentalität gewarnt worden war. Ich konnte am Ende des letzten von mir mitveranstalteten Forums resümieren:

"Datenschützer und Forscher haben viel zu lange übereinander, aber nicht miteinander gesprochen. Der Dialog lohnt sich und ist dringend notwendig, um die wechselseitigen Anliegen

[9] Tagungsband 7, S. 51 f.

auszutauschen und die jeweils vertretenen Grundrechte (RiS und Forschungsfreiheit) in eine praktische Konkordanz zu bringen.“[10]

Erfreulicherweise konnten wir in dem Tagungsband auch noch ein Papier der Deutschen Arbeitsgemeinschaft für Epidemiologie mit Leitlinien zum Thema „Epidemiologie und Datenschutz“ anhängen, das unter Mitwirkung meiner Mitarbeiterin für Forschung, Frau Wellbruck, und mir in manchmal mühsamen, aber am Ende doch gedeihlichen Diskussionsrunden verabschiedet worden war und auch in der Forschungsszene viel beachtet wurde.

Meine Damen und Herren. Das waren die Amtszeiten der Hessischen Datenschutzbeauftragten Hassemer und Hamm im Spiegel der ersten sieben Wiesbadener Foren Datenschutz in den 90er Jahre.

Ich habe mich auf diese Spiegelung beschränkt und Ihnen erspart, die in den jährlichen Tätigkeitsberichten dokumentierten vielfältigen Einzelaufgaben aber auch fallübergreifende weitere Themenbehandlung noch vorzustellen.

Dabei wäre auch davon zu sprechen gewesen, dass zu Beginn der 90er Jahre nicht zuletzt bedingt durch die wirtschaftliche Entwicklung in den öffentlichen Debatten ein Klima entstanden war, das Missbrauch von Sozialleistungen oder Steuerverkürzung als weitverbreiteten unerträglichen Anschlag auf gemeinsame Ressourcen einstufte. Auch in den Augen der Bevölkerung wurde als Voraussetzung der Unterbindung solchen Verhaltens eine möglichst lückenlose Kontrolle angesehen. In der Folge hatte sich der Datenschutz mit Änderungen etwa in der Abgabenordnung oder umfangreichen Missbrauchskontrollen im Sozialhilfebereich auseinander zusetzten, die zum Abgleich von Datenbeständen führten, dessen Tolerierung durch die Datenschutzaufsicht sich wenige Jahre vorher niemand hätte vorstellen können.

Und dass auch dies noch übertroffen werde konnte, haben die jüngsten Ereignisse beim Ankauf von kriminell erlangten Kontendaten der deutschen Kunden ausländischer Banken gezeigt. Vielleicht wäre auch ein solches Thema, ob der Zweck die Mittel heiligt, wenn es um Fiskalinteressen geht, einmal ein Forum wert. „Datenhehlerei“ durch den Staat, wenn die Rechtfertigung lauten soll: „Was sind schon 5 Mio. € Kaufpreis aus Steuergeldern für „geklaute“ Daten, um vielleicht 200 Mio. € zusätzlich einzunehmen? Eine solche Kalkulation und Abwägung zwischen Förderung von Kriminalität und finanziellem Ertrag erlaubt derselbe Staat seinen Bürgern und Privatunternehmen mit guten rechtlichen Gründen nicht (5 Mio. landesüblicher Bestechung in Nigeria, um einen 200-Mio-Auftrag an Land zu ziehen!). Hier habe ich schon ein wenig den Aufschrei der Datenschützer vermisst. Zumal es dabei einmal nicht um Freiheit versus Sicherheit ging.

Jenes Spannungsfeld zwischen innerer Sicherheit und informationeller Selbstbestimmung spielte während Hassemers und meiner Amtszeit schon eine große Rolle. Aber der 11. September 2001 mit seinen global wirkenden tektonischen Veränderungen stand erst noch bevor. Die Gesetze zur Bekämpfung der organisierten Kriminalität, die Einführung des großen Lauschangriffs, Verschärfungen im Bereich der Telefonüberwachungen konnten in einer Zeit diskutiert und mit dem Ziel einer Rechtsstaatsverträglichkeit teilweise auch modifiziert werden, als man z.B. an die Möglichkeit der heimlichen Einschleusung von Trojanern oder anderer Spionagesoftware in private Computer durch staatliche Stellen noch lange nicht dachte. –

Aber dafür haben wir auch noch nicht daran gedacht, dass eines Tages auch unseren Computern vom Bundesverfassungsgericht so etwas wie eine Subjektstellung als Grundrechtsträger zugebilligt werden wird. Das neue IT-Grundrecht (Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme[11]) ist natürlich so nicht gemeint. Aber es schließt eine Lücke. Wo das Grundrecht auf Unverletzlichkeit der Wohnung nicht

[10] Tagungsband 7 S. 94.
[11] BVerfGE 120, 274 = NJW 2008, 822

hinreicht (Laptop im Stadtpark), die informationelle Selbstbestimmung einfach nicht funktionieren kann (die Bios-Ebene des Betriebssystems, deren Inhalt der Nutzer nicht kennt) und wo die Telekommunikationsfreiheit nicht gilt (bei lokal gespeicherte Daten), hat das BVerfG eine neue Tabuzone markiert, die gegen jeglichen staatlichen Eingriff geschützt ist. Ich wünsche dem IT-Grundrecht eine ähnliche Karriere wie sie das seit dem Volkszählungsurteil geltende Recht auf informationelle Selbstbestimmung erleben durfte. Und die beiden werden hoffentlich nicht als Konkurrenten, die sich gegenseitig die Zuständigkeiten streitig machen, auftreten, sondern als sich ergänzendes Grundrechtsgeschwisterpaar die Rechtsprechung und das Datenschutzrecht bereichern.