Es gilt das gesprochene Wort *12. April 2008*

Festrede anlässlich der Verleihung des 43. Theodor-Heuss-Preises am 12. April 2008

Prof. Dr. Dres. h.c. Spiros Simitis

Sicherheit stärken - Bürgerrechte sichern

I.

Das Programm lässt Zweifel gar nicht erst aufkommen. Die „Festrede" ist keine Laudatio, vielmehr eindeutig einem ebenso pointiert formuliertem wie präzise umschriebenem Thema gewidmet. Und doch lässt sich beides nicht trennen. Wer nach dem Verhältnis von Sicherheit und Bürgerrechten fragt und den Konsequenzen ihrer mittlerweile immer schärferen Konfrontation nachgeht, begegnet unweigerlich Gerhard Baum, zumal dann, wenn Notwendigkeit und Voraussetzungen eines wirklich effizienten Datenschutzes zur Debatte stehen.

Ich sehe ihn, als wäre es heute, im Bundesinnenministerium, zunächst als Parlamentarischen Staatssekretär und später als Minister, energisch, fordernd, auf wirklich sorgsam überlegte Argumente bedacht, fast allergisch reagierend auf die besonders unter Juristen kultivierte Flucht in eine endlose Kasuistik, mit deren Hilfe die jeweils zur Debatte stehende Regelung selbstverständlich keineswegs „grundsätzlich" in Frage gestellt, aber doch „einmal mehr" auf nicht hinreichend bedachte Einzelaspekte überprüft werden soll, und unnachgiebig bestrebt, gerade dort neue, allen scheinbar so gefestigten Traditionen widersprechende Anforderungen durchzusetzen, wo der Respekt vor dem Einzelnen sowie seiner, für eine demokratische Gesellschaft konstitutiven Selbstbestimmung auf dem Spiel steht.

Leicht hatte er es nicht. Schon deshalb nicht, weil, um beim Datenschutz zu bleiben, die siebziger Jahre ganz im Vorzeichen der Länder standen. Ein Bundesland, Hessen, war es, das 1970 den Datenschutz weltweit zum ersten Mal garantiert hat. Und nur wenig später, 1974, beschränkte sich ein weiteres Bundesland, Rheinland-Pfalz, nicht darauf, sich anzuschließen, sondern entschied sich für ein anderes Kontrollmodell. Die Anfangszeit des Datenschutzes war so gesehen vom Wettbewerb der Länder geprägt. Wie konstruktiv er sich gestaltete, zeigt sich allein schon an der zunächst keineswegs unwidersprochen hingenommenen, letztlich aber doch akzeptierten Unabhängigkeit der Datenschutzbeauftragten und ihrer Kontrollkompetenz.

Der Bund hinkte hinterher. Der offenkundige Kontrast zwischen dem nachdrücklichen Plädoyer des damaligen Hessischen Ministerpräsidenten Albert Osswald für ein Datenschutzgesetz und den zögerlichen, von Hinweisen auf konfligierende Interessen und unvermeidliche Grenzen durchsetzten einleitenden Bemerkungen von Bundesinnenminister Hans-Dietrich Genscher im November 1972 bei der Anhörung zum Referentenentwurf eines Bundesdatenschutzgesetzes spiegeln genau diesen Unterschied wider, illustrieren aber zugleich, mit welchen Widerständen und Schwierigkeiten man Mitte der siebziger, Anfang der achtziger Jahre beim Versuch rechnen musste, das Bundesdatenschutzgesetz konsequent anzuwenden, und erst recht bei den frühen Ansätzen bereichsspezifischer Regelungen, nicht zuletzt im Sicherheitssektor.

Gerhard Baum hat maßgeblich dazu beigetragen, den Konkretisierungsprozess des Datenschutzes tatsächlich in Gang zu setzen und den Datenschutz endgültig in eine am Grundgesetz orientierte und ihm verpflichtete Rechtsordnung zu integrieren.

Wer verstehen will, was die 1983 vom Bundesverfassungsgericht formulierte und zuletzt in seinem Urteil v. 27. Februar dieses Jahres nachdrücklich bestätigte Forderung genau bedeutet, personenbezogene Daten nur ausnahmsweise und wenn es sich nicht vermeiden lässt, ausschließlich

für klar vordefinierte Zwecke zu erheben und lediglich solange zu verarbeiten wie es für diese Ziele notwendig ist, gleichviel im Übrigen, ob es dabei um Sicherheits-, Beschäftigungs-, Gesundheits-, Kredit-, Versicherungs- oder sonst welche Fragen geht, muss zunächst den Blick auf die Verarbeitungstechnologie richten.

Sie ist es, die Ende der sechziger Jahre den Gesetzgeber vor dem Hintergrund geplanter oder schon im Aufbau befindlicher Datenzentralen, welche, wie es wörtlich hieß, die strenge und unwiderlegbare Rationalität einer sich nicht zuletzt in der Bürgernummer manifestierenden, allwissenden staatlichen Verwaltung gewährleisten sollten, alarmierte und die Forderung nach einer radikal beschränkten sowie jederzeit kontrollierbaren Verwendung personenbezogener Daten begründete. Sie ist es aber auch, die seither, dank ihrer immer schnelleren Entwicklung, den Anreiz für immer neue Informationsansprüche gegeben und die Möglichkeit, sie zu realisieren, geschaffen hat.

Anders und schärfer formuliert: Wer eine Verarbeitung von Kommunikationsdaten auf Vorrat vorschreibt, die sofortige Zugänglichkeit der meisten von den Sicherheitsbehörden verwendeten Angaben quer durch die Europäische Union propagiert oder sich für eine ebenso generelle wie umfassende Untersuchung und Beobachtung, sei es aller Kinder, sei es bestimmter Gruppen ausspricht, kann es nur tun, weil die Verarbeitungstechnologie einen Stand erreicht hat, der es erlaubt, Vorstellungen, welche noch vor kurzem illusorisch erschienen, sofort und bedingungslos zu verwirklichen. Mit anderen Worten und direkt auf den Leitsatz des heutigen Tages bezogen: Reflexionen über „Sicherheit stärken - Bürgerrechte sichern" machen erst Sinn, wenn sie bei der Verarbeitungstechnologie ansetzen und so den Operationsrahmen verdeutlichen.

Vor allem dreierlei gilt es dabei zu bedenken:

Erstens, anders als in den Anfangszeiten des Datenschutzes und noch bis in die neunziger Jahre hinein stellt sich heute nicht mehr die Frage, welche Daten, allein schon aus technischen Gründen, erhoben und verarbeitet werden sollen. Mittlerweile ist nahezu jede personenbezogene Angabe gesammelt und gespeichert. Die einst noch für selbstverständlich gehaltenen Speicherungsgrenzen sind endgültig entfallen. Freilich nicht weil, wie ebenfalls lange angenommen, Datenbanken gigantische Ausmaße erreicht haben, die eine genauso beispiel- wie endlose Akkumulation von Daten ermöglichen. Die immer schnellere, ja inzwischen selbstverständliche Automatisierung der Verarbeitung hat zwar auch Art und Anzahl der jeweils verwendeten Angaben um ein Vielfaches gesteigert. Ausschlaggebend ist jedoch nicht die Größe der Datenbank, sondern die Intensität der Vernetzung. Sie hebt letztlich die Verarbeitungsgrenzen auf und multipliziert uneingeschränkt den verfügbaren Datenbestand.

Zweitens: Die Verarbeitungstechnologie sichert keineswegs nur die Erreichbarkeit der Daten. Sie schafft zugleich die Voraussetzungen für eine multifunktionale Verwendung. Bereits gespeicherte Angaben verwandeln sich so in eine Informationsquelle, die aus den unterschiedlichsten Gründen für die unterschiedlichsten Zwecke genutzt werden kann. Stichworte wie „Data Mining" deuten genau diesen Zusammenhang an. Der Datenbestand mag feststehen, seine Verwendung ist dagegen unendlich variabel. In dem Masse, in dem die Verarbeitung zunimmt, verschärft sich daher zugleich der Druck, die Daten als Elemente eines tendenziell offenen Informationsprozesses zu sehen und zu behandeln. So war, um nur ein Beispiel aus jüngster Zeit zu nehmen, die Britische Biobank, mit deren Hilfe spezifische Alterskrankheiten, wie Demenz oder Parkinson, besser bekämpft werden sollen, und die deshalb langfristig angelegte, ständig überprüfte und verfeinerte Profile von Personen erstellt, welche das vierzigste Lebensjahr überschritten

haben, kaum gegründet, als sich Versicherungsgesellschaften sowie Sicherheitsbehörden meldeten und ihr Interesse an der Verwertung dieser Profile bekundeten.

Drittens: Die kontinuierlich zunehmende Verwendung personenbezogener Daten sowie die Multifunktionalität der Angaben haben den organisatorischen Aufbau der Verarbeitung von Grund auf verändert. So verflüchtigt sich mehr und mehr die sorgfältige Trennung zwischen den Datenbanken öffentlicher Stellen einerseits und den Datensammlungen nichtöffentlicher Stellen andererseits. Vorexerziert haben es die Vereinigten Staaten. Die Regierung erklärte zwar sehr bald nach dem 11. September ihre Absicht, eine Vielzahl bis dahin nicht gesammelter Angaben zu Personen, die in den USA wohnhaft sind, verwenden zu wollen, sah aber weitgehend davon ab, die Daten selbst zu

erheben. Sie überließ es stattdessen einer kleinen Gruppe von Unternehmen, welche mittlerweile über nahezu jede Angabe zu den Lebensumständen aller Einwohner der USA verfügen, die jeweils gewünschten Profile zu erarbeiten. Regelungen wie die jüngsten Vorschriften zu den Telekommunikationsdaten liegen auf derselben Linie. Der Staat definiert seine Informationswünsche, zieht es jedoch vor, die je spezifischen Daten von privaten Unternehmen erheben zu lassen und sichert sich lediglich das Zugriffsrecht. So gesehen, überrascht es nicht weiter, dass die betroffenen Unternehmen, durchaus folgerichtig, nicht lange gezögert haben, eine Erstattung der von eindeutig staatlichen Aufgaben verursachten Kosten zu fordern, eine Erwartung, die sie schon bei den Verhandlungen über die Richtlinie zu den Vorratsdaten vorgebracht hatten.

Die Trias einer ebenso umfassenden wie erschöpfenden Verarbeitung personenbezogener Daten, ihrer multifunktionalen Verwendbarkeit und einer systematischen Vernetzung der Datenbestände erklärt auch den Perspektivenwandel: Wo nur bestimmte Daten vorhanden sind oder gar erhoben werden können, ist es nur konsequent, ja „natürlich", lediglich auf Angaben zurückzugreifen, welche für die Bewertung eines besonderen Sachverhalts nötig sind. Gleichviel ob es um die Aufklärung einer Straftat oder die Übernahme von Krankheitskosten geht, die Verwendung der Daten rechtfertigt sich aus dem Konnex zum konkreten Vorgang. Er löst die Verarbeitung aus, indiziert ihren Umfang und beschränkt zugleich die Datennutzung. Wo dagegen nahezu alle Daten über jeden Einzelnen vorhanden sind, drängt sich staatlichen Stellen genauso wie privaten Unternehmen die Akzentverschiebung von der Reaktion auf den Einzelfall auf die systematische Prävention sämtlicher genauso oder ähnlich gestalteter Fälle geradezu von selbst auf, ohne Rücksicht im Übrigen darauf, ob man es bei öffentlichen Stellen beim traditionellen Verständnis der Vorbeugung belässt, oder, wie erst jüngst, im Interesse einer wirksamen Terrorismusbekämpfung, für „ein neuartiges Präventionsrecht mit kriegsrechtlichen Elementen" plädiert.

Deutlich wird allerdings zugleich: Vorbeugung ist keine Erwartung, die ausschließlich im Zusammenhang mit der Sicherheitspolitik auftaucht und deshalb nur in ihrem Kontext gesehen und beurteilt werden muss. Kontroversen wie der Konflikt über die Vorratsdaten, Vorschläge wie die Anregung, kriminogene Faktoren durch eine fortlaufende Beobachtung von Kindern, und zwar schon vom embryonalen Zustand an, oder Datenkombinationen wie die inzwischen fast selbstverständliche Verknüpfung von Angaben aus den unterschiedlichsten Dateien qualifizieren die Prävention gewiss als besonderes, wenn nicht singuläres Wahrzeichen einer bewusst langfristig angelegten Sicherheitspolitik. Nichts anderes gilt jedoch für den Gesundheitsbereich. Allein schon die Debatte über die elektronische Gesundheitskarte sowie die damit verbundene Konzentration der Daten und die Vielfalt ihrer möglichen Verwendungen lässt die Dominanz von Präventionsbestrebungen erkennen. Erst recht manifestiert sie sich in den Vorstellungen zu den von Gesundheitsämtern und privaten Versicherungsgesellschaften gleichermaßen geforderten regelmäßig wiederkehrenden, tendenziell lebenslangen krankheitsspezifischen Untersuchungen. Im einen

wie im anderen Fall mehren sich, nicht zuletzt im Zeichen einer Kostenreduktion, die Ansätze für eine eindeutig, möglichst frühzeitig einsetzende präventive Observation. In beiden Fällen deckt sich daher das Ergebnis: eine bewusste, von einer fortlaufenden Verarbeitung personenbezogener Daten begleitete Verhaltenssteuerung, die wie bei der Sicherheitspolitik repressive Konsequenzen einkalkuliert, ja sogar offen anspricht.

Ebenso klar ist allerdings: Die Vorherrschaft der Prävention wirkt sich unmittelbar und nachhaltig auf die verfassungsrechtlich vorgegebenen, in den Datenschutzgesetzen präzisierten Rechte der Betroffenen aus. Regelungen, die Präventionsstrategien konkretisieren, weiten den Verarbeitungskreis unvermeidlich um ein Vielfaches aus. Relevant sind durchweg Daten, die noch nicht für das jeweils verfolgte Ziel gebraucht, aber doch zu einem späteren Zeitpunkt benötigt werden könnten. Wer mit wem wann und warum telefoniert, spielt vorderhand keine Rolle. Wichtig sind zunächst nur das Mittel und der Zeitpunkt der Kommunikation. Ebenso gleichgültig ist es, ob jemand bestimmte Krankheitssymptome aufweist. Seine oder ihre Zugehörigkeit zu einer Altersgruppe oder überhaupt zur Bevölkerung genügt schon. In jedem dieser Fälle sind die personenbezogenen Daten Teil einer Informationsmasse, deren Relevanz offen ist, und die betroffenen Personen Objekte eines Informationsprozesses, der sie restlos instrumentalisiert. Was ihnen bleibt, ist nur die Hoffnung, dass ihre Daten später einmal gelöscht werden. Selbst dann freilich, wenn Löschungsfristen explizit vorgesehen sind, werden sie in aller Regel so angelegt, dass genug Zeit bleibt, die Daten unterdessen für andere Zwecke zu verwerten.

Mehr denn je kommt es unter diesen Umständen darauf an, sich die verfassungsrechtlichen Prämissen zu vergegenwärtigen, denen jeder Zugriff auf personenbezogenen Daten genügen muss. Mit dem üblichen Hinweis auf die „informationelle Selbstbestimmung" ist es nicht getan. Das Bundesverfassungsgericht hat es im Volkszählungsurteil eben nicht dabei belassen, vielmehr das Grundrecht des Einzelnen festzulegen was mit den Angaben zu seiner Person geschehen darf, an eine Aussage geknüpft, die immer wieder übergangen wird: Das Entscheidungsvorrecht über die eigenen Daten ist, so das Gericht, „elementare Funktionsbedingung" eines „freiheitlichen demokratischen Gemeinwesens". Nur wenn die Betroffenen über die Verwendungsabsicht ebenso rechtzeitig wie genau informiert werden und sich sowohl die Zulässigkeit als auch der Verlauf der Verarbeitung nach ihren Vorgaben richtet, bleibt ihre für eine demokratische Gesellschaft unerlässliche Kommunikations- und Mitwirkungsfähigkeit erhalten.

Nicht von ungefähr hat sich deshalb die Europäische Union keineswegs damit zufrieden gegeben, den Datenschutz ausdrücklich in die Charta der Grundrechte aufzunehmen. Er kehrt an einer anderen Stelle der Verfassungsvorschläge wieder, nämlich bei der Bestimmung der für den demokratischen Charakter der Union unverzichtbaren Anforderungen. Eine nachhaltige Restriktion der Verwendung personenbezogenen Daten umschreibt so einmal mehr keineswegs nur Sinn und Tragweite eines individuellen Grundrechts, sondern zunächst und vor allem den Maßstab dafür, wie viel an Verarbeitung die Demokratiefähigkeit einer Gesellschaft verträgt.

Genau diese Wahrnehmung der Verarbeitungsbedingungen wird freilich wieder und wieder verdrängt. Prüf- und Zulässigkeitsmaßstab ist stattdessen ein zunehmend formal verstandener Rechtsstaat. So verwundert es nicht, wenn nachdrücklich vor einem „Überbietungswettbewerb" der,, hypertrophen Exegeten" des Grundrechts auf informationelle Selbstbestimmung gewarnt wird, die durchweg bestrebt sind, „rechtsstaatlichen Hürden für staatliches Handeln gerade auf dem Gebiet der Gefahrenabwehr stetig zu erhöhen" und „dem Staat den Zugang zu Informationen zu erschweren, deren er im Vorfeld der Gefahr bedarf, um die Sicherheit seiner Bürger zu gewährleisten." Und ganz in diesem Sinn heißt es an die Adresse des Bundesverfassungsgerichts in einem wenig später erschienenen Beitrag eines anderen Autors: die „simple Erwägung, eher als

durch einen sekundenschnellen Datenabgleich würden die Bürger durch die ernstzunehmende Furcht von Terroranschlägen eingeschüchtert", lasse „am Gefahrbewusstsein der Richtermehrheit zweifeln". Oder noch deutlicher und entschieden schärfer: „Ehe das Datenschutzsektiererwesen die Blutgruppe eines Terrorverdächtigen freigibt, nimmt es das Risiko eines Blutbades in Kauf."

Wo dagegen die Auswirkungen der Verwendung personenbezogener Daten auf die Substanz einer demokratischen Gesellschaftsordnung der primäre Ansatz und Maßstab möglicher Reaktionen sind, stellt sich spätestens in dem Augenblick, in dem feststeht, dass es kaum noch personenbezogene Daten gibt, die nicht verarbeitet werden und die deshalb, technisch jedenfalls, jederzeit erreichbar wären, dringlicher denn je die Frage, ob ein Zugriff nicht selbst dann unterbleiben muss, wenn er sich durchaus realisieren ließe. Mit anderen Worten: eine Gesellschaft, die sich allein schon durch die lange Liste der tagtäglich benutzten oder neu entwickelten Karten, angefangen bei den Kunden- über die Kredit-, Banken- und Versicherungskarten bis hin zu den Gesundheitskarten, mit einer allgegenwärtigen Verarbeitung konfrontiert sieht, kann nicht umhin, ihre Demokratiefähigkeit auch und gerade an der Bereitschaft zum Informationsverzicht zu messen.

Wie schwer es allerdings fällt, einen Verzicht zu akzeptieren, hat sich bereits an der Debatte über die Verwendung der Mautdaten eindringlich gezeigt. Der Gesetzgeber musste gleich mehrmals eingreifen, um die Verpflichtung sicherzustellen, die Angaben lediglich für die Berechnung der Autobahngebühren zu nutzen. Aber: die Auseinandersetzung um genau diese Einschränkung ist offensichtlich längst nicht beendet. Und wieder sind es die Sicherheitsbehörden, die sich auf ihre Aufgaben, vor allem also die Aufklärung von Straftaten, berufen, um einen Anspruch auf die Daten zu begründen.

Mehr noch gibt ein zweites Beispiel zu denken: die schon erwähnte britische Biobank. Verarbeitet werden dort keineswegs nur medizinische und genetische Daten. Die Biobank erhebt vielmehr genauso detaillierte Angaben zu den familiären Bedingungen, der beruflichen Tätigkeit und ihrem speziellen Umfeld, den Wohn- und Umweltverhältnissen und den persönlichen Gewohnheiten. Das Ergebnis ist ein in der Tat geradezu singuläres Profil. Auch hier haben die Sicherheitsbehörden ihre Informationserwartungen sehr bald durchgesetzt. Der Kontrast zur Stellungnahme des deutschen Nationalen Ethikrates könnte nicht schärfer sein. Der Ethikrat knüpft die Einrichtung von Biobanken zuvörderst an eine Bedingung: Der Forschungszweck muss nicht nur legitimer Verarbeitungsanlass, sondern genauso zwingende Verwendungsgrenze sein. Wer also die Daten haben möchte, ist gleichgültig. Den Sicherheitsbehörden bleibt der Zugang ebenso verwehrt wie etwa Arbeitgebern oder Versicherungsgesellschaften. Was freilich der klaren Mehrheit der Ratsmitglieder selbstverständlich erschien, ist keineswegs unwidersprochen hingenommen worden. Die noch kurz vor der Abstimmung gestellte Frage, ob die strikte Zweckbindung auch bei der Fahndung nach einem Mörder gelten solle, spiegelt Zweifel und Ablehnung deutlich wider.

Das Dilemma lässt sich schwerlich besser illustrieren: Die Verarbeitungstechnologie bietet spät- oder schon nachindustriellen Gesellschaften die Chance, Informationen zu bekommen, ohne die es kaum gelingen könnte, existentiell wichtige Konsequenzen einer sich unwiderruflich verändernden Altersstruktur verlässlich aufzuzeigen und erfolgreich anzugehen. So evident dieser Vorteil ist, so klar ist ebenso, dass jede derart minutiöse Verwendung personenbezogener Daten das Tor für letztlich unüberschaubare Interventions- und Steuerungsmaßnahmen öffnet, kurzum den demokratischen Charakter der Gesellschaft tangiert und zu gefährden droht. Eine Alternative zu der vom Nationalen Ethikrat geforderten Beschränkung der Verarbeitung auf den ursprünglichen Verwendungszweck kann es deshalb nicht geben. Der Verzicht bietet den Betroffenen und unserer Gesellschaftsordnung den denkbar besten Schutz, ohne die mit den Daten verbundenen For-

schungsaufgaben in Frage zu stellen. Anders ausgedrückt: Solange allen Versuchen, den Forschungsvorbehalt zu umgehen, eindeutig verbindliche Schranken gesetzt sind, ist der Respekt vor den Rechten der Bürger und damit ihre Mitwirkungs- und Kommunikationsfähigkeit gesichert.

Ein konsequenter Informationsverzicht muss zwar die primäre Reaktion auf eine inzwischen allumfassende Verarbeitung personenbezogener Daten und eine Technologie sein, die einen jederzeitigen Zugang zu allen Angaben ebenso ermöglicht wie ihre gezielte Verknüpfung. Realistisch gesehen, kann aber ein Verzicht nur in seltenen vor allem an den langfristigen gesellschaftlichen Folgen der konkreten Verarbeitungsstrategien orientierten Ausnahmefällen erwartet werden. Erst recht kommt es deshalb, zumal vor dem Hintergrund der bisherigen Erfahrungen, darauf an, Verwendungsbedingungen festzuschreiben, die einen Verarbeitungsverlauf gewährleisten, der sich in jeder seiner Phasen tatsächlich an die Anforderungen einer wirklich ernst genommenen und konsequent praktizierten informationellen Selbstbestimmung hält.

So viel sollte unstreitig sein: Wer immer personenbezogene Daten verwenden möchte, ist begründungspflichtig. Eigentlich eine Selbstverständlichkeit, sofern die auch vom Bundesverfassungsgericht wieder und wieder bekräftigte Feststellung, dass die Verarbeitung solcher Angaben nur ausnahmsweise tolerierbar ist, nicht endgültig zur rhetorischen Floskel verkommen soll. Die Erfahrung zeigt jedoch, wie übermächtig die Tendenz ist, es bei möglichst allgemeinen Aussagen zu belassen, die allenfalls Vorspiel einer ebenso substantiierten wie präzisen Angabe der je spezifischen Gründe sein können, welche genau die angestrebte Regelung rechtfertigen. „Terror" und „Sicherheit" sind exemplarisch dafür. Niemand kann ernsthaft in Frage stellen, dass beidem Rechnung getragen werden muss. Doch die Reflexion über erforderliche Maßnahmen beginnt selbst bei einer noch so nachdrücklich vorgebrachten Betonung beider erst jenseits ihrer bloßen Erwähnung. Sie vermittelt allenfalls den Schein einer Begründung, verdrängt aber dafür die Begründungspflicht.

Nichts anderes gilt für die Gesetzessprache. „Schwere" oder nur „besonders schwere" Straftaten, „schwerwiegende" Nachteile oder lediglich solche von „erheblicher Bedeutung", die schlichte „Gefährdung des Gemeinwohls" oder dessen „schwerwiegende Beeinträchtigung" sind längst gängige und zudem in immer neuen Varianten auftauchende Rechtfertigungen des Informationszugriffs. Mit jedem dieser Anknüpfungspunkte verlagert sich zugleich der Schwerpunkt der Gesetzesanwendung. Der unklare Gesetzestext ist genau genommen nur die Brücke zu einem Gesetzesverständnis, das von den Erwartungen der an den Daten interessierten und sie verarbeitenden Stellen dominiert wird.

Es ist deren Sicht, die das Anwendungsfeld von Vorschriften bestimmt, die hinreichend unpräzise formuliert sind, um den Aktionsspielraum der konkret in Betracht kommenden Stellen nicht „ungebührlich" einzuschränken. Und ebenso wenig verwundert es, dass ausgerechnet dann, wenn der Gesetzgeber eine Sprache benutzt, welche, zumindest bei der Wortwahl, nur eine bedingte, offenkundig auf Ausnahmefälle zugeschnittene Verarbeitungsmöglichkeit suggeriert, die jeweiligen öffentlichen Stellen ihre Verwendungsbefugnis gezielt ausgebaut haben, angefangen bei Grenzsituationen bis hin zu weiteren aus ihrer Perspektive mindestens ebenso wichtigen Verarbeitungsfällen. Wo aber, wie bei einer tatsächlich unmissverständlich festgeschriebenen Zweckbindung, alle Interpretationsbestrebungen versagten, kam es nicht nur zu einer offenen Kritik der spezifischen Regelung, sondern, um nur an die Mautdaten zu erinnern, zu immer wieder neu unternommenen Versuchen einer Gesetzesänderung.

Eigentlich hätte schon der Umgang mit den Datenschutzgesetzen vorsichtig stimmen müssen. Gemeint sind nicht so sehr jene Vorschriften, welche Ausnahmen vom Datenschutz statuieren,

vielmehr ausgerechnet diejenigen Bestimmungen, mit deren Hilfe eine Verwendung personenbezogener Daten eingeschränkt und damit der Datenschutz garantiert werden soll. Auch sie waren gerade in der Anfangszeit ähnlich allgemein gehalten, allerdings aus einem ganz anderen Grund: Der Gesetzgeber war sich durchaus darüber im Klaren, dass er sich in einem Bereich bewegte, dessen Konturen sich zwar bereits abzeichneten, dessen genaue Bedeutung dagegen, besonders in Anbetracht einer sich immer schneller entwickelnden Technologie, kaum abschätzbar war. Die allgemein formulierten Regelungen sollten eine fortlaufende Anpassung ermöglichen, die Datenschutzgesetze also davor bewahren, allzu schnell überholt zu werden. Doch die durchaus datenschutzfreundliche Formulierungsstrategie hatte die gegenteilige Wirkung. Öffentliche und nichtöffentliche Stellen nutzten ihren Interpretationsspielraum zu einer betont restriktiven Auslegung, die den Geltungsbereich der Datenschutzbestimmungen gezielt reduzierte.

Ganz gleich daher, ob es um mehr oder weniger Datenschutz geht, eines bestätigt sich durchweg: Wie real die Chancen der informationellen Selbstbestimmung sind, entscheidet sich auch und vor allem an der Gesetzessprache. In dem Masse, in dem unverbindliche, gewollt abstrakte Formulierungen vorherrschen, schwindet zugleich die Möglichkeit, sie konsequent und ohne Schwierigkeit in einer Weise anzuwenden, die sich zuvörderst an der Notwendigkeit ausrichtet, Verarbeitung als Ausnahme zu begreifen und zu praktizieren, keineswegs nur um der betroffenen Personen, vielmehr genauso und erst recht um des Bestandes einer demokratischen Gesellschaft willen.

Ebenso nachdrücklich muss aber vor einem Missverständnis gewarnt werden: Der Mangel an Präzision in der Gesetzessprache lässt sich nicht durch eine noch so ausgeklügelte Verweisungsstrategie beheben. Wohl keine andere Vorschrift ist hierfür so bezeichnend wie jene Bestimmung der Strafprozessordnung, in der die Überwachung und Aufzeichnung der Telekommunikation definiert werden (§ 100a StPO). Die Verpflichtung, genau anzugeben, wann es dazu kommen darf, scheint auf den ersten Blick gewahrt zu sein; doch die schier endlose Aufzählung einschlägiger Regelungen, eine in der Tat echte „Rundreise durchs Strafgesetzbuch", täuscht Präzision nur vor. Wer die Tragweite der Paragraphenkompilation ermessen will, kann sich nicht mit dem bloßen Hinweis auf Gesetzesbestimmungen zufrieden geben. Die Konsequenzen lassen sich vielmehr erst in Kenntnis der Interpretation und damit der effektiven Anwendungsbedingungen jeder dieser Vorschriften ausmachen. Präzision ist aber gerade bei grundrechtsrelevanten legislativen Interventionen lediglich solange gegeben wie ihre Bedingungen und Folgen möglichst direkt und nachvollziehbar dem Gesetzestext selbst zu entnehmen sind. Abgesehen davon dürfen Sondervorschriften, die eine Datenverarbeitung legalisieren, nicht für sich betrachtet werden. Sie sind vielmehr durchweg im Kontext aller übrigen Ausnahmen zu sehen und zu bewerten, weil nur dann die Auswirkungen auf den Realitätsgehalt der informationellen Selbstbestimmung verlässlich einzuschätzen sind.

Präzision hat ihren Preis. Sie begrenzt zwar den Aktionsspielraum der Daten verarbeitenden Stellen, verdeutlicht aber umso mehr die Vorläufigkeit aller Regeln, die sich auf die Verwendung personenbezogener Angaben beziehen. Was schon für ihre Frühzeit bezeichnend war, gilt nach wie vor: Damals wie heute messen sich Bedeutung und Wirksamkeit der legislativen Eingriffe an der Verarbeitungstechnologie. Damals wie heute sind deshalb gesetzliche Vorschriften immer nur vorläufige Reaktionen. Konsequenterweise muss der Gesetzgeber für eine Regelungsstrategie optieren, die genau dieser Einsicht Rechnung trägt.

Die skandinavischen Länder haben sich schon früh dafür entschieden: Datenschutzvorschriften werden ausdrücklich befristet. Sie gelten lediglich für einen bestimmten, exakt vorgegebenen Zeitraum. Der Gesetzgebungsprozess verwandelt sich so aus einer tendenziell einmaligen Entscheidungsfindung in einen ebenso kontinuierlichen wie offenen Diskurs. Der Gesetzgeber mag

sich mithin für eine besondere Reaktion ausgesprochen haben, er verpflichtet sich jedoch zugleich, seine Position auch und vor allem mit Rücksicht auf die Verarbeitungstechnologie fortwährend zu überprüfen. Nur unter dieser Voraussetzung lässt sich die Effizienz der gesetzlichen Regelung gleich in doppeltem Sinn sicherstellen: Veränderungen der Technologie können durch den Gesetzgeber genauso wirksam aufgefangen wie Umgehungen und Aufweichungen der Datenverarbeitung rechtzeitig korrigiert werden.

Ich gebe zu, dass ich einen etwas anderen Weg gegangen bin, als manche vielleicht erwartet haben. Weder habe ich auf konkrete Maßnahmen hingewiesen, die dazu verhelfen könnten, die Sicherheit zu stärken, noch einzelne Bürgerrechte detailliert behandelt, die gesichert werden müssten. Gerade die Erfahrung der letzten Jahre hat gezeigt, wie müßig es ist, den Akzent ganz auf einzelne Maßnahmen,zu setzen oder die Aufmerksamkeit ausschließlich auf eine ebenso fragmentierte Reflexion bei den Bürgerrechten zu lenken. Wenn wir wollen, dass die Bürgerrechte garantiert werden und auch nicht verkennen, dass auf Gefährdungen der Sicherheit reagiert werden muss, dann gilt es zuallererst sich auf die Grundelemente einer demokratischen Gesellschaft zu besinnen und sodann Bedingungen festzuschreiben, die für jede Sicherheitsmaßnahme sowie die Sicherheitspolitik überhaupt verbindlich sind. Begründungspflicht, eine wirklich präzise Gesetzessprache, die Bereitschaft zum Informationsverzicht und die Befristung der gesetzlichen Entscheidungen zur Verarbeitungstechnologie gehören zu den Meilensteinen eines alternativlosen Weges.