BKA
Vortragsreihe

POLIZEILICHE DATENVERARBEITUNG

BUNDESKRIMINALAMT WIESBADEN

BKA-Vortragsreihe

Die »BKA-Vortragsreihe« enthält die Referate und Diskussionsbeiträge der Arbeitstagungen des Bundeskriminalamtes.

Zitiervorschlag:

> Edwin Kube, Rechtsgrundlagen polizeilicher Datenverarbeitung; in: BKA-Vortragsreihe Bd. 28 (hrsg. vom Bundeskriminalamt), Wiesbaden 1983, S. 99–119.

Die Bände werden in der Regel nur an Polizeidienststellen, Justizbehörden und ähnliche Institutionen abgegeben. Interessenten werden gebeten, sich an das Bundeskriminalamt, KI 13, Postfach 18 20, 6200 Wiesbaden, zu wenden.

Bisher sind folgende Bände erschienen:

1. Bekämpfung des Falschgeldunwesens (1954)
2. Bekämpfung der Jugendkriminalität (1955)
3. Bekämpfung von Glücks- und Falschspiel (1955)
4. Bekämpfung von Rauschgiftdelikten (1956)
5. Bekämpfung von Betrug und Urkundenfälschung (1956)
6. Das kriminalpolizeiliche Ermittlungsverfahren (1957)
7. Bekämpfung der Wirtschaftsdelikte (1957)
8. Grundfragen der Kriminaltechnik (1958)
9. Bekämpfung von Diebstahl, Einbruch und Raub (1958)
10. Kriminalpolitische Gegenwartsfragen (1959)
11. Bekämpfung der Sittlichkeitsdelikte (1959)
12. Internationale Verbrechensbekämpfung (1960)
13. Strafrechtspflege und Strafrechtsreform (1961)
14. Brandermittlung und Brandverhütung (1962)
15. Grundfragen der Wirtschaftskriminalität (1963)
16. Vorbeugende Verbrechensbekämpfung (1964)
17. Kriminalpolizei und Technik (1967)
18. Grundlagenforschung und Kriminalpolizei (1969)
19. Fahndung (1970)
20. Datenverarbeitung (1972)
21. Organisiertes Verbrechen (1974)
22. Polizei und Prävention (1975)
23. Polizei und Justiz (1976)
24. Der Sachbeweis im Strafverfahren (1978)
25. Möglichkeiten und Grenzen der Fahndung (1979)
26. Polizei und Kriminalpolitik (1980)
27. Bestandsaufnahme und Perspektiven der Verbrechensbekämpfung (1981)
28. Polizeiliche Datenverarbeitung (1982)

(Jahreszahl in Klammern:
Veranstaltungsjahr der Arbeitstagung)

BKA-Vortragsreihe Band 28

POLIZEILICHE DATENVERARBEITUNG

Arbeitstagung
des Bundeskriminalamtes Wiesbaden
vom 2. bis 5. November 1982

Herausgeber
BUNDESKRIMINALAMT WIESBADEN
1983

Druck Bundesdruckerei

I n h a l t

	Seite
Begrüßung Heinrich Boge	5
Eröffnungsansprache Carl-Dieter Spranger	9
Thesen zur Funktion und Bedeutung der Datenverarbeitung bei der Polizei Heinrich Boge	19
Informationstechnologie der Zukunft Fritz Krückeberg	37
Das INPOL-System - Zielsetzungen und Ausbaustand 1982 Dieter Küster	57
Polizeitaktische Aspekte des Einsatzes der Datenverarbeitung Gerd Lehmann	73
Polizeiliche Datenverarbeitung in Schweden Anna Greta Gehnich	87
Rechtsgrundlagen polizeilicher Datenverarbeitung Edwin Kube	99
Informationsverbund Justiz - Polizei Günter Ernesti	121
Informationsverbund Ordnungsbehörden - Polizei Horst Julich	149

Seite

Die Datenverarbeitung der Polizei und die öffentliche Meinung
Dagobert Lindlau 165

Polizei und Datenschutz
Herbert Tolksdorf 175

Datenschutz und Polizei
Spiros Simitis 191

Technisch-wissenschaftliche Datenverarbeitung und Forschung im BKA
Ernst Bunge 213

Die Veränderung der Arbeitswelt des polizeilichen Sachbearbeiters
Hans-Georg Stuff 221

ADV-Probleme in der Aus- und Fortbildung
Thomas Gnad 227

Ausbildungs- und Informationsprobleme - aus der Sicht der Anwendung
Hans-Georg Kaesehagen 231

Innere Sicherheit und Datenverarbeitung
Podiumsgespräch mit
Paul Laufs, Herbert Neu, Axel Wernitz, Heinrich Boge, Kuno Bux, Hans Peter Bull, Heinrich Weyer 237

Schlußwort
Edwin Kube 283

Verzeichnis der Verfasser 289

Begrüßung

Heinrich Boge

Ich darf Sie zur Arbeitstagung 1982 des Bundeskriminalamtes herzlich willkommen heißen. Es ist mir eine Ehre, in unserer Mitte den Parlamentarischen Staatssekretär beim Bundesminister des Innern, Herrn Carl-Dieter Spranger, begrüßen zu können, der diese Tagung eröffnen wird. Ich werte die Anwesenheit des Herrn Parlamentarischen Staatssekretärs als Beweis seines Engagements zum Thema der Tagung "Polizeiliche Datenverarbeitung". Es wird uns in diesem Jahr besonders interessieren, aus seinem Munde die Auffassungen der neuen Leitung des Bundesinnenministeriums zu den grundlegenden Fragen der polizeilichen Verbrechensbekämpfung ebenso wie zur Rolle und Bedeutung der polizeilichen Datenverarbeitung einschließlich der besonderen Aspekte des Datenschutzes zu erfahren.

INPOL - das gemeinsame Informationssystem der Polizei des Bundes und der Länder - verkörpert im Blickfeld von Politik und interessierter Öffentlichkeit die Gesamtheit der polizeilichen Datenverarbeitung. In dem "Programm für die Innere Sicherheit in der Bundesrepublik Deutschland", das die Innenminister des Bundes und der Länder 1972 vorlegten, heißt es denn auch: "Es soll ein gemeinsames Informations- und Auskunftssystem für die gesamte Polizei in der Bundesrepublik mit dem Bundeskriminalamt als Zentralstelle geschaffen werden". Das INPOL-System gilt mit seinem heutigen Ausbaustand zu Recht als ein Aktivposten der Kooperation von Bund und Ländern auf dem Gebiet der Inneren Sicherheit. Es schmälert nicht die Verdienste aller Beteiligten und Verantwortlichen, wenn es festzuhalten gilt, daß das Gesamtsystem noch nicht vollendet ist und es weiterer großer Anstrengungen zur Verwirklichung der gesetzten Ziele bedarf.

INPOL besteht in diesen Tagen fast genau 10 Jahre. Am 13. November 1972 wurde das Fahndungsauskunftssystem von INPOL offiziell in Dienst gestellt. In den Jahren danach ist es Bund und Ländern gemeinschaftlich gelungen, eine arbeitsteilige Datenverarbeitung zur Unterstützung der Verbrechensbekämpfung zu errichten, die sich in der täglichen Arbeit der Polizei bewährt hat und nicht mehr zu ersetzen ist und in ihrem heutigen Ausbaustand bereits national und international hohe fachliche Anerkennung genießt.

Das Bundeskriminalamt hat nicht zuletzt deshalb das 10jährige Bestehen des INPOL-Systems zum Anlaß genommen, seine diesjährige Tagung unter das Thema Datenverarbeitung zu stellen. Bei der Wahl dieses Themas geht es dem Bundeskriminalamt aber um mehr als eine Jubiläumsveranstaltung. Die Tagung gibt uns vielmehr die Gelegenheit zu einer kritischen Bestandsaufnahme und sachbezogenen Aufarbeitung der in den letzten Jahren aufgekommenen, beim Aufbau der polizeilichen Datenverarbeitung nicht immer sogleich erkennbaren Probleme der Praxis. Es geht allerdings auch um die Aufarbeitung der verbliebenen Probleme und Konflikte des Datenschutzes. In der mitunter hektischen Debatte um die Dateien und Karteien der Polizei sind Irrtümer und Mißverständnisse aufgetreten, die der Korrektur und Aufklärung bedürfen, indem das polizeiliche DV-Instrumentarium offengelegt wird und die Konfliktfelder in sachlicher Atmosphäre ausdiskutiert werden.

Die Polizei stellt sich rückhaltlos der Diskussion. Wer wie die Polizei täglich mit schutzbedürftigen personenbezogenen Daten umgeht, sieht die Notwendigkeit datenschutzrechtlicher Regelungen selbstverständlich ein. Es muß aber auch gewährleistet sein, daß die Polizei ihren gesetzlichen Auftrag zur Verbrechensbekämpfung sachgerecht erfüllen kann.

Die Entwicklung der Kriminalität macht heute den Einsatz der Datenverarbeitung zur effektiven Unterstützung der Verbrechensbekämpfung erforderlicher denn je. Erwähnt seien nur die Bereiche der Massenkriminalität und des organisierten Verbrechens, deren neue Verbrechensphänomene ohne die Hilfe der modernen Informationstechnologie nicht mehr wirksam bekämpft werden können.

Die Polizei bezieht aber auch keine ideologischen Positionen und sieht im Einsatz der Datenverarbeitung keineswegs das Allheilmittel, das allein kriminalistische Erfolge verspricht. Die Datenverarbeitung ist für die Polizei nicht mehr und nicht weniger als ein notwendiges Hilfsmittel zur besseren Unterstützung der Polizeiarbeit. Sie orientiert sich dabei ebenfalls nicht ausschließlich an bloßen Effizienzerwägungen. Die bisherigen Ausbauschritte des INPOL-Systems stehen trotz mancher gegenteiliger Behauptungen überzeugend für die Gewährleistung der Rechtmäßigkeit und Verhältnismäßigkeit der polizeilichen Datenverarbeitung ein.

Die Informations- und Kommunikationstechnologie kennt keinen Stillstand und befindet sich in einem Prozeß ständiger Fortentwicklung. Viele durch das Eindringen der Datentechnik in alle Arbeits- und Lebensbereiche aufgekommenen Folgeprobleme sind gesamtgesellschaftliche Fragen, die jedermann interessieren und angehen. Auch bei der Polizei dringt die Datentechnik zunehmend in neue Arbeitsbereiche vor. Das Bundeskriminalamt hat deshalb, wie das Tagungsprogramm zeigt, den Bogen der Themen bewußt weit gespannt; polizeiliche Datenverarbeitung umfaßt heute viele Bereiche, von der Fahndung bis zur technisch-wissenschaftlichen Forschung. Insbesondere die technischen Neuerungen stehen häufiger im Blickpunkt des Interesses.

Ich gebe meiner Hoffnung Ausdruck, daß diese Tagung neben der notwendigen Sachinformation dazu verhelfen möchte, die anstehenden Probleme der Lösung näherzubringen und die Perspektiven der zukünftigen Entwicklung aufzuzeigen. Den Damen und Herren Referenten möchte ich an dieser Stelle meinen besonderen Dank für die Übernahme dieser Aufgaben aussprechen. Sie alle besitzen in ihren jeweiligen Fachgebieten ein hohes Ansehen. Es ist deshalb zu erwarten, daß die Referate und die begleitenden Diskussionen zu richtungsweisenden Ergebnissen für die polizeiliche Arbeit führen werden.

Ich hoffe, daß die folgenden Tage Ihnen hierzu die Impulse vermitteln mögen und wünsche Ihnen einen angenehmen Aufenthalt in Wiesbaden.

Eröffnungsansprache

Carl-Dieter Spranger

Es entspricht einer guten Tradition, daß der Bundesminister des Innern die jährliche Arbeitstagung des Bundeskriminalamtes eröffnet. Wenn ich heute anstelle von Bundesminister Dr. Zimmermann zu Ihnen spreche, so soll dies nicht einen Bruch dieser Tradition bedeuten. Minister Dr. Zimmermann hatte die feste Absicht, Ihre Tagung zu eröffnen, gerade auch, weil er in der Sicherheitspolitik einen wesentlichen Schwerpunkt seines neuen Aufgabenbereichs sieht. Leider kann er wegen zwingender anderer Verpflichtungen heute nicht anwesend sein. Er bedauert dies und hat mich gebeten, Ihnen die besten Wünsche für einen guten und erfolgreichen Verlauf der Tagung zu übermitteln.

Die jährlichen Arbeitstagungen des Bundeskriminalamtes finden nicht nur in Fachkreisen, sondern auch in der Öffentlichkeit breite Resonanz. Der Erfahrungs- und Meinungsaustausch zwischen Praktikern von Polizei und Justiz, Wissenschaftlern, Publizisten und Politikern aus dem In- und Ausland hat stets zu einer wirkungsvollen Aufhellung von Problembereichen der Kriminalitätsentwicklung und -bekämpfung beigetragen. In vielen Fällen sind wertvolle Anregungen für die Fortentwicklung der Kriminalpolitik, ja der Rechts- und Innenpolitik auf dem Gebiet der Inneren Sicherheit, gegeben worden.

Bereits die Aktualität des Themas der diesjährigen Tagung "Polizeiliche Datenverarbeitung" läßt einen Verlauf Ihrer Veranstaltung erwarten, der den hohen Stellenwert der Arbeitstagungen unterstreicht. Die Ausgestaltung des Programms macht deutlich, daß unterschiedliche Auffassungen zu Wort kommen sollen. Kreative Meinungsvielfalt - sei es aufgrund von Interessengegensätzen, sei es aufgrund von unterschiedlichen politischen Standorten - ist notwendig, wenn es gelingen soll, die Klärung schwieriger Fragen - wie etwa im Zusammenhang mit der polizeilichen Datenverarbeitung - voranzutreiben und Lösungsmöglichkeiten aufzuzeigen.

Es trifft sich, daß in diesen Tagen das INPOL-System, das gemeinsame Informationssystem der Polizeien des Bundes und der Länder, 10 Jahre besteht. Dies wird Anlaß geben, Rückblick auf das bisher Erreichte zu halten, den gegenwärtigen Standort zu bestimmen und die Frage zu erörtern, wie es weitergehen soll.

Es liegt 10 Jahre zurück, daß im Bundeskriminalamt zu diesem Thema eine der heutigen Tagung entsprechende Fachtagung stattfand. Damals war die Situation, wie überall, auch bei der Polizei durch erste tastende Gehversuche mit dem neuen Medium Datenverarbeitung gekennzeichnet. Die Referate des Jahres 1972 gaben deshalb im wesentlichen die Planungsstände der damaligen Zielvorstellungen und Nutzungskonzeptionen wieder, ohne daß die Tragweite und aufkommende Folgeprobleme bereits zu erkennen waren.

1982 blicken Bund und Länder mit Stolz auf die beim Ausbau des Informationssystems der Polizei erzielten Fortschritte. Die Verbrechensbekämpfung verfügt damit über ein Hilfsmittel, das aus dem polizeilichen Alltag nicht mehr hinwegzudenken ist. Insbesondere die mit dem INPOL-Fahndungssystem seit Jahren erzielten Erfolge sind ein beeindruckender Leistungsbeweis. Das INPOL-System erfährt national und international große Anerkennung. Diese gemeinsame Aufbauleistung der Polizeien des Bundes und der Länder verdient Dank und Anerkennung.

Die polizeiliche Datenverarbeitung ist nicht statistisch, sondern als dynamischer Prozeß zu begreifen. Dies gilt nicht nur für die Herausforderung, die durch die stürmische Entwicklung der Technik der Datenverarbeitung bedingt ist. Sie zwingt immer wieder zu arbeitsintensiven Systemanpassungen in Bund und Ländern. Dies gilt noch mehr für die inhaltliche Fortentwicklung des arbeitsteiligen Bund/Länder-Systems, die zum Ziele hat, die Datenverarbeitung für neue polizeiliche Anwendungen nutzbar zu machen.

Gegenwärtig befindet sich das INPOL-System in einer entscheidenden Fortentwicklungsphase. Nach intensiven Verhandlungen haben sich die Innenminister des Bundes und der Länder einvernehmlich auf ein Konzept zur Fortentwicklung des INPOL-Systems sowie auf ein Konzept zum Aufbau und zur Führung eines zentralen Kriminalaktennachweises, beschränkt auf schwere und überregional bedeutsame Straftaten, verständigt. Es gilt nunmehr, auf der Basis dieser Entscheidungen für eine zügige Realisierung zu sorgen. Wer mit der Materie vertraut ist, weiß, wieviele Schwierigkeiten im Detail noch überwunden werden müssen. Er weiß aber auch, daß Wünsche offengeblieben sind, daß es sich insbesondere hinsichtlich des Kriminalaktennachweises um Wünsche von Praktikern handelt.

Ich nehme an, daß diese Wünsche auf der Arbeitstagung artikuliert und diskutiert werden. Bundesminister Dr. Zimmermann wird das Ergebnis in seine Überlegungen einbeziehen, ob hier Nachhol- oder Verbesserungsbedarf besteht. Für die polizeiliche Arbeit ist nicht nur die Datenverarbeitung bei der Polizei selbst interessant. Eine wesentliche Frage wird m.E. künftig auch sein, inwieweit es gerechtfertigt und zulässig ist, der Polizei unmittelbaren Zugriff auf Informationssysteme anderer Behörden - ich denke etwa an das Kraftfahrt-Bundesamt, das Ausländerzentralregister sowie das Bundeszentralregister - einzuräumen.

Zu entscheiden wird aber auch sein, ob und in welchem Umfang polizeiliche Informationssysteme anderen Behörden, insbesondere den Staatsanwaltschaften, zu öffnen sind. Mir ist bewußt, daß es zu diesen Fragen unterschiedliche Positionen gibt. Ich nehme an, daß dies in den hierzu vorgesehenen Einzelreferaten herausgearbeitet wird. Ich hoffe, daß die Erörterung auch dieser Fragen einen Beitrag zur Lösung der tatsächlich und rechtlich komplexen Problematik bringen wird.

Der Einsatz modernster technischer Mittel bei der Verbrechensbekämpfung ist unverzichtbar, insbesondere auch, um der höheren Mobilität der Straftäter und raffinierteren Tatmethoden wirkungsvoller zu begegnen. Ein sinnvoller Einsatz der Datenverarbeitung bei der Polizei findet deshalb unsere volle Unterstützung. Wir dürfen allerdings nicht in den Fehler verfallen, allein auf die Technik zu setzen. Diese ist nicht Selbstzweck, sie kann immer nur Hilfsmittel sein.

Die Notwendigkeit, behutsam mit den Mitteln der Datenverarbeitung umzugehen, betone ich hier nicht aus Gründen des Datenschutzes, sondern aus Sorge um die Effizienz polizeilicher Aufgabenerfüllung. Wenn zunehmend polizeiliche Kapazität zur Bedienung von Computersystemen gebunden wird, entsteht die Gefahr, daß die Polizei verbürokratisiert und das Verbrechen nur noch verwaltet wird. Ich meine, wir müssen erste Stimmen aus der Praxis ernst nehmen, die beklagen, daß die Beamten vor den Datensichtgeräten festgehalten werden und immer weniger Zeit finden, sich an den Ort des Geschehens zu begeben, um dort zu ermitteln.

Nach jüngsten Pressemeldungen hat etwa der Landesverband Niedersachsen des Bundes Deutscher Kriminalbeamter in einer umfangreichen Untersuchung nicht zu Unrecht darauf hingewiesen, daß allein mit dem "Kollegen Computer", in den beispielsweise Fahndungsersuchen eingegeben werden, Kriminalität nicht aufgeklärt werden könne. Aber nicht nur dies: erfolgreiche polizeiliche Aufgabenerfüllung erfordert auch Bürgernähe.

Ich glaube, es ist heute allgemeine Auffassung, daß ein polizeilicher Streifendienst nicht allein vom Streifenwagen aus erfolgen kann. Die Bürger begrüßen es, daß sie wieder vermehrt polizeilichen Fußstreifen begegnen und wieder einen persönlichen Kontakt zu "ihrem" Polizeibeamten finden. Der Bürger darf diesen zurückgewonnenen Kontakt nicht durch zu starke Bindung des Beamten an neue Technik wieder verlieren.

Die heutigen Computersysteme sind durchaus in der Lage, Beeindruckendes zu leisten. Dennoch: die Fähigkeit des Menschen zu intuitivem und assoziativem Denken ist nach wie vor unerreicht. Gerade die Verbrechensbekämpfung lebt jedoch von der Intuition und der individuellen Kreativität des einzelnen Kriminalbeamten, seiner Sachkunde, seiner Erfahrung und seinem persönlichen Einsatz. Dies kann kein Computer ersetzen.

Gerade weil diese Eigenschaften für den Polizeiberuf so wesentlich sind, lassen Sie mich an dieser Stelle betonen: die Beamten werden zu Leistungsbereitschaft und persönlichem Engagement nur dann motiviert, wenn sie die Gewißheit haben, daß Vorgesetzte und Politiker für sie auch in schwierigen Situationen einstehen. Sie müssen erwarten können, daß ungerechtfertigter Kritik unmißverständlich entgegengetreten wird. Daß dieses im Verantwortungsbereich des Bundesministers Dr. Zimmermann geschieht, dessen dürfen Sie versichert sein.

Sie werden erwarten, daß ich bei diesem Thema der Arbeitstagung einige Worte zum Datenschutz im Sicherheitsbereich sage. Datenschutz ist notwendig. Die Bundesregierung bekennt sich zum Datenschutz als Garanten für den Schutz der Privatsphäre. Dies gilt auch für den Sicherheitsbereich. Datenschutz hat jedoch keinen absoluten Vorrang vor den Erfordernissen der öffentlichen Sicherheit. Gefahr sowohl für die Institution des Datenschutzes als auch für die Arbeit der Sicherheitsbehörden und für unsere Bürger tritt dann ein, wenn die notwendige Balance zwischen den berechtigten Belangen der Bürger und der zu ihrem Schutz tätigen Sicherheitsbehörden nicht gewahrt wird.

Die Bundesregierung wird den Datenschutz - entsprechend seinem Stellenwert - auch im Bereich der Inneren Sicherheit gemeinsam mit den Ländern weiterentwickeln und präzisieren. Dabei sind Sachlichkeit und Augenmaß geboten. Vor Perfektionismus müssen wir uns hüten. Polizeiliche Arbeit ist so unmittelbar mit der Vielfalt des Lebens konfrontiert, daß wir die polizeiliche Arbeit nicht in Regelwerken völlig erfassen können. Wir wollen daher nicht nur, sondern wir müssen auf das Verantwortungsbewußtsein und das rechtsstaatliche Vorgehen der handelnden Polizeibeamten setzen. Wir haben keinen Anlaß, ihnen grundsätzlich zu mißtrauen.

Klar muß sein, daß beim Datenschutz Übertreibungen, die dem Bürger keinen Nutzen bringen, zu vermeiden sind. Wir werden jedem konkreten Hinweis nachgehen, ob etwa überzogene Datenschutzregelungen oder falsch verstandene Anwendung zu nicht gerechtfertigten Defiziten bei der Kriminalitätsbekämpfung führen. Niemand bestreitet, daß durch den Einsatz und die vielfältigen Möglichkeiten der elektronischen Datenverarbeitung Gefahren für die Freiheitssphäre einzelner verbunden sein können. Deswegen unterliegen die Datenverarbeitung wie die Behörden überhaupt den hierfür vorgesehenen rechtsstaatlichen Kontrollen. Der Gedanke des Datenschutzes darf jedoch nicht als Vehikel benutzt werden, einseitig Mißtrauen gerade gegenüber den Sicherheitsbehörden zu artikulieren. Die Sicherheitsbehörden sind in den Rechtsstaat eingebunden. Wir leben nicht in einem Polizeistaat.

Lassen Sie mich bei dieser Gelegenheit auf einige grundsätzliche Aspekte eingehen, die nach unserer Auffassung Voraussetzung für eine erfolgreiche Arbeit im Sicherheitsbereich sind.

Sicherheit im wohlverstandenen Sinne ist unerläßliche Voraussetzung für die Freiheit. In der öffentlichen politischen Diskussion wird immer wieder die Frage nach dem Verhältnis von Freiheit und Sicherheit gestellt. Häufig werden beide in einen Gegensatz gesetzt. Betrachtet man totalitäre Staaten, so kann kein Zweifel bestehen, daß dort eine schrankenlose Staatsmacht, die sich einseitig dem Sicherheitsgedanken verpflichtet fühlt, den Freiheitsraum des einzelnen in unerträglicher Weise aushöhlt. Dort sind Freiheit und Sicherheit in der Tat Gegensätze.

In einem Rechtsstaat jedoch, der von freiheitlichen Grundwerten geprägt ist, dient die Sicherheit der Wahrung der verfassungsmäßigen Ordnung, in deren Rahmen sich die Freiheit des einzelnen voll entfalten kann. Es geht nicht um Freiheit oder Sicherheit, sondern um die gesicherte Freiheit, um Freiheit in Sicherheit. Es geht darum, daß der Staat Sicherheit und inneren Frieden gerade um der Freiheit willen zu gewährleisten hat.

So gesehen besteht also ein Gegensatz zwischen Freiheit und Sicherheit nicht. Diese Grundaussage enthebt jedoch nicht der Notwendigkeit, bei allem staatlichen Handeln jeweils sorgfältig abzuwägen, mit welchen staatlichen Mitteln in die Freiheitssphäre des einzelnen eingegriffen werden darf, um die Freiheit aller zu sichern.

Dies macht deutlich, daß die Sicherheit eben nur eine dienende - wenn auch notwendige - Funktion für die Freiheit hat. Mit aller Deutlichkeit lassen Sie mich aber bitte auch sagen, daß die Freiheitsrechte unserer Verfassung sich nicht dadurch zu bewähren haben, daß sie den Gegnern der Verfassung und Rechtsordnung jeden von ihnen gewünschten Handlungsspielraum verschaffen.

Die Sicherheitsbehörden müssen imstande sein, ihre schwierige Aufgabe nach Maßgabe unserer Rechtsordnung effizient zu erfüllen. Dazu bedürfen sie der Unterstützung der Bürger. Dies ist ohne Stärkung des Vertrauens in die Arbeit der Sicherheitsbehörden nicht möglich. Die Sicherheitsbehörden sind bereit, zur Gewährleistung dieses Vertrauens im größtmöglichen Umfang Transparenz zu ertragen. Sie stellen sich auch etwa berechtigter Kritik.

Sie haben jedoch Anspruch darauf, daß ihr schwieriger Auftrag und ihre Leistungen anerkannt und jede unberechtigte Kritik zurückgewiesen wird, insbesondere dann, wenn gegenüber den Sicherheitsbehörden in ungerechtfertigter Weise Mißtrauen geschürt wird. Die Sicherheitsbehörden müssen sich also gleichermaßen auf das Vertrauen der Bürger sowie der politisch Verantwortlichen stützen können. Fehlt es hieran, führt dies zu Verunsicherungen, die nicht hingenommen werden können.

Ich bin sicher, daß die ganz überwiegende Mehrheit unserer Bevölkerung Vertrauen in die Arbeit der Sicherheitsbehörden hat. Vertrauen bedeutet allerdings auch, daß Einvernehmen über die Notwendigkeit besteht, geltendes Recht zu achten, anzuerkennen und durchzusetzen. Es gilt, dieses Rechtsbewußtsein unter allen Bürgern des Staates, insbesondere unserer Jugend, zu festigen und, soweit es in Teilbereichen in Frage gestellt wird, wieder herzustellen. Dies umfaßt auch die Respektierung demokratisch legitimierter Mehrheitsentscheidungen. Jedenfalls dürfen die Sicherheitsorgane nicht diskreditiert werden, wenn sie geltendes Recht vollziehen oder die Durchsetzung demokratischer Entscheidungen sichern. Hier sehe ich auch eine staatspolitisch wichtige Aufgabe der Medien.

Die Politik hat andererseits sicherzustellen, daß dringende politische und soziale Probleme bereits im Anfangsstadium erkannt und aufgegriffen werden. Die Politiker dürfen die Polizei mit gesellschaftspolitischen Problemen nicht alleine lassen. Die Bundesregierung bekennt sich zu unserer freiheitlichen Rechtsordnung. Jeder dem demokratischen Rechtsstaat Verpflichtete wird sich einem Abbau oder einer Aushöhlung rechtsstaatlicher Errungenschaften widersetzen.

Meinungsäußerung und Demonstration im Rahmen unserer Rechtsordnung zur Durchsetzung politischer Ziele sind unverzichtbarer Teil unserer Grundordnung. Wir widersetzen uns allerdings mit aller Entschiedenheit dem Mißbrauch von Freiheitsrechten durch einzelne Minderheiten. Wir werden vor Gruppen, die Forderungen, welcher Art auch immer - mit Gewalt und Rechtsbruch durchsetzen wollen, nicht zurückweichen. Das Gewaltmonopol liegt allein beim Rechtsstaat. Wir müssen klar unterscheiden zwischen Demonstranten und Gewalttätern.

Über die Frage einer Änderung des Demonstrationsrechts wird seit längerem intensiv nicht nur in den Parteien, sondern auch innerhalb der Polizei nachgedacht. Mich hat die engagierte Diskussion auf der GdP-Tagung in Nürnberg zu diesem Thema beeindruckt. Ich glaube, es ist möglich, in dieser bisher sehr streitig geführten Frage zu einer insbesondere für die Praxis hilfreichen Lösung zu kommen. Der Vorschlag der GdP könnte hier vielleicht ein erster Ansatz für einen Konsens sein.

Der Anstieg der Kriminalitätsentwicklung ist erschreckend. 4 Mio. registrierte Straftaten im Jahre 1981 bedeuten einen unerträglichen Rekord. Diese Entwicklung ist nicht schicksalhaft. Es kann keine Kapitulation vor dem Verbrechen geben. Der Bundesminister des Innern wird gemeinsam mit den Innenministern der Länder erörtern, wie dem bisherigen Anstiegstrend durch gezielte Maßnahmen für einzelne besonders stark angewachsene Kriminalitätsbereiche entgegengewirkt werden kann.

Den Terrorismus wird die Bundesregierung mit aller Intensität bekämpfen. Er hat sein Gesicht gegenüber den 70er Jahren entscheidend verändert; die Anschlagstätigkeit beschränkt sich längst nicht mehr auf die harten Kerne; zu den Terroristen von links sind die von rechts gekommen. Entsprechend der Mobilität und der Anpassungsfähigkeit der Terroristen muß die Bekämpfungskonzeption ständig angepaßt werden. Grenzüberschreitende Aktivitäten der Terroristen und der internationale Terrorismus überhaupt lassen sich nur durch intensive internationale Zusammenarbeit wirksam bekämpfen. Wir werden daher die Kooperation mit allen Staaten, die bereit sind, dem Terrorismus Einhalt zu gebieten, fortsetzen und ausdehnen.

Wir werden aber auch nicht zulassen, daß Gäste und Freunde unseres Landes in der Bundesrepublik Deutschland durch terroristische Anschläge bedroht werden. Das gilt insbesondere für unsere amerikanischen Verbündeten, die auch zu unserem Schutz hier sind. Wer unsere Freunde und ihre Familien angreift, greift uns selbst an. Die Täter sind bei ihren Anschlägen so skrupellos, daß sie schwerste Verletzungen und sogar den Tod von Frauen und Kindern in Kauf nehmen. Die deutschen Sicherheitsbehörden werden alles tun, diesen Tätern das Handwerk zu legen.

Sie werden daher mit aller Entschiedenheit und Klarheit gegen jeden Extremismus von links wie von rechts vorgehen. Die Bundesregierung wird nicht zögern, wenn es geboten ist, von den grundgesetzlichen Instrumenten zum Schutz der freiheitlichen demokratischen Grundordnung Gebrauch zu machen.

Die große Mehrheit der bei uns lebenden über 4,6 Mio. Ausländer verhält sich durchaus gesetzestreu. Auch in ihrem Interesse wird es die Bundesregierung nicht dulden, daß extremistische und terroristische ausländische Gruppen ihre Auseinandersetzungen im Bundesgebiet gewalttätig austragen. Die in der Koalitionsvereinbarung angekündigte Kommission für Ausländerpolitik wird daher auch zu prüfen haben, wie rechtsstaatliche Wege gefunden werden können, um diesem Treiben wirksamer zu begegnen und wie das Instrumentarium verbessert werden kann, um straffällig gewordene Ausländer abzuschieben. Dies gilt auch für die Frage, wie illegale Einreisen und Beschäftigungen von Ausländern wirksam unterbunden werden können.

Die Bundesregierung wird Entscheidungen für bereits vorgeschlagene Maßnahmen, die einen Sicherheitsgewinn erwarten lassen, herbeiführen. Ich denke insbesondere an die Einführung eines fälschungssicheren, automatisch lesbaren Personalausweises und eines fälschungssicheren Kfz-Kennzeichens.

Die Gesamtverantwortung für die Innere Sicherheit der Bundesrepublik Deutschland tragen in unserem föderativen System die Innenminister von Bund und Ländern gemeinsam. Eine erfolgreiche Bewältigung der schwierigen Sicherheitsprobleme ist daher nur möglich, wenn in wesentlichen Punkten einvernehmliche Auffassungen erarbeitet werden. Wir brauchen auf dem Gebiet der Inneren Sicherheit eine geschlossene und entschlossene Politik. Hierzu bedarf es sicherlich in manchen Fragen auch der allseitigen Bereitschaft, aufeinander zuzugehen. Sachgerechte Lösungen kann es aber nur geben, wenn die Zusammenarbeit von gegenseitigem Vertrauen getragen ist. Für den Bundesminister des Innern ist es deshalb ein sehr großes Anliegen, den notwendigen atmosphärischen Konsens in der Innenministerkonferenz wieder herzustellen. Denn dies dient dem Erfolg unserer sachlichen Arbeit.

Die Bereitschaft, die Probleme offen und im Interesse sachgerechter Lösungen zu diskutieren, wird sicherlich auch diese Arbeitstagung bestimmen. Ich wünsche ihr einen guten Verlauf.

Thesen zur Funktion und Bedeutung der Datenverarbeitung bei der Polizei

Heinrich Boge

Zu Beginn dieses Vortrags möchte ich kurz mein Thema abgrenzen. Das Sammeln, Auswerten und Umsetzen von Informationen, also Daten, ist seit jeher ein wesentlicher Bestandteil polizeilicher Arbeit gewesen. Die Polizei hat also schon immer "Datenverarbeitung" betrieben. Anlaß dieser Arbeitstagung ist jedoch die Inbetriebnahme des INPOL-Fahndungssystems vor zehn Jahren. Aus diesem Grunde nehme ich - wohl in Übereinstimmung mit den Organisatoren und den übrigen Referenten dieser Tagung - an, daß das Thema "Thesen zur Funktion und Bedeutung der Datenverarbeitung bei der Polizei" ausschließlich auf die elektronische Datenverarbeitung zu beziehen ist, also auf den Einsatz von Computern zur Unterstützung der polizeilichen Tätigkeit. Zunächst möchte ich - im wesentlichen exemplarisch anhand der Fahndung - umreißen, welche Veränderungen die elektronische Datenverarbeitung im polizeilichen Alltag in den letzten zehn Jahren bewirkt hat. Anschließend werde ich das Anwendungsspektrum dieses neuen Hilfsmittels näher beleuchten. Drittens gehe ich - und das ist ein besonderes Anliegen des Präsidenten des Bundeskriminalamtes - auf die Zusammenarbeit zwischen Bund und Ländern, mit anderen Behörden sowie mit dem Ausland ein. Abschließend müssen auch Probleme und Grenzen der Datenverarbeitung bei der Polizei angesprochen werden.

These 1

Bereits der nach zehn Jahren erreichte Ausbaustand der elektronischen Datenverarbeitung hat die polizeiliche Arbeit in Bund und Ländern grundlegend verändert.

Ein kurzer Rückblick in die "vorelektronische Zeit" dient der Erläuterung dieser These. Ich möchte mich dabei aus Zeitgründen, weil dies das augenfälligste Beispiel ist, schwerpunktmäßig auf den Bereich Fahndung beschränken. Aktuellstes Hilfsmittel der Personenfahndung war die parallel in ca. 80 Kriminaldienststellen der Bundesrepublik sowie zentral beim Bundeskriminalamt geführte Fahndungskartei (1). Ausschreibungs- bzw. Löschungsanträge gingen von den örtlichen Dienststellen über die Landeskriminalämter an das Bundeskriminalamt. Von hier aus wurden die Aktualisierungen arbeitstäglich auf dem Postwege an die karteiführenden Dienststellen versandt.

Dienststellen ohne Fahndungskartei bzw. Beamte im Außendienst waren auf das monatlich (für Festnahmen) und vierteljährlich (für Aufenthaltsermittlungen) erscheinende Deutsche Fahndungsbuch angewiesen.

Eine umfassende Sachfahndungskartei bzw. ein allgemeiner Sachfahndungsnachweis mit allen Gegenständen, nach denen gefahndet wurde, bestand auf Bundesebene nicht. Beim Bundeskriminalamt wurde jedoch eine Kartei über alle als abhandengekommen gemeldeten Kraftfahrzeuge geführt. Alle vier Monate wurde vom Bundeskriminalamt ein Sachfahndungsnachweis-Kraftfahrzeuge herausgegeben. Sonstige Gegenstände waren in Sachfahndungsnachweisen/-karteien auf örtlicher bzw. auf Landesebene erfaßt. Lediglich ein Teil davon wurde dem Bundeskriminalamt gemeldet.

Das Beispiel Fahndung zeigt aus heutiger Sicht, welche Einbußen an Aktualität und Schnelligkeit hingenommen werden mußten. Selbst täglich aktualisierte Fahndungskarteien hinkten um bis zu 2-3 Wochen hinter der Wirklichkeit her. So lange nämlich konnte es dauern, bis Ausschreibungs- und Löschungsanträge von den ausschreibenden Dienststellen bei der zentralen Fahndungskartei beim Bundeskriminalamt anlangten. Noch inaktueller war naturgemäß das Deutsche Fahndungsbuch. Vor Festnahmen aufgrund des Fahndungsbuches mußte deshalb bei der nächsten Personenfahndungskartei Rückfrage gehalten werden, ob die Fahndungsausschreibung noch aktuell war. Dazu kam das Mengenproblem. Zwischen 1951 und 1970 verdoppelte sich ungefähr der Bestand der Personenfahndungskartei. Welche Folgen das hinsichtlich der Handhabbarkeit des Fahndungsbuches hatte, läßt sich leicht ausmalen.

Zu dem Mengen- und Zeitproblem, das außer im Bereich der Fahndung vor allem bei der Nachrichtensammlung und -auswertung immer akuter wurde, gesellten sich andere, qualitative Herausforderungen an die polizeiliche Arbeit. Auch wenn der überwiegende Teil der Straftäter früher wie heute im örtlichen oder regionalen Bereich tätig war und ist, stellte gerade der nicht dazu gehörende Täterkreis die Polizei vor neue Aufgaben. Komfortablere Kommunikationsmöglichkeiten, schnellere und bequemere Verkehrs- und Transportmittel und durchlässigere Staatsgrenzen schufen Raum für überregional und international organisierte Eigentumskriminalität. Aus den gleichen Gründen konnten Einzeltäter ihre Wirkungsstätten leichter wechseln bzw. begrenzten Fahndungsmaßnahmen ausweichen. Das Aufkommen der politisch motivierten Gewaltkriminalität mit den daraus resultierenden hoch komplexen Ermittlungsverfahren Ende der 60er / Anfang der 70er Jahre tat ein übriges, um die Grenzen der herkömmlichen Instrumente polizeilicher Arbeit aufzuzeigen.

Als eines der wirksamsten Gegenmittel wurde angesichts dieser Entwicklung schon in den 60er Jahren die Nutzung der technischen Möglichkeiten der elektronischen Datenverarbeitung für die Polizei (2) in Betracht gezogen. Die ersten Versuche jener Jahre der "Elektronisierung" der Nachrichtenauswertung fanden auf der Ebene von Großstadt- bzw. der damals noch existierenden Kommunalpolizeien - z.B. durch den damaligen Nürnberger Polizeipräsidenten Herold (3) - statt. Die ersten auf Bund-Länder-Ebene koordinierten Planungen gab es ab 1966. Nachdem dann 1970 die Bundesregierung den Einsatz der elektronischen Datenverarbeitung bei der Polizei in ihr Sofortprogramm zur Verbrechensbekämpfung aufgenommen hatte, wurde im Januar 1972 das erste gemeinsame Konzept, der elektronische Fahndungsverbund, von der Innenministerkonferenz verabschiedet. Die Realisierung dieses Beschlusses im November 1972 ist der Anlaß dieser Arbeitstagung.

Obwohl die Entwicklung nach zehn Jahren sicher noch nicht an ihrem Ende angekommen ist, hat es bereits eindrucksvolle Veränderungen gegeben:
Die vorhin geschilderten zeitraubenden Abläufe bei der Personen- und Sachfahndung schrumpften auf Minuten, wenn nicht gar Sekunden zusammen. Von über 2.000 direkt an den Rechner des Bundeskriminalamtes bzw. an einen Landesrechner angeschlossenen Terminals aus können Fahndungsausschreibungen und -löschungen unmittelbar in das System eingegeben werden. Der Zentralrechner beim Bundeskriminalamt sorgt dafür, daß die Fahndungskartei in allen bestandführenden Ländern aktualisiert wird, so daß theoretisch ein gesuchter Rechtsbrecher bereits Minuten nach der Ausschreibung - z.B. aufgrund eines Haftbefehls - bei seiner Flucht anläßlich einer Flughafenkontrolle festgenommen werden kann (4). Nicht vergessen werden darf, daß sich diese Schnelligkeit auch zugunsten der Bürger auswirkt. In Sekunden ist die entlastende Information verfügbar, und die polizeiliche Kontrolle ist im Vergleich zu früher nach einem Bruchteil der Zeit vorüber.

Der Bestand im Personenfahndungssystem ist von ca. 116.000 Personen im November 1972 auf ca. 183.000 im Oktober 1982 gestiegen. Dennoch erfolgen die Auskünfte am Datensichtgerät in aller Regel nach weniger als 10 Sekunden. Mehr als ein Drittel aller eingegebenen Festnahmeersuchen können bereits nach einer Woche, mehr als drei Viertel können nach drei Monaten wieder gelöscht werden.

In der Sachfahndung sind nunmehr sämtliche in der Bundesrepublik gesuchten alphanumerisch identifizierbaren Gegenstände erfaßt und bundesweit abfragbar, z.Z. ca. 1,9 Millionen, davon ca. 570.000 Kraftfahrzeuge. Das Leistungsvermögen des Sachfahndungssystems ist z.B. daran zu erkennen, daß etwa 40% aller Ausschreibungen von Kraftfahrzeugen nach einer Woche und etwa 70% spätestens nach drei Monaten wieder erledigt sind.

Ähnliche Veränderungen, allerdings wegen des (noch) nicht so fortgeschrittenen Ausbaustadiums der elektronischen Datenverarbeitung nicht so gravierende, sind in anderen polizeilichen Arbeitsbereichen festzustellen: Personenauskunftssysteme (Aktenhinweissysteme) ersetzen Zentralkarteien, das DV-Verfahren "Daktyloskopie" unterstützt und ersetzt mehr und mehr die konventionellen Arbeitsweisen beim Erkennungsdienst, Falldateien unterstützen die Auswerte- und Recherchearbeit mittels Karteien und anderen herkömmlichen Hilfsmitteln. Ich möchte es bei diesen kurzen Andeutungen bewenden lassen. Auf einige Punkte komme ich im Verlauf dieses Vortrags noch zurück. Im übrigen werden andere Referenten noch auf Einzelheiten näher eingehen, so daß ich nicht zuviel vorwegnehmen möchte.

These 2

"Elektronisierungen" konventioneller Karteien und Abläufe müssen in die Breite ausgebaut werden, damit die daraus erwachsenden Mengen- und Zeitvorteile möglichst weit "vor Ort" genutzt werden können.

Die realisierten bzw. geplanten Anwendungen der elektronischen Datenverarbeitung bei der Polizei umfassen ein breites Spektrum, von dem die bereits angesprochene Fahndung nur eine der Möglichkeiten darstellt, nämlich die 1:1-Übernahme von Karteien. Wie dort sind in Datenbanken Personen registriert, nach denen z.B. gesucht wird, die in Haft sind oder über die Akten geführt sind. Wie auf Karteikarten ist in einem Personendatensatz z.B. niedergelegt, seit wann, durch wen und warum nach einer Person gefahndet wird, wie lange und wo jemand in Haft ist und unter welcher Nummer die Kriminalakte geführt wird. Im Prinzip werden bisherige Strukturen nachgebildet, doch sollte man auch hier - wie schon vorhin ausgeführt - die Bedeutung der Umstellung auf EDV nicht unterschätzen. Man bekommt das Zeit- und das Mengenproblem in den Griff, und bei entsprechender Ausstattung mit Terminals können die Datenbestände anders als herkömmliche Karteien relativ nahe am Ort des polizeirelevanten Geschehens unmittel-

bar genutzt werden. Das "Herrschaftswissen" von Zentralen nimmt tendenziell ab. Das beste Beispiel ist hier der Einsatz von Datenfunkterminals in Streifenwagen der Schutzpolizei oder bei Kontrollen durch Beamte des Grenzschutzeinzeldienstes. Hierdurch entfällt sogar die sonst übliche Übermittlung einer Anfrage per Sprechfunk an die nächste Dienststelle mit Datensichtgerät. Es ist also unabdingbar, Standardfunktionen der polizeilichen Datenverarbeitung, sobald sie zu einer gewissen "Reife" entwickelt sind und ihre Nutzung dezentral erforderlich ist, gezielt "in die Breite" auszudehnen. Nur so können dem einzelnen Schutzpolizeibeamten und kriminalpolizeilichen Sachbearbeiter die, auch bei einfachem "Karteiersatz" erzielbaren, Vorteile der elektronischen Datenverarbeitung unmittelbar vor Augen geführt werden.

These 3

Elektronische Datenverarbeitung bildet nicht nur konventionelle Strukturen und Abläufe ab. Sie schafft darüber hinaus neue Möglichkeiten des Auswertens und Abgleichens sowie der Handhabung und Verknüpfung komplexer Datenbestände.

Auch konventionelle Informationssammlungen bieten mehr als nur reine Auskunftsfunktionen. Herkömmliche Auswertungen finden jedoch ihre Grenzen in den dabei zur Verfügung stehenden praktischen Möglichkeiten und in der endlichen Leistungsfähigkeit des menschlichen Gedächtnisses. Die elektronische Datenverarbeitung schafft nicht nur graduelle Verbesserungen. Sie ermöglicht z.B. nicht nur eine schnellere Erfüllung bestimmter Aufgaben oder eine Verarbeitung und Handhabung größerer Informationsmengen in einem bestimmten Zeitlimit, sondern sie bietet Leistungen, die manuell unter realistischen personellen bzw. zeitlichen Umständen überhaupt nicht erbringbar sind. Ich möchte mich auch hier, da die INPOL-Anwendungen und die taktischen Einsatzmöglichkeiten der elektronischen Datenverarbeitung noch im Detail vorgetragen werden, auf einen Abriß beschränken (5):
Bei der Täterermittlung und der Herstellung von Tatzusammenhängen ist es mit den Mitteln der herkömmlichen Daktyloskopie nicht möglich, z.B. gesicherte Fingerspuren mit sämtlichen abgelegten Einzelfingerabdrücken zu vergleichen. Vielmehr muß man vorher in etwa wissen, in welcher Deliktsgruppe (und damit in welcher Untermenge der Einzelfingerabdrücke) man zu suchen hat. Mit Hilfe der elektronischen Datenverarbeitung kann dem-

gegenüber eine am Tatort vorgefundene und verformelte Fingerspur mit sämtlichen in der Sammlung vorhandenen Einzelfingerformeln verglichen werden. Seit 1977, dem Jahr der Einführung des Systems, bis zum 30.09.1982 wurden so insgesamt 2.560 Spurenverursacher identifiziert.

Auch für die Fallrecherche hat die elektronische Datenverarbeitung neue Maßstäbe gesetzt. Der Modus operandi eines Straftäters läßt sich in eine weit größere Zahl von Tatbegehungs-, Täter- und Opfermerkmalen aufteilen als manuell auswertbar und recherchierbar ist. Die für bestimmte Deliktsbereiche geplanten zentralen Falldateien - die Falldatei Rauschgift wird bereits erprobt - sowie in einigen Ländern verwirklichte Falldateien liefern prinzipiell alle Kombinationen der vorhandenen Daten und erlauben, soweit es die DV-Kapazitäten zulassen, Bereichsauswertungen. So können z.B. Rauschgiftfälle mit unbekanntem Täter hinsichtlich der Merkmale Straftat, Tatzeit, Tatmittel, Begehungsweise usw. den zu bekannten Tätern erfaßten gleichen Merkmalen gegenübergestellt werden, um ggf. eine Zuordnung bereits ermittelter Täter zu unaufgeklärten Fällen vorzunehmen. Zugrunde liegt den Falldateien die kriminologische Grundannahme der Perseveranz (Beibehaltung) von Modus-operandi-Merkmalen.

Ein weiteres Beispiel betrifft die Handhabung und Verknüpfung komplexer Datenbestände aus Akten zu Personen, Institutionen, Objekten und Sachen in bestimmten Ermittlungskomplexen (Verfahren PIOS). So können manuell nicht oder nur durch Zufall erkennbare Sachzusammenhänge und Beziehungen hergestellt werden. Auch hier ist der Fortschritt gegenüber konventionellen Aktenauswertungen nicht mehr nur gradueller, sondern schon qualitativer Natur.

Ich möchte noch auf eine Funktion der elektronischen Datenverarbeitung kurz eingehen, der ein öffentliches Interesse entgegengebracht wird, das meiner Auffassung nach unberechtigt, zumindest aber übertrieben ist. Gemeint ist der systematisierte Datenabgleich, auch "Rasterfahndung" genannt. Auch hier bestehen gegenüber der manuellen Vorgehensweise unbestrittenermaßen völlig neue Möglichkeiten. Es geht, kurz gesagt, darum, große Datenbestände aus dem nichtpolizeilichen Bereich (z.B. Einwohnermeldedaten oder Kundendaten) miteinander oder mit polizeilichen Datenbeständen abzugleichen, um - je nach Ermittlungsziel - Übereinstimmungen oder Nichtübereinstimmungen herauszufiltern oder darum, solche Daten isoliert nach vorgegebenen ermittlungsbedingten Merkmalen stufenweise auszuwerten (6). Bei der Bekämpfung terroristischer Gewalttaten kommt es beispielsweise darauf an, sich im Alltag äußerst unauf-

fällig verhaltende Täter zu ermitteln. Vermutet man dennoch bestimmte Besonderheiten, müssen die Daten großer Personenkreise nach diesen Kriterien hin untersucht werden. Die Möglichkeiten dazu schafft die elektronische Datenverarbeitung. Naturgemäß sind fast ausschließlich unbeteiligte Bürger von den Abgleichmaßnahmen "betroffen", doch trifft es nicht zu, hierin ein unzulässiges "Überwachen" oder "Datensammeln" durch Staatsorgane zu sehen. Diese Daten werden bis auf die "Treffer", die konventionell nachermittelt werden, bei der Polizei nicht menschlich wahrgenommen und nirgends gespeichert. Die Datenträger werden nach Abschluß der jeweiligen Aktion zurückgegeben bzw. gelöscht.

Das Spektrum möglicher Funktionen der polizeilichen Datenverarbeitung ist damit immer noch nicht erschöpfend dargestellt. Die Datenverarbeitung muß - und hier liegt noch ein großer Teil der Aufgaben vor uns - gerade in ihren spezifisch neuen Funktionen mehr der unmittelbaren Unterstützung des Sachbearbeiters dienen als es bisher der Fall ist. Ein weiterer Ausbau "in die Tiefe" ist notwendig. Die Sachbearbeiter werden die elektronische Datenverarbeitung wohl nie als voll anerkanntes Hilfsmittel der Verbrechensbekämpfung akzeptieren, wenn die einzelnen Anwendungen "Inseln" bleiben und Informationen mehrfach - für jedes Verfahren getrennt - eingegeben und überdies auch noch konventionelle Melde- und Berichtspflichten erfüllt werden müssen. Das polizeiliche Datenverarbeitungssystem der Zukunft muß als "Funktionsverbund" gestaltet werden. Es muß neben den bereits bestehenden bzw. vor der Realisierung stehenden Möglichkeiten z.B.

(1) dem Sachbearbeiter - wie bereits in Berlin vorbildlich praktiziert - Vorgangsverwaltungsfunktionen abnehmen (u.a. Tagebuchführung)

(2) Textverarbeitungsmöglichkeiten bereitstellen, um den auch in Zukunft sicherlich nötig bleibenden Papierrückhalt rationell anfertigen zu können

(3) die Einmaleingabe von Informationen ermöglichen, damit z.B. nicht wie heute Daten im Extremfall dreimal erfaßt werden müssen (Personendatei beim Bundeskriminalamt, System PIOS, Landessystem)

(4) die direkten Kommunikationsmöglichkeiten erweitern, indem der Terminal-Terminal-Nachrichtenverkehr (Nachrichtenvermittlungssystem) ausgeweitet wird und

(5) vom reagierenden zum "aktiven" System werden, indem bestimmte "Auslöser" vorher festgelegte Aktivitäten selbständig in Gang setzen (z.B. als Folge eines "Fahndungstreffers" an der Grenze, Meldung an die ausschreibende Dienststelle, ohne daß dies noch gesondert veranlaßt werden muß).

These 4

Elektronische Datenverarbeitung dient nicht nur der Erfassung und Wiedergewinnung alphanumerischer Informationen, sondern optimiert und unterstützt die Polizei auch bei weitergehenden kriminaltechnischen Aufgabenstellungen.

Das Funktionsspektrum der elektronischen Datenverarbeitung bei der Polizei ist immer noch nicht vollständig umrissen. Es handelte sich bei dem bisher Gesagten ausschließlich um Anwendungsbeispiele, bei denen die zugrundeliegenden elektronisch verarbeiteten Informationen aus Buchstaben oder Zahlen bestanden. Die können unmittelbar in den Binärcode übersetzt werden, den der Rechner "versteht". Auch das Daktyloskopie-System, dessen Grundlage eigentlich Muster bzw. Bilder sind, nämlich die Bilder von Fingerabdrücken und -spuren, arbeitet im Prinzip nicht anders, da diese Informationen vor Eingabe in den Rechner in alphanumerische Formeln umgewandelt werden. Ob manuell oder demnächst wahrscheinlich teilautomatisiert (mit Hilfe des Fingerabdruck-Registriersystems - FARS - was wesentlichen Zeitgewinn mit sich bringt) - stets handelt es sich bei der Verformelung, bei der Umwandlung in eine alphanumerische Information, um einen separaten Schritt vor der eigentlichen Datenspeicherung, den das Daktyloskopiesystem selbst nicht durchführt.

Es wird jedoch auch daran gearbeitet, Muster- bzw. Bildinformationen, aber auch phonetische Informationen, direkt computerunterstützt "lesen", erkennen, klassifizieren und zum Zwecke späteren Vergleichs in digitalisierter Form speichern zu lassen. Konkret meine ich den

- rechnergestützten Handschriftenvergleich, d.h. die (Wieder-)Erkennung von Handschriften auf der Grundlage computergestützter Bilder- und Musterverarbeitungstechniken (7)

sowie die

- rechnergestützte Sprechererkennung, d.h. die Identifizierung von Personen (Straftätern) anhand ihrer Stimme (8).

Über die kriminalpolizeiliche Bedeutung dieser Forschungsprojekte brauche ich keine langen Worte zu verlieren. Auch hierzu wird im Verlauf der Tagung sicher noch mehr berichtet werden - z.B. aus Anlaß von Erpressungsfällen - seit jeher bei der Polizei betrieben. Die elektronische Datenverarbeitung bietet insoweit keine prinzipielle Neuerung, sondern sie wirkt unterstützend und optimierend, da bei den konventionellen Verfahrensweisen auch hier das Massen- und damit das Zeitproblem den Wunsch nach Beschleunigung aufkommen ließ. Zugleich wird von der Rechnerunterstützung ein Gewinn erwartet hinsichtlich der Objektivierung, Quantifizierung, Reproduzierbarkeit sowie der Erhöhung der Anzahl von auswertbaren Handschrift- bzw. Sprachmerkmalen.

Die Forschungsprojekte sind noch nicht abgeschlossen, so daß ein Gesamturteil noch nicht möglich ist. Angesichts der Komplexität der Aufgabenstellung müssen jedoch bei den künftigen "serienreifen" Verfahren sicherlich Grenzen einkalkuliert werden. Eine Identifikationssicherheit, wie sie die Daktyloskopie bietet, darf meiner Erwartung nach beim rechnerunterstützten Handschriften- und Stimmvergleich nicht erhofft werden.

These 5

INPOL ist kein Informationssystem des Bundeskriminalamtes, sondern das gemeinsame System von Bund und Ländern. Die elektronische Datenverarbeitung ist und bleibt daher ein wesentlicher Inhalt der polizeilichen Bund-Länder-Zusammenarbeit.

Das Informationssystem der Polizei (INPOL) ist nicht als zentralistisches System konzipiert. Das erkennt man schon daran, daß alle wesentlichen Entscheidungen in der ständigen Konferenz der Innenminister/-senatoren der Länder (IMK) fallen. Vorbereitet werden die Beschlüsse im Arbeitskreis II ("Öffentliche Sicherheit und Ordnung") der IMK, in der Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt (AG Kripo) und einer Vielzahl weiterer Kommissionen und Arbeitsgruppen auf Bund-Länder-Ebene.

Ich weise hierauf so ausführlich hin, um darzustellen, welch großer Koordinierungsaufwand nötig war und ist, damit 11 Bundesländer und das Bundeskriminalamt die vom Grundgesetz vorgeschriebene Zusammenarbeit des Bundes und der Länder in der Kriminalpolizei in die Tat umsetzen.Die Polizeihoheit der Länder hat sich auch auf dem Sektor der elektronischen Datenverarbeitung ausgewirkt. Sechs Länder sowie das Bundeskriminalamt nutzen Hardware der Firma Siemens, 3 Bundesländer (Schleswig-Holstein, Hessen und Rheinland-Pfalz) haben IBM- bzw. IBM-kompatible Hardware im Einsatz.
Zwei Bundesländer (Bremen und das Saarland) betreiben kein eigenes polizeiliches Informationssystem, sondern nutzen die Anlagen des Bundeskriminalamtes. Alle Länder mit eigenen Systemen haben - in unterschiedlichem Umfang - in der Aufgabenstellung zwar ähnliche, jedoch in der Ausgestaltung voneinander abweichende und somit nicht kompatible landesspezifische Verfahren entwickelt. Einheitlich im Verbund, d.h. von sämtlichen Terminals aus bundesweit nutzbar, ist bislang nur die Personen- und Sachfahndung. Weitere Verbundanwendungen (Kriminalaktennachweis, Haftdatei, erkennungsdienstliche Daten) sind in Vorbereitung. Die bislang bestehende Heterogenität in der polizeilichen Datenverarbeitung beim Bund und in den Ländern war im August 1978 Anlaß für die IMK, einen Beschluß zur "INPOL-Neuordnung" zu fassen, der eine stärkere technische und inhaltliche Vereinheitlichung der polizeilichen DV-Systeme und die stärkere Betonung der Rolle des Bundes zum Ziel hatte. Die damals angestrebte Entwicklung ist nicht voll eingetreten. Es gibt dafür sicher mehrere Gründe, einer davon war aber offenbar, daß zumindest einige Länder ihre vormalige Entscheidung, Verantwortung und Kompetenzen, aber auch finanzielle Verpflichtungen, an den Bund abzugeben, nachträglich revidiert haben. Das nunmehr gültige INPOL-Fortentwicklungskonzept vom Juni 1981 verwirft jedenfalls den Gedanken der Vereinheitlichung aller Systeme wieder.
Statt dessen wurde festgelegt, welche DV-Anwendungen Bund und Länder gemeinsam im Verbund planen und betreiben.

Die also auf absehbare Zeit nicht behebbaren Unterschiede zwischen den polizeilichen DV-Systemen in Bund und Ländern erhöhen die Bedeutung solcher Projekte, die zum Ziel haben, die Inkompatibilitäten auf andere Weise zu beheben bzw. zu umgehen. Es muß angestrebt werden, daß zwischen unterschiedlichen Systemen, einschließlich denen verschiedener Gerätehersteller, dennoch ein gegenseitiger Zugriff möglich ist. Zwischen Siemens-Anlagen ist dies technisch durch bestimmte Nachrichtensteuermechanismen im Datenübertragungsnetz bereits möglich. Der nächste Schritt wäre, daß auch von IBM-Terminals aus auf Siemens-Rechner zurückgegriffen

werden kann und umgekehrt. Dies soll mit dem vom Bund und den Ländern Hessen und Rheinland-Pfalz getragenen Projekt SNATCH-POL erreicht werden. Gemäß Projektplan wird es ab nächstem Jahr möglich sein, mit IBM-Terminals in den genannten Ländern Anwendungen (und zwar als erstes das Literaturdokumentationssystem) beim Bundeskriminalamt zu nutzen.

Noch weiter geht das vom Bund und von allen Ländern getragene Vorhaben DISPOL (Digitales Sondernetz der Polizei) (9): Die IMK hat im August 1978 die Rahmenrichtlinien DISPOL beschlossen. Sie bilden die Grundlage der Projektarbeit. Mit DISPOL soll nicht nur das INPOL-Datennetz aufgabenunabhängig und herstellerneutral gestaltet werden (indem die zur Datenübertragung nötige "Intelligenz" aus den Datenverarbeitungsanlagen ins Übertragungsnetz verlagert wird), sondern DISPOL soll die bisher getrennt betriebenen Sondernetze der Polizei

- INPOL-Datennetz
- Fernschreibnetz

in einem Netz vereinen.

DISPOL, dessen endgültige Realisierung allerdings erst gegen Ende dieses Jahrzehnts erwartet werden kann, wird den Benutzern zumindest technisch über ein "vermaschtes" Netz einen "freizügigen" Nachrichtenaustausch mit allen am System beteiligten Datenverarbeitungsanlagen und Endgeräten erlauben. Es wird keine ausschließliche Bindung eines Terminals an einen bestimmten Rechner mehr geben. Die schon lange angestrebte "hierarchiefreie" Datenverarbeitung wird dann in vollem Umfang verwirklicht sein.

These 6

Polizeiliche Datenverarbeitung bedeutet auch Zusammenarbeit mit Informationssystemen anderer Behörden sowie internationale Zusammenarbeit.

Die technischen Möglichkeiten des Zugriffs auf Daten aus nichtpolizeilichen Informationssystemen sind bereits Anfang der 70er Jahre in die INPOL-Planung einbezogen und in das im Dezember 1975 von der IMK verabschiedete "INPOL-Gesamtkonzept" mit aufgenommen worden. Auch wenn nicht mehr alle der damals genannten Bedürfnisse aktuell sind, bleibt als "harter Kern" der Direktzugriff

- beim zentralen Verkehrsinformationssystem ZEVIS des Kraftfahrt-Bundesamtes (KBA)
- beim Bundeszentralregister (BZR) und
- beim Ausländerzentralregister (AZR).

Für den Zugriff beim BZR und AZR sind derzeit die technischen Voraussetzungen noch nicht voll erfüllt. Hinsichtlich des AZR sind auch noch Rechtsfragen offen. Die Direktanfrage beim KBA, und zwar bei der Halterdatei und bei der Datei über entzogene Fahrerlaubnisse, ist bereits in Form eines Pilotprojekts teilweise verwirklicht und wird in nächster Zeit weiter ausgebaut. Umgekehrt wird zur Zeit über die Modalitäten des Zugriffs von Justizdienststellen auf bestimmte Daten im INPOL-Fahndungssystem diskutiert. Gerade das ist ein Beispiel dafür, daß die Polizei nicht nur einseitig Daten fordert, sondern daß die Zusammenarbeit mit anderen Behörden auch in umgekehrter Richtung stattfinden kann, soweit das erforderlich und rechtlich geboten ist.

Internationale Zusammenarbeit mit Hilfe der polizeilichen Datenverarbeitung (10) findet aus rechtlichen Gründen derzeit ausschließlich auf dem Gebiet der Sachfahndung statt. Personendaten sind aus allen on-line-Übermittlungen eliminiert. Es werden vielfältige Formen praktiziert:

- Austausch bzw. gegenseitige Zurverfügungstellung von Listenausdrucken:
  Z.B. geht vierteljährlich eine Liste über gestohlene Kraftfahrzeuge an IP AMMAN.

- Bestandsabgleiche:
  Z.B. wird den USA vierteljährlich ein Band mit dem INPOL-Kfz-Bestand zur Verfügung gestellt.

- Zugriff über Telex-Geräte:
  Seit 1975 sind inzwischen neun europäische Interpolstaaten über insgesamt 10 Telexgeräte berechtigt, automatisch auf den INPOL-Bestand, "gestohlene/unterschlagene Kraftfahrzeuge" zuzugreifen.

- Zugriff über Datensichtstationen:
  Im Gefolge der sogenannten TREVI-Vereinbarungen auf EG-Ebene befürwortete die IMK im November 1978 den gegenseitigen Zugriff ausländischer Polizeidienststellen in europäischen Interpol-Staaten auf folgende Gegenstandsarten der Sachfahndung:

  - Kraftfahrzeuge
  - Blankodokumente
  - Waffen
  - Banknoten.

Realisiert ist diese Form der Zusammenarbeit bislang mit Italien und Belgien.

Weitergehend sind seit ca. 10 Jahren laufende Planungen auf Interpol-Ebene zur Einrichtung eines polizeilichen Informationssystems FIR (Fichier Informatisé de Recherches) mit dem Generalsekretariat in Paris als Zentrale. Hier sollen auch Personendaten international elektronisch übermittelt werden. Das Sitzabkommen zwischen dem Generalsekretariat und der französischen Regierung sowie die jüngst verabschiedeten Datenschutzkonventionen der IKPO-Interpol stellen einen weiteren wichtigen Schritt bei der Lösung hier noch offener Datenschutzprobleme dar. Zur technisch-finanziellen Realisierung des FIR-Systems können allerdings derzeit keine verläßlichen Prognosen abgegeben werden.

Wenn Datenschutzprobleme die internationale Übermittlung von Personendaten problematisch machen, muß die internationale Zusammenarbeit wenigstens dort fortgeführt werden, wo keine Eingriffe in Persönlichkeitsrechte stattfinden können. Über die Internationalisierung der Sachfahndung hinaus sollte deshalb beispielsweise angestrebt werden,

- Daten über Beweismittel zu terroristischen oder schwerkriminellen Straftaten
- kriminaltechnische Daten
- Sprengkörper- und Sprengstoffdaten

in Datenbanken bereitzustellen, auf die international zugegriffen werden kann. Das Bundeskriminalamt ist dabei, entsprechende Vorstellungen auf Interpol-Ebene einzubringen.

These 7:

Die elektronische Datenverarbeitung muß sich stets ihrer tatsächlichen und rechtlichen Grenzen bewußt bleiben, um sowohl innerhalb der Polizei als auch in der Bevölkerung als wertvolles und unerläßliches Hilfsmittel der Verbrechensbekämpfung akzeptiert zu werden.

Bei der Einrichtung und beim Betrieb polizeilicher Informationssysteme muß der Grundsatz "Qualität vor Quantität" eingehalten werden. Durch organisatorische und DV-technische Vorkehrungen (z. B. Erarbeiten von Erfassungskriterien, Datenqualitätskontrollen, regel-

mäßige Prüfungen auf Datenlöschung) ist sicherzustellen, daß Dateien nicht mehr Daten enthalten als ihr Zweck gebietet. Das ist nicht allein ein datenschutzrechtliches Erfordernis. Jedes Auskunftssystem stößt irgendwann an die Grenzen seiner Leistungsfähigkeit, wenn Bestände einen zu großen Umfang annehmen und so inakzeptable Antwortzeiten hinzunehmen sind. Außerdem erfüllt eine Datei nicht mehr ihren Zweck, wenn der Anfrager zwar rechtzeitig Auskünfte bekommt, aber die Auskunftsinhalte nicht die geforderte Relevanz haben.

Diese Erwägungen, und nicht etwa nur Einflußnahmen von außerhalb der Polizei, haben beispielsweise umfangreiche Löschungen von Daten in der Anwendung "PIOS-Terrorismus" nach sich gezogen. Allein eine seit Beginn dieses Jahres laufende Überprüfungsaktion hat hier bisher zur Löschung von über 16.000 Personendatensätzen geführt. Daß solche Überprüfungen jedoch nicht nur neueren Datums sind, sondern permanent praktiziert werden, läßt sich dadurch belegen, daß seit April 1979 insgesamt über 70.000 Personendatensätze in "PIOS-Terrorismus" gelöscht wurden.

Weiter möchte ich auf die Gefahr der Überschätzung elektronischer Auskunfts- und Informationssysteme hinweisen. Selbst die komplexeste Datei kann nur verkürzte Informationen enthalten. Die Personen- bzw. Ermittlungsakte wird daher in absehbarer Zeit ihre Bedeutung nicht verlieren. Es ist davor zu warnen, außer in Situationen, die sofortiges Handeln verlangen (wie z. B. bei einer Festnahme aufgrund eines Fahndungstreffers), polizeiliche Maßnahmen und Entscheidungen - vor allem zu Lasten eines Bürgers - allein auf Auskünfte aus einem DV-System zu stützen. Nicht ohne Grund werden in den INPOL-Anwendungen in irgendeiner Form Aktenhinweise, Aktenzeichen, Fundstellen und ähnliches angegeben. Diesen Informationen ist nachzugehen, sofern es die zeitlichen Umstände erlauben.

Eine künftig immer wirksamer werdende Grenze des Ausbaus polizeilicher Datenverarbeitungssysteme sind angesichts der bekannten Engpässe in allen öffentlichen Kassen die Kosten. Die Zeit der großzügigen Expansion dürfte sowohl in den Ländern als auch beim Bund auf absehbare Zeit vorbei sein. Das verschärft die Anforderungen an künftige Planungen, denn mehr denn je müssen Prioritäten gesetzt werden. Ich habe bereits angedeutet, wo ich diese sehe: in der Dezentralisierung der Standardfunktionen, vor allem aber im Ausbau "in die Tiefe", d. h. in der Unterstützung und Entlastung insbesondere des Sachbearbeiters an der polizeilichen "Front". Nur wenn der unmittelbare Beitrag der elektronischen Datenverarbeitung zur Verbrechensbekämpfung dort ersichtlich ist, wird es politisch durchsetzbar sein, weitere unabdingbare Maßnahmen zu finanzieren.

Zum Schluß noch ein Wort zu dem öffentlich wohl am meisten diskutierten Thema, nämlich "polizeiliche Datenverarbeitung und Datenschutz". Wir werden hierzu noch Vorträge hören. Ich möchte nur folgendes feststellen und damit zugleich mein Referat schließen:
Die Polizei wird sich weiterhin nie den Anforderungen des Datenschutzes verschließen, aktiv am wirksamen Schutz der Persönlichkeitsrechte der Bürger mitzuarbeiten. Die Vielzahl von Regelungen, die bereits in Kraft gesetzt wurden, zeigen, daß dies keine leeren Worte sind. Es wird weiterhin Diskussionen und wohl auch Auseinandersetzungen geben. Ich habe dennoch den Eindruck, daß die Positionen von Polizei und Datenschutz gar nicht so weit voneinander entfernt sind, wie es manchmal scheinen könnte. Die insgesamt sachliche Zusammenarbeit in einer Vielzahl von Einzelfällen und -problemen beweist dies. Was jedoch meiner Meinung nach das Klima unnötig verschärft, ist weniger der Inhalt als die häufig unangemessene Form, in der von seiten des Datenschutzes öffentlich an der Polizei Kritik geübt wird. Die Verwendung juristischer Techniken bei der Argumentation dient in diesem Fall nicht immer der Versachlichung. Es ist zwar richtig, daß Datenschutz eine Rechtsmaterie ist. Wer jedoch ehrlich ist, muß zugeben, daß die hier beziehbaren Positionen in Wirklichkeit keine ausschließlich juristischen Standpunkte sind, sondern auch die gesellschaftspolitische Werthaltung des jeweiligen Betrachters widerspiegeln, z. B. die Auffassung über die Rolle der Polizei in unserer Gesellschaft. Dies bitte ich dann aber auch deutlich zu machen. Wer hier juristische Argumentationstechniken vorschiebt, erhebt einen Verbindlichkeitsanspruch, der ihm nicht zukommt.

Anmerkungen

(1) Vgl. zu den folgenden "historischen Darstellungen" u. a. Holle, R.: Kriminaldienstkunde, III. Teil: Fahndung, Schriftenreihe des Bundeskriminalamtes 1957/3, hrsg. vom Bundeskriminalamt Wiesbaden, S. 22 ff. und Dickopf, P./Holle, R.: Das Bundeskriminalamt, Bonn 1971, S. 91 ff.

(2) Als "Pionier" gilt hier Kaleth, H.: Die elektronische Datenverarbeitung. Ein Beitrag zur Automatisierung der kriminalpolizeilichen Karteiarbeit, Schriftenreihe des Bundeskriminalamtes 1961/3, hrsg. vom Bundeskriminalamt Wiesbaden.

(3) Vgl. u. a. Herold, H.: Organisatorische Grundzüge der elektronischen Datenverarbeitung im Bereich der Polizei. Versuch eines Zukunftsmodells, Taschenbuch für Kriminalisten, Bd. 18, Hilden 1968, S. 240 ff. und später ders.: Künftige Einsatzformen der EDV und ihre Auswirkungen im Bereich der Polizei, Kriminalistik 1974, S. 385 ff.

(4) Gesucht wird ..., Elektronische Datenverarbeitung im Dienste der Verbrechensbekämpfung und -verhütung, hrsg. vom Bundeskriminalamt, 4. Auflage, Wiesbaden 1981, S. 5.

(5) Aktuelle INPOL-Darstellungen: Wiesel, G.: INPOL - Das Informationssystem der deutschen Polizei, ÖVDV 1 (Öffentliche Verwaltung und Datenverarbeitung), S. 71 ff., Gerster, H.: Informationssystem der Polizei (INPOL). Ziele, Grundlagen, Organisation und Bausteine, DVR (Datenverarbeitung im Recht) 1983 (voraussichtl. Heft 4).

(6) Näheres z. B. bei Ermisch, G.: Fahndung und Datenschutz - aus der Sicht der Polizei, BKA-Vortragsreihe Bd. 25, Wiesbaden 1980, S. 70 ff. und Herold, H.: Datenverarbeitung und Menschenrechte, RuP (Recht und Politik) 2/1980, S. 22 ff.

(7) Klement, V./Naske, R. D./Steinke, K. H./Kuckuck, W.: Die Anwendung von Bildverarbeitungs- und Mustererkennungstechniken zur Untersuchung von Handschriften, Kriminalistik 5/1981, S. 199 ff.

(8) Van der Giet, G./Künzel, H. J.: Rechnergestützter Stimmenvergleich für forensische Anwendungen, Kriminalistik 9/1981, S. 341 ff.

(9) Näheres z. B. bei Lotz, P./Funk, W.: DISPOL. Das polizeiliche Nachrichtennetz der 80er Jahre, PTV (Polizei, Technik und Verkehr) 6/1981, S. 223 ff.

(10) Vgl. hierzu auch Wiesel, G.: Ziele, Planungsstand und Teilergebnisse der Datenverarbeitung im Rahmen internationaler Zusammenarbeit, Schlußbericht über die Arbeitstagung "Aktuelle Themen der Datenverarbeitung" vom 18. - 20.02.81 an der Polizei-Führungsakademie Münster, S. 253 ff. und Herold, H.: Informationssysteme in der internationalen Verbrechensbekämpfung (Entwicklungsstand und Perspektiven), Bund Deutscher Kriminalbeamter (Hrsg.): Grenzüberschreitende Verbrechensbekämpfung im Spiegelbild zwischenstaatlicher Verträge und gesetzlicher Regelungen, Düsseldorf 1981, S. 14 ff.

Informationstechnologie der Zukunft

Fritz Krückeberg

Auch wenn mein Thema sich im Bereich der Technologie und Technik bewegt, so ist die Verbindung und Wechselwirkung besonders der Informationstechnologie mit fundamentalen Sachverhalten unseres Lebens und der Gesellschaft doch so bedeutsam, daß ich mich verpflichtet und berechtigt fühle, mit einem sehr breit angelegten Einstieg meinen Vortrag zu beginnen.

A) Entwicklung zur Informationsgesellschaft

Wenn man die technischen Entwicklungslinien im Bereich der Information betrachtet, so sieht man, daß sie eine Teilentwicklung einer umfassenden und allgemeinen Entwicklung darstellen: das zunehmende Entstehen einer Informationsgesellschaft beobachten wir in allen Lebensbereichen als einen äußerst bedeutsamen Wandlungsprozeß von geschichtlicher Dimension. Betrachten wir den Gesamtbereich unserer Volkswirtschaft, so sehen wir, daß die volkswirtschaftlichen Prozesse der Produktion, Umwandlung und Auswertung von Gütern aller Art sich beziehen auf Eingangsgrößen aus Materie (Rohstoffe, Vorprodukte), aus Energie (Elektrizität, Wärmeenergie) und Information (Produktionssteuerung, technische Zeichnungen, Auftragslisten, Fachliteratur, Lizenzen usw.) sowie sich beziehen auf Ausgangsgrößen, nämlich materielle Ergebnisse (fertige Produkte oder Zwischenprodukte) beziehungsweise Ergebnisse in der Form von Energie (bei Kraftwerken, aber auch als Nebenprodukt bei Herstellungsprozessen) und Ergebnisse in der Form von Informationen (Daten, Statistiken, Konstruktionszeichnungen, Gutachten, Analysen, Stellungnahmen, Pläne, Zeitungen, Bücher). Wir können feststellen, daß der Anteil der Information bei diesen Prozessen ständig zunimmt. Dies spiegelt sich wider in der Zunahme nationaler und internationaler Kommunikationsverflechtungen, in der Zunahme der mit Informationen und deren Verarbeitung befaßten Berufe (knowledge worker), in der wachsenden Rolle von Wissen, von Patenten, Lizenzen usw. Die Information besitzt die Bedeutung eines immer wichtiger werdenden Wirtschaftsgutes, neben dem Wirtschaftsgut Energie und den materiellen Wirtschaftsgütern. Bild 1 soll diesen Sachverhalt schematisch andeuten: Wertschöpfung durch Umwandlung und Auswertung von Informationen zu neuen (wertvolleren) Informationen, Wertschöpfung durch Produktion

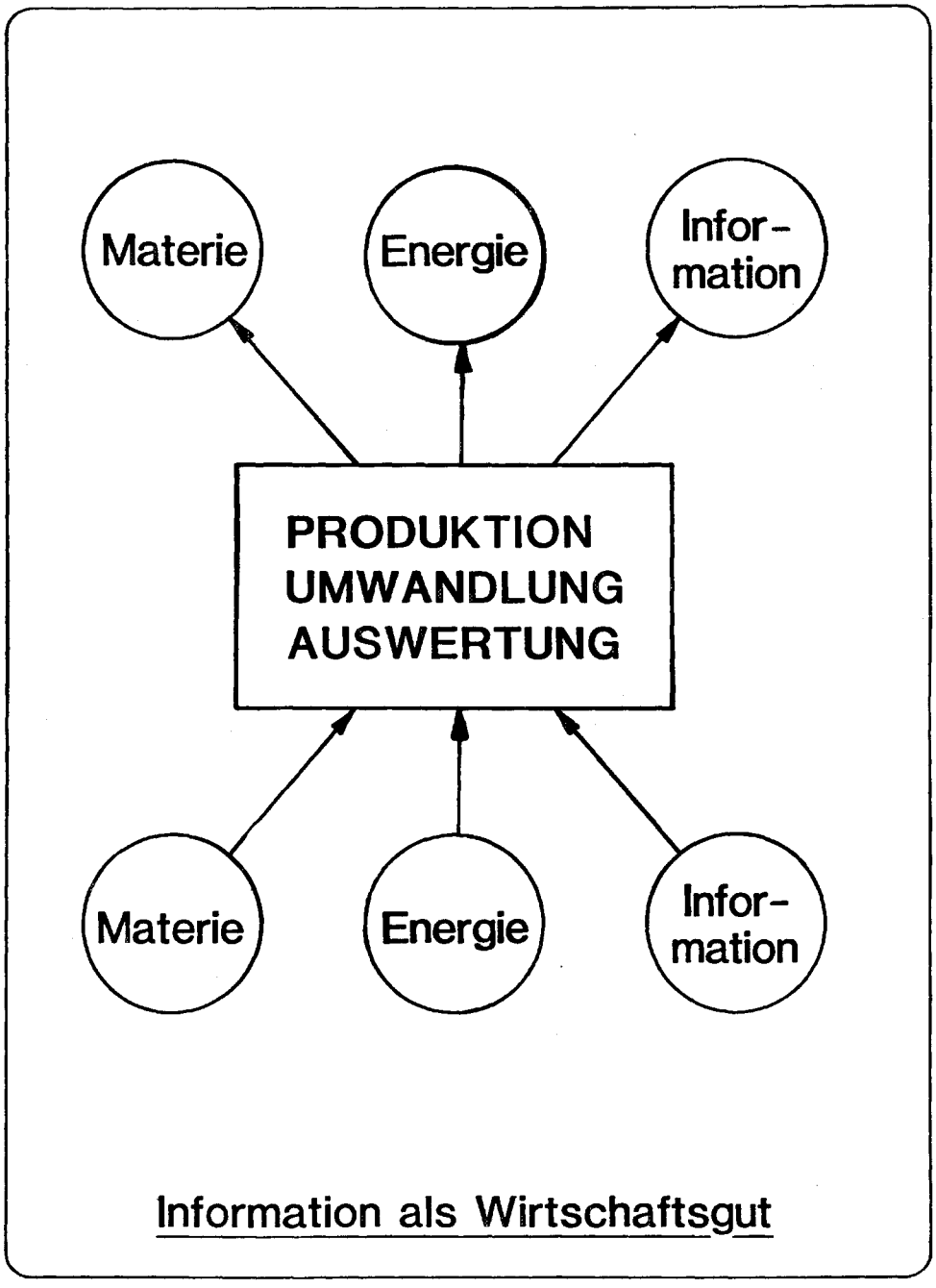
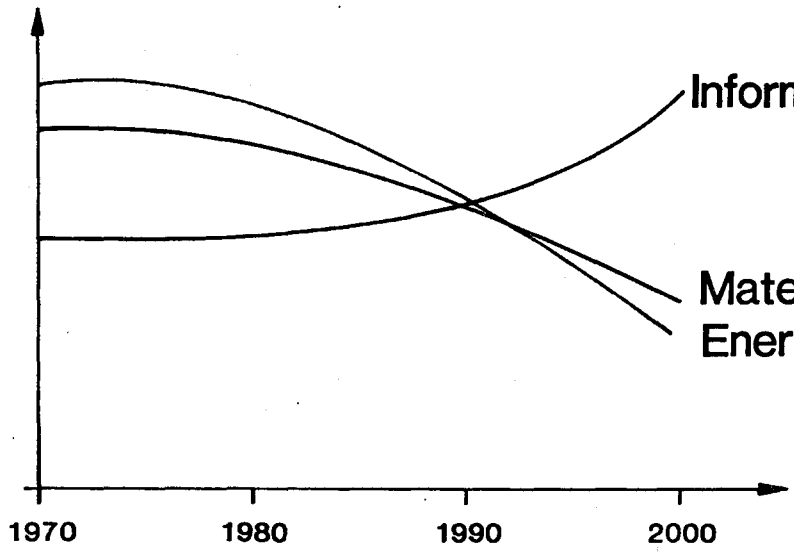

Materie
Energie
Infor-
mation
PRODUKTION
UMWANDLUNG
AUSWERTUNG
Materie
Energie
Infor-
mation
Information als Wirtschaftsgut
GMD

Bild 1



Wandel des Einsatzes von

Materie	Energie	Information

in Geräten des täglichen Lebens

- Auto
- Waschmaschine
- Flugzeug
- Tischrechner
- Heizungsanlage

GMD

Bild 2

materieller Güter unter intensiver Nutzung von Informationen, sind Beispiele dafür, wie das Schema in Bild 1 zu interpretieren ist.

Aber nicht nur der volkswirtschaftliche Produktionsprozeß spiegelt unsere Entwicklung zu einer Informationsgesellschaft wider; wir erkennen dies auch an Geräten des täglichen Lebens, wie in Bild 2 schematisch dargestellt ist. Zum Beispiel beim Auto stellen wir eine Abnahme des Gewichtes (weniger materielle Komponenten), eine Abnahme des Benzinverbrauchs (weniger Energieverbrauch) und eine Zunahme der Nutzung von Informationen (mehr elektronische Anzeigen am Armaturenbrett, mehr elektronische Steuerungstechnik für Motor und Getriebe) fest. Waschmaschinen sind mit energieschonenderen Programmen ausgestattet und erlauben die Durchführung vielfältiger komplizierter Waschprogramme, d. h. der Waschprozeß wird durch mehr Informationen komplexer gesteuert. Moderne Flugzeuge wiegen weniger, besitzen mehr elektronische Prozeß-Steuerung, operieren generell mit mehr Informationen (Landeanflugelektronik, elektronische Triebwerksteuerung usw.) und verbrauchen weniger Kerosin. Tischrechner enthalten immer weniger mechanische Teile, lassen sich immer kleiner und flacher ausführen und verbrauchen immer weniger elektrische Energie. Heizungsanlagen werden zunehmend mit Mikroprozessoren gesteuert, welche detailliertere Informationen nutzen und umsetzen (Außentemperatur, Uhrzeit, Wochentage, Abwesenheitsabschnitte usw.). So lassen sich Energieeinsparungen bis ca. 20 % erreichen, bereits ohne die natürlich zusätzlich sinnvollen wärmedämmenden Maßnahmen. Auch im Straßenverkehr sind die gleichen Prinzipien erkennbar: Durch intensivere Nutzung von komplexeren und zahlreicheren Informationen zur Steuerung des Straßenverkehrs (Computersteuerung der Ampeln, Computersteuerung von Verkehrsumleitungen) werden die Verkehrsströme flüssiger (weniger Standzeiten, kürzere Fahrtzeiten, weniger Unfälle) und können dadurch Straßenneubauten teilweise sich erübrigen. Informationen und deren Verarbeitung und Umsetzung durch Informationstechnik stellen also ein wichtiges Wirtschaftsgut dar, welches zugleich eine teilweise Substitution von Rohstoffen und Energie gestattet. Beim Straßenverkehr läßt sich dieses auf die Formel bringen: mehr Information statt mehr Benzin und Beton. Im Diagramm von Bild 2 ist in der Form von 3 Kurven (die als prinzipielle Darstellung zu verstehen sind) die Entwicklung der Größen Information, Materie und Energie vom Jahr 1970 bis zum Jahr 2000 bezogen auf typische Geräte des täglichen Lebens dargestellt.

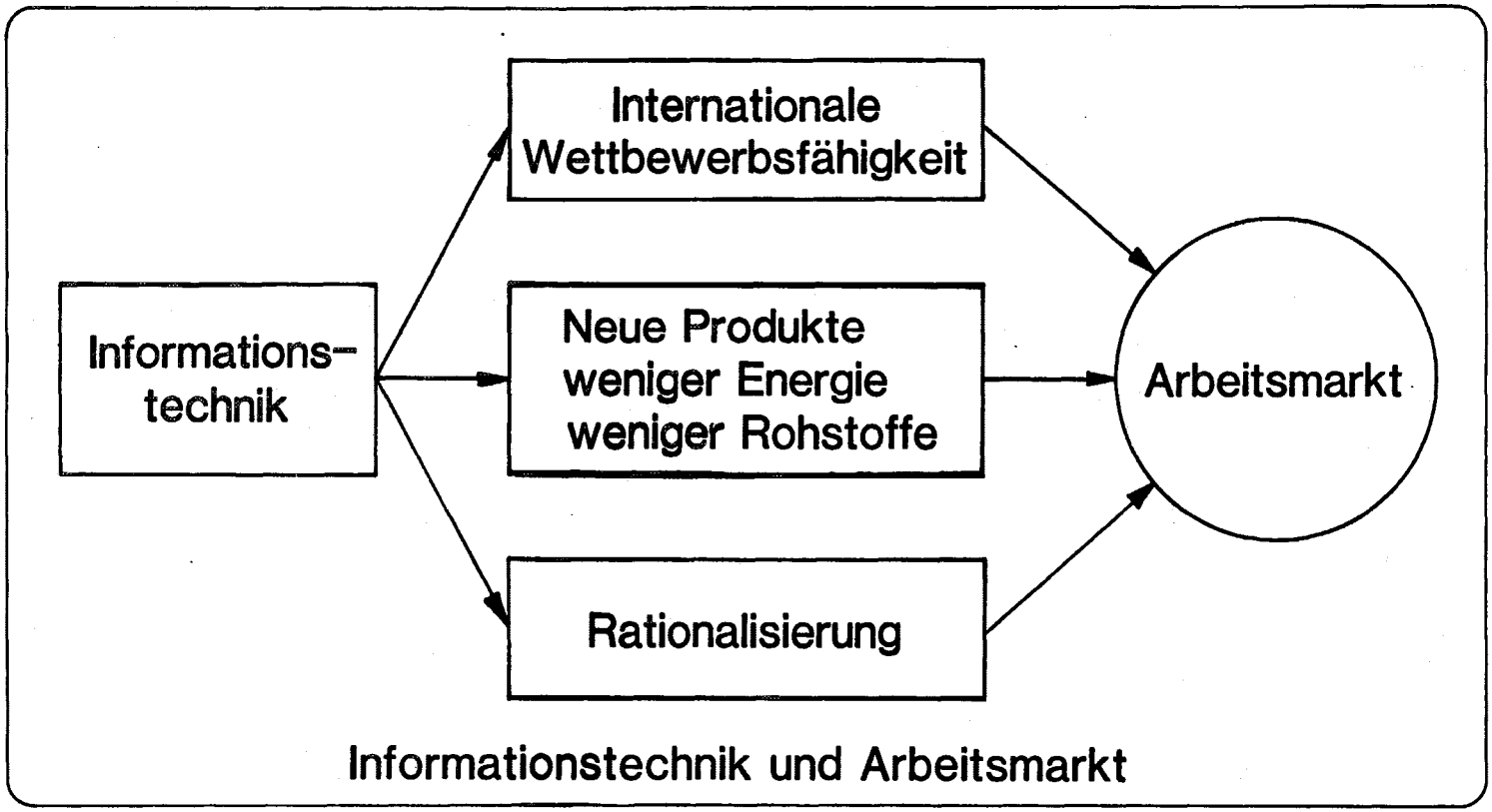

Internationale
Wettbewerbsfähigkeit
Informations-
technik
Neue Produkte
weniger Energie
weniger Rohstoffe
Arbeitsmarkt
Rationalisierung
Informationstechnik und Arbeitsmarkt

Bild 3

Allgemein kann festgestellt werden, daß die Informationstechnik eine Querschnittswirkung entfaltet quer durch alle Bereiche des wirtschaftlichen und gesellschaftlichen Lebens. Keine andere neuere Technologie hat daher eine so weitreichende und vielfältige Bedeutung wie die Informationstechnologie. Allerdings ist diese Entwicklung zur Informationsgesellschaft zugleich verknüpft mit Existenzproblemen. Wir brauchen hier nur an den Arbeitsmarkt zu denken. Wenn wir den Arbeitsmarkt (Bild 3) betrachten, so sehen wir, daß die Informatisierung mehrere gegenläufige Wirkungen auf den Arbeitsmarkt ausübt. Die mit der Einführung der Informationstechnik eintretende Rationalisierung führt, wenn man diese Rationalisierung für sich selbst betrachtet, zu einer Reduktion der Arbeitsplätze. Die Informationstechnik bietet jedoch die Chance, neue Produkte zu entwickeln, die aufgrund des Einsatzes von Informationstechnik weniger Energie verbrauchen und mit weniger Rohstoffen hergestellt werden können. Der verminderte Verbrauch von Energie und Rohstoffen bezieht sich dabei sowohl auf die Anwendungen beim Produktionsprozeß selbst als auch auf die Eigenschaften der Produkte als solche. Darüber hinaus ergeben sich durch die Informationstechnik Möglichkeiten zur Schaffung völlig neuer Produkte, die bisher nicht herstellbar waren. Wenn neue Produkte zu einer Ausweitung der Produktionsmenge insgesamt führen, so kann dies einen positiven Einfluß auf den Arbeitsmarkt ausüben. Man denke etwa an solche Produkte, durch welche neue Dienstleistungen erschlossen werden können. Schließlich und nicht zuletzt wird durch den Einsatz von Informationstechnik die internationale Wettbewerbsfähigkeit positiv beeinflußt, so daß damit die Exportchancen stabilisiert oder gar verbessert werden können und letztlich günstige Einflüsse auf den Arbeitsmarkt wirken. Es ist allerdings nicht zu erwarten, daß die Wirkungen von Rationalisierung, neuen Produkten und internationaler Wettbewerbsfähigkeit insgesamt zu einer Zunahme von Arbeitsplätzen führen. Sie schaffen jedoch insgesamt eine bessere Arbeitsmarktsituation, als sie sich ergeben würde, wenn bei unzureichendem Einsatz der Informationstechnik die internationale Wettbewerbsfähigkeit leiden, der Export zurückgehen und die Chance zur Erschließung neuer Produkte sinken würde.

Die Probleme Informationstechnik und Arbeitsmarkt machen deutlich, daß es erforderlich ist, die informationstechnologische Entwicklung aus einer ganzheitlichen Sicht zu beurteilen. Dieses soll an Bild 4 verdeutlicht werden, welches relevante Bereiche in einem geschichteten Aufbau charakterisiert, die mit der Informationstechnologie in einem engen Zusammenhang stehen.

Gesellschaftliche Willensbildung

Rechtlicher Rahmen

Arbeitsmarkt

Arbeitsorganisation

Arbeitsablauf

Arbeitsplatzbild

Technik selbst

Die Relevanzschichten
der Informationstechnologie

GMD

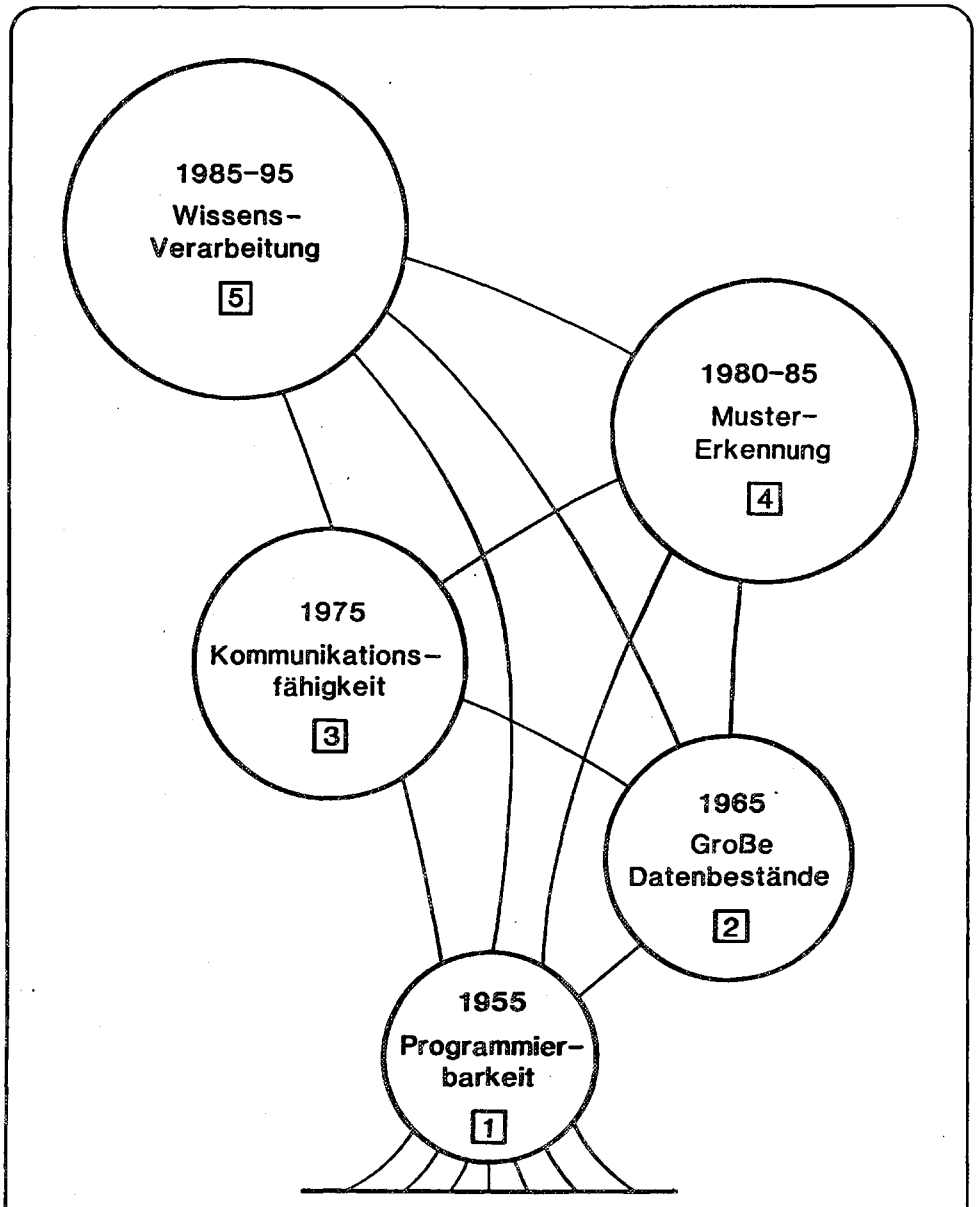
Bild 4

In Bild 4 ist dargestellt, daß neben der Technik selbst bei einer ganzheitlichen Sicht das Arbeitsplatzbild mit zu betrachten ist. Durch die Informationstechnik werden Einflüsse auf die Gestaltung des einzelnen Arbeitsplatzes ausgehen. Aber nicht nur der einzelne Arbeitsplatz, sondern auch der Arbeitsablauf wird durch die Informationstechnik ggf. modifiziert, was schließlich auch Änderungen der Arbeitsorganisation bedeuten kann (man denke etwa an die Diskussion über zentrale und dezentrale Organisationsformen im Licht der Installation von Datenbanken). Schließlich münden alle Änderungen im Arbeitsbereich beim Arbeitsmarkt, über dessen Problematik ich bereits sprach. Betrachtet man bei einer ganzheitlichen Sicht die Informationstechnik noch umfassender, so ergeben sich die relevanten Aspekte des rechtlichen Rahmens, der mit dem Wandel und Wachstum der Informationstechnik einer entsprechenden Weiterentwicklung bedarf. Unter dem rechtlichen Rahmen soll nicht nur der Bereich des Datenschutzgesetzes verstanden werden, sondern die Vielfalt rechtsrelevanter Sachverhalte im Umfeld des Einsatzes der Informationstechnik. Es wird sehr darauf ankommen, daß es der Justiz gelingt, eine adäquate, also weder eine verengte oder noch eine zu isolierte Entwicklung rechtlicher Strukturen und Instrumente zu leisten. Schließlich ist ins Bewußtsein zu rücken, daß die gesellschaftliche Willensbildung die eigentlich entscheidende Relevanzschicht darstellt für die Art und Weise unserer Entwicklung zur Informationsgesellschaft. Wenn auch aus dem Zwang des internationalen Wettbewerbs heraus die Entwicklung der Informationstechnik als schicksalhaft angesehen werden muß, so ist doch das Wie der Gestaltung dieser Technik und der Gestaltung des Arbeitslebens sowie des Lebens überhaupt eine Angelegenheit der gesellschaftlichen Willensbildung, denn es gibt viele Wege und viele alternative Gestaltungsmöglichkeiten für informationstechnische Lösungen. Insofern sind wir hier unseres Glückes Schmied, also nicht Opfer, sondern Herr dieser neuen Technologie.

Zusammenfassend können wir feststellen, daß eine Auseinandersetzung und genauere Befassung mit Informationstechnik für uns alle unumgänglich geworden ist.

B) Hauptentwicklungslinien der Informationstechnik

In Anlehnung an die übliche Vorstellung von "Generationen" informationstechnischer Geräte und Systeme, die stufenartig aufeinanderfolgen und einander überlagern, werden fünf Generationen zu Trägern der Hauptentwicklungslinien. Dieses soll in Bild 5 schematisch dargestellt werden. In Abständen von etwa 10 Jahren haben sich die Leistungsstufen informationstechnischer



Die Evolution der Informationstechnologie

GMD

Bild 5

Systeme zu einem jeweils neuen Leistungsniveau weiterentwickelt, wobei die vorherigen Stufen notwendige Voraussetzungen sind für das Funktionieren der späteren Stufen. Es entsteht so ein Evolutionsschema, dessen innere Verflechtung durch die die Kreise verbindenden Linien in Bild 5 angedeutet sein soll. So begann mit den ersten auf dem Markt befindlichen DV-Anlagen etwa 1955 die Einsatzmöglichkeit programmierfähiger Systeme. Zu nennen sind in diesem Zusammenhang auch die ersten deutschen Nachkriegs-Computerentwicklungen von Zuse (Zuse Z 22), dem als erstem in der Welt der Bau einer programmierfähigen Rechenanlage 1941 gelang. Etwa ab Mitte 1965 besteht die Möglichkeit, große Datenbestände in der Form von Datenbanken zu führen und unter Verwendung programmierfähiger Systeme zu nutzen. Seit 1975 besteht allgemein die Möglichkeit, Computer miteinander zu verbinden (und per Datenfernverarbeitung zu nutzen). Ferner besteht Kommunikationsfähigkeit im Sinne einer Interaktionsfähigkeit des informationstechnischen Systems mit dem Menschen unter Verwendung von Daten, Text, grafischen Informationen und akustischen Informationen (Sprache). Allerdings muß einschränkend hinzugefügt werden, daß 1975 die Fähigkeit informationstechnischer Systeme noch nicht ausreichte, Sprache in der Form frei gesprochener akustischer Sprachsignale oder handschriftliche Notizen zu erkennen. Diese und andere Probleme der Mustererkennung, zu deren Lösung sowohl umfangreiche statistische Methoden als auch ansatzweise Komponenten künstlicher Intelligenz benötigt werden, sollen von den Systemen der 4. Generation gelöst werden. Bereits jetzt gibt es Geräte auf dem Markt, die aus einem Wortschatz von etwa 500-1000 Worten bei gleichbleibendem Sprecher diese erkennen, wenn sie frei gesprochen werden. Auch Handschrift ist bereits sehr weitgehend automatisch analysierbar. Die 4. Generation informationstechnischer Systeme kann mit der Fähigkeit der automatischen Mustererkennung charakterisiert werden; diese wird in diesem Jahrzehnt zunehmend zum Einsatz kommen. Dabei gibt es bereits jetzt interessante Systemlösungen, auf welche ich im nächsten Abschnitt meines Vortrages eingehen werde.

Schließlich kann davon ausgegangen werden, daß es eine 5. Generation informationstechnischer Systeme geben wird, deren weiterentwickelte Leistungsstufen etwa ab 1995 zur Verfügung stehen werden. Diese Systeme sollen mit gespeichertem Wissen durch Einsatz künstlicher Intelligenz sinnvoll operieren können und dadurch dem diese Systeme nutzenden Menschen einen intelligent aufbereiteten Zugang zu Informationen vermitteln als auch eine Interaktion mit dem System auf hoher Intelligenzstufe ermöglichen. Dies bedeutet, daß die Kommunikationsfähigkeit der Systeme der 4. Generation in weiterentwickelter Form für die Systeme der 5. Generation benötigt wird. Auf einer internationalen Konferenz

über japanische Planungen für die Entwicklung von informationstechnischen Systemen der 5. Generation wurden diese nach Meinung der Japaner so dargestellt: Computer der 5. Generation müssen "intelligenter" als die jetzigen Rechnersysteme sein, um sie zu einem besseren Werkzeug, um nicht zu sagen "Gesprächspartner", für den Menschen zu machen. Das schließt ihre Fähigkeit ein, mit dem Menschen in natürlicher Sprache zu kommunizieren und Anweisungen entgegenzunehmen, zu lernen, zu assoziieren und Schlußfolgerungen zu ziehen.

Folgende Leistungsdaten werden bei den Geräten der 5. Generation angestrebt: Datenbankmaschinen mit der Fähigkeit, 500 Millionen beschriebene Seiten DIN A4 zu speichern, 100 Millionen arithmetische Operationen in einer Sekunde auszuführen, eine Milliarde logische Operationen pro Sekunde zu leisten.

Typische Anwendungen der Systeme der 5. Generation sind die maschinelle Sprachübersetzung von natürlichen Sprachen ineinander, automatische Erzeugung von Hintergrundwissen und vielschichtige Nutzungsmöglichkeiten dieses Hintergrundwissens durch den Menschen, Expertensysteme (in denen unter Verwendung von Methoden der künstlichen Intelligenz der besondere Erfahrungsschatz bestimmter Expertenbereiche dem Systemnutzer in aufbereiteter Form als Hilfsmittel zur Verfügung gestellt wird).

Nach diesem Blick auf die Hauptentwicklungslinien sollen nun einige Anwendungsbeispiele geschildert werden.

C) Anwendungsbeispiele

Kehren wir nun zurück zu dem Stand der Informationstechnik heute, wobei ich also mich bewußt beschränke auf solche Techniken, die es bereits gibt und die entweder schon auf dem Markt erhältlich sind oder als Spezialentwicklungen zur Verfügung stehen bzw. in allernächster Zeit zur Verfügung stehen werden.

Sprachauswertung und Stimmenvergleich

Es ist heute möglich, gesprochene Sprache (die z.B. auf einem Tonband festgehalten wurde) auf dem Computer näher zu analysieren. Hierzu können die in den gesprochenen Worten enthaltenen charakteristischen Schwingungsmerkmale der menschlichen Stimme sehr genau herausgefiltert werden. Es ist möglich, gewissermaßen einen "Stimmabdruck" herzustellen, mit dessen Hilfe dann durch Stimmenvergleich, d.h. durch Vergleich mit den Stimmabdrücken gesprochener Worte anderer Sprecher, die Identifizierung etwa eines bestimmten gesuchten

Sprechers möglich ist. Verwendet werden hierzu Methoden der Mustererkennung. Die Methode des Stimmvergleichs ist bereits einsatzfähig, befindet sich jedoch außerdem in intensiver Weiterentwicklung. Hingewiesen sei noch darauf, daß es gelungen ist, charakteristische Merkmale der Stimme durch den Computer zu extrahieren, die auch bei bewußter Verstellung oder Abänderung der Stimme oder bei Störungen durch technische Übertragungsmittel (Telefon) unverändert erhalten bleiben.

Handschriftauswertung und Handschriftvergleich

Es ist möglich, Handschriften in den Computer einzugeben, deren charakteristische Merkmale automatisch zu ermitteln und Schriftproben nach diesen charakteristischen Merkmalen miteinander zu vergleichen. Hierdurch ist es dann in objektiver Weise erreichbar, Schreiber durch ihre Handschriften weitgehend automatisch zu identifizieren. Entsprechende Laborversuche sind bereits sehr weit vorangeschritten, so daß eine praktische Nutzung bald bevorsteht.

Linguistische Textanalyse

In den Texten eines Verfassers treten, wie linguistische Forschungen ergeben haben, bestimmte Wortarten und Wortkombinationen in typischer Häufigkeit auf, werden bestimmte Grammatikanwendungen gern benutzt oder gar bestimmte Grammatikfehler immer wieder gemacht, hat der Satzbau bestimmte charakteristische Eigenheiten. Es ist nun unter Einsatz von Computern möglich, eine dementsprechende linguistische Textanalyse vorzunehmen und charakteristische linguistische Parameter des Verfassers zu ermitteln. Eine derartige Methode linguistischer Textanalyse ist bereits fertiggestellt und kann z.B. zur Identifizierung des Verfassers eines Textes verwendet werden.

Bilderfassung, Bildspeicherung und Bilderkennung

Mit den heute schon sehr weit entwickelten Methoden der interaktiven grafischen Datenverarbeitung ist es möglich, Lichtbilder von Personen auf dem Computer in einem halbautomatischen Verfahren zu vermessen und daraus ermittelte charakteristische Merkmale des Gesichts einer Person in einer Datenbank zu speichern. Soll nun ein vorliegendes Lichtbild identifiziert werden, so wird dieses in gleicher Weise vermessen, die charakteristischen Merkmale werden dann vom Computer errechnet und mit den gespeicherten Merkmalen der Datenbank nach Methoden der Mustererkennung verglichen.

Die auf diese Weise als hinreichend ähnlich erkannten Personenbilder werden mit zugehörigen Angaben dem Benutzer des Systems angeboten. In diesem Zusammenhang sei darauf hingewiesen, daß es äußerst leistungsfähige Techniken zur Speicherung von Bildern marktreif gibt. Besonders hervorzuheben ist hierbei die mit einem Laserstrahl arbeitende Bildplatte, welche übrigens für private Zwecke vor kurzem auf dem deutschen Markt eingeführt wurde.

Aber auch die Bilderfassung für andere Zwecke ist durch die Bildplatte gerade dann in ausgezeichneter Weise gegeben, wenn es sich um große Bildmengen handelt, die nach bestimmten Merkmalen rasch wieder aufrufbar sein sollen.

Die von mir angegebenen Verfahren der Mustererkennung zur Sprachauswertung und zum Stimmenvergleich, zur Handschriftauswertung, zur linguistischen Textanalyse und zur Bilderfassung und Bilderkennung werden in der technisch-wissenschaftlichen Forschungseinheit im Bundeskriminalamt erforscht und entwickelt; sie befinden sich zu einem erheblichen Teil in einer einsatzbereiten bzw. erprobungsbereiten Entwicklungsphase. Aufgrund des Vergleiches zu anderen internationalen Forschungs- und Entwicklungsarbeiten auf dem Gebiet der Mustererkennung, welcher mir aufgrund eigener Kontakte zu derartigen Arbeiten möglich ist, kann ich an dieser Stelle legitimiert zum Ausdruck bringen, daß die im Bundeskriminalamt geleisteten Forschungs- und Entwicklungsarbeiten dem neuesten Stand internationaler Arbeit auf diesem Gebiet entsprechen und im Hinblick auf die hier speziell behandelten Fragestellungen international führend sind.

Kommunikationstechniken

Es stehen heute außerordentlich leistungsfähige Kommunikationstechniken zur Verfügung. Die Möglichkeiten der Datenfernverarbeitung sind ausgereift und erlauben u.a. eine flexible und nahezu entfernungsunabhängige interaktive Kommunikationsverbindung zwischen dem Benutzer und der Datenverarbeitungszentrale. Zu nennen sind insbesondere mobile Stationen, welche mit der Computerzentrale in Verbindung stehen können. Durch Zusammenschaltung mehrerer Bildschirmgeräte, ggf. ergänzt durch eine gleichzeitige akustische Verbindung, sind Fernkonferenzsysteme möglich, die nicht nur mehrere Konferenzpartner über große Entfernung gleichzeitig miteinander verbinden, sondern gleichzeitig die Informationsverarbeitungsleistung und die Zugriffsmöglichkeit zu gespeicherten Daten bieten. Aber auch Konferenzsysteme für eine zeitlich versetzte Beteiligung der Teilnehmer an einer Konferenz sind eine äußerst effektive Alterna-

tive zum Austausch und zur Abstimmung von Informationen. Beispielsweise wird in der Gesellschaft für Mathematik und Datenverarbeitung ein dort entwickeltes Konferenzsystem KOMEX für die täglichen Abstimmungsbelange von über 100 Teilnehmern intensiv genutzt. Eine Erweiterung derartiger computerunterstützter Konferenzsysteme ist vorstellbar durch die Hinzunahme der Übertragung von stehenden und beweglichen, mit Fernsehkameras aufgenommenen Bildern zwischen den Konferenzpartnern. Dies könnte man sich besonders dann als sehr wirksam vorstellen, wenn gleichzeitig eine Ankopplung an ein computergestütztes Bildspeichersystem (Bildplatten) existiert.

Bürosysteme

Die Informationstechnik im Büro befindet sich z.Z. in stürmischer Entwicklung. Immer leistungsfähigere und vielseitigere kommunikationsfähige elektronische Textverarbeitungssysteme werden auf dem Markt angeboten. Das Büro der Zukunft nimmt Gestalt an. Mit der Einführung moderner Bürosysteme ist zugleich die Einrichtung von hausinternen Verbindungsnetzen verbunden. Diese Netze können dann vielseitig verbunden werden. Es sollte zu den Selbstverständlichkeiten gehören, daß bei der Beschaffung von Bürosystemen zugleich an die damit sich anbietenden Kommunikationsmöglichkeiten und Anschlußmöglichkeiten an Großrechner gedacht wird. Wenn diese Kompatibilitätsbedingungen erfüllt sind, bietet sich die Chance zu einem integrierten System der Textverarbeitung, der Textkommunikation und der Interaktion mit großen Computersystemen und Datenbanken. Um die für den Einsatz derartiger Bürosysteme notwendigen ersten Erfahrungen zu gewinnen, befindet sich zum Beispiel im Bundesministerium des Innern ein Feldtest mit einem modernen kommunikationsfähigen Textsystem in Vorbereitung, bei dem die Gesellschaft für Mathematik und Datenverarbeitung als Kooperationspartner beteiligt ist.

Expertensysteme

In jüngster Zeit sind sogenannte Expertensysteme in rascher Verbreitung. Expertensysteme sind auf bestimmte spezielle Fachbereiche ausgerichtete intelligente Auskunftssysteme, die das für diesen speziellen Fachbereich bestehende Wissen und die hierzu bekannten methodischen Erfahrungen, Denkweisen und Handhabungstechniken per Computer vollziehen und so dem Benutzer eine sehr fachspezifische Unterstützung geben. Bekannt geworden sind zunächst spezielle medizinische Diagnosesysteme für besondere Krankheitsbereiche, welche ein besonderes Fachwissen erforderlich machen (z.B. Diagno-

sesysteme für Blutkrankheiten unter Einbeziehung sehr seltener Krankheitsformen). Wesentlich für Expertensysteme ist, daß sie auf eine intensive Interaktion zwischen System und Benutzer angelegt sind. Der Benutzer "unterhält" sich gewissermaßen mit dem System und gelangt in einem Dialog nach und nach zu der speziellen Auskunft, die ihn interessiert. Es liegt auf der Hand, sich Expertensysteme auch in vielen anderen, besondere Spezialkenntnisse erforderlich machenden Einsatzbereichen vorzustellen.

Weitere Anwendungsbeispiele

Die Liste der Anwendungsbeispiele ließe sich erheblich fortsetzen. Genannt seien hier nur Stichworte wie Computersimulation, computerunterstützter Entwurf von Plänen und Planungen, Sprachübersetzung durch Computer, computergestützte Dispositionssysteme usw.

Bevor ich zum nächsten Abschnitt meines Vortrages übergehe, möchte ich darauf hinweisen, daß im weiteren Verlauf dieser Arbeitstagung in einer Arbeitsgruppe die technisch-wissenschaftliche Datenverarbeitung und Forschung im Bundeskriminalamt behandelt werden wird. Dort werden die von mir hier nur kurz dargelegten Arbeiten des Bundeskriminalamtes zur Mustererkennung ausführlicher vorgetragen werden; den hohen fachlichen Qualitätsstand dieser Arbeiten und deren erhebliche praktische Bedeutung möchte ich besonders hervorheben.

D) Formen der Arbeitsorganisation

Moderne informationstechnische Systeme zeichnen sich dadurch aus, daß sie neue Dimensionen der Arbeitsformen des Menschen eröffnen. Dies bedeutet, daß die Arbeitsorganisation ein wichtiges, von der künftigen Informationstechnik nicht abtrennbares Thema ist. Ein zentrales Element der Arbeit des Menschen mit dem informationstechnischen System ist die Kommunikation. Je mehr die Leistungsmerkmale der 4. und 5. Generation informationstechnischer Systeme zum Tragen kommen, um so mehr gewinnt der Dialog des Menschen mit dem System an Bedeutung: Im Dialog des Menschen mit dem System verstärken sich wechselseitig seine spezifischen Fähigkeiten und die des informationsverarbeitenden Systems. Dieser arbeitsorganisatorische Sachverhalt wird in Bild 6 schematisch dargestellt. Wenn der Mensch mit dem System im Dialog steht, so kann er u.a. folgende spezifische Leistungen des Systems nutzen, die von diesem mit großer Präzision, Schnelligkeit und Objektivität erbracht werden können: Selektion, Analyse, Zuordnung, Kombination, Vergleich usw. Die aufgrund dieser Systemleistungen dem Menschen zur Verfügung gestellten Infor-

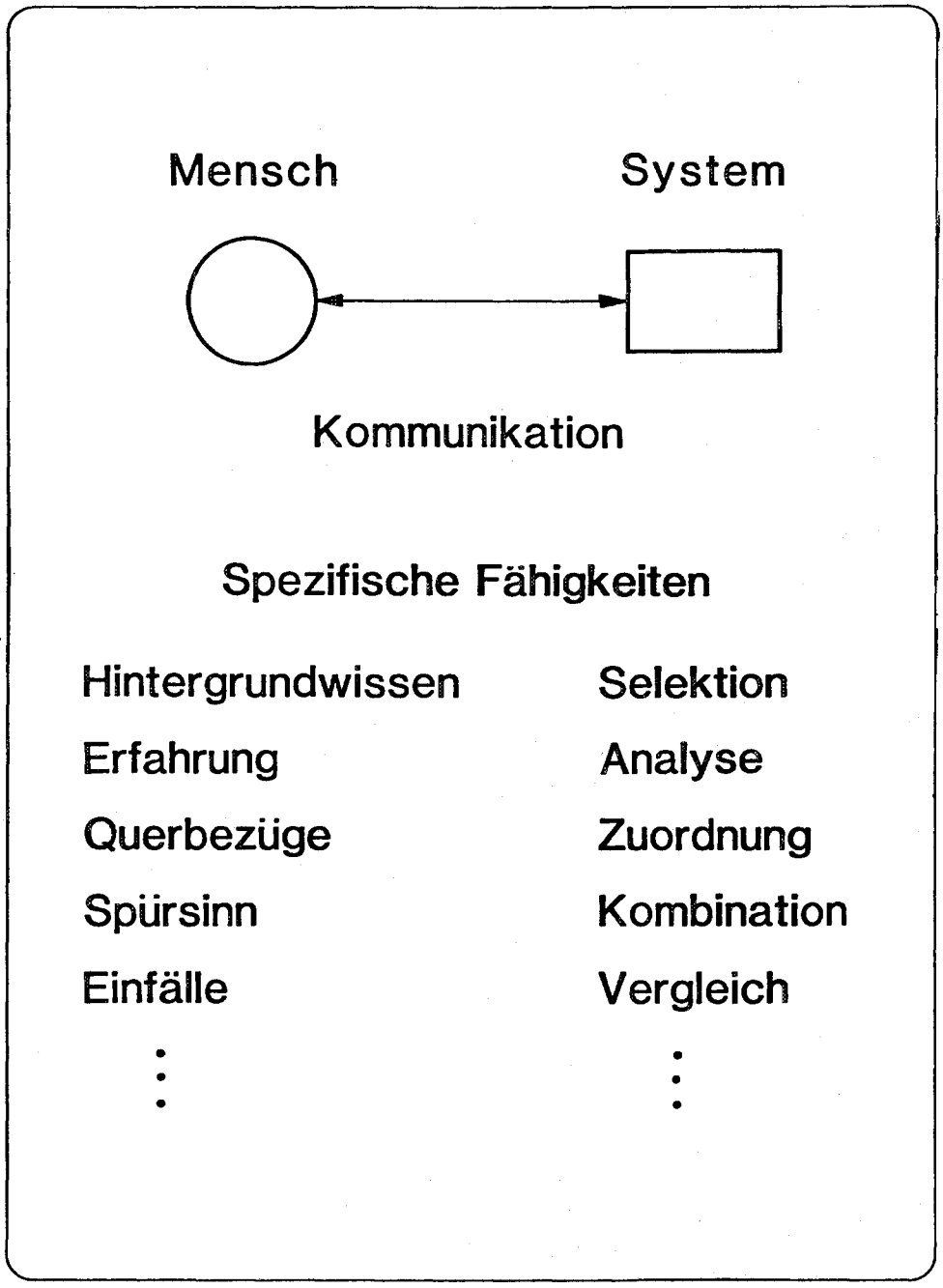

Mensch
System
Kommunikation
Spezifische Fähigkeiten
Hintergrundwissen
Erfahrung
Querbezüge
Spürsinn
Einfälle
Selektion
Analyse
Zuordnung
Kombination
Vergleich
GMD

Bild 6

mationen kann dieser unter Verwendung seines Hintergrundwissens, seiner Erfahrung, unter Ausnutzung ihm bekannter Querbezüge zu anderen Informationen, unter Einsatz seines Spürsinns, seiner Intuition und seiner Einfälle neue Fragen an das System richten und durch die Antworten des Systems Anregungen für neue intuitive Überlegungen bekommen. Deutlich wird an diesem Dialogschema auch, daß das informationstechnische System den Menschen keineswegs ersetzt, dem Menschen also auch nicht seine Verantwortung und seine Entscheidung abnimmt, wohl aber den Menschen wirksam unterstützt und zur Objektivierung des sich für den Menschen ergebenden Bildes einer zu beurteilenden Situation beiträgt.

Für die Arbeitsorganisation ist es ebenfalls von entscheidender Bedeutung, daß die Möglichkeiten der Datenfernübertragung (man denke unter anderem an moderne Glasfaserleitungen) eine Kommunikation über größere Entfernungen und von nahezu beliebigen Orten erlauben. Dies gestattet Mischformen eines zentralen/dezentralen kooperativen arbeitsteiligen Leistungsverbundes der zentral und/oder dezentral installierten Geräte und Einrichtungen. Hierdurch wird die Fragestellung, ob die informationstechnische Leistung zentral oder dezentral erbracht wird, a priori wertfrei. Die Frage, ob eine Leistung zentral oder dezentral erbracht wird, kann dann flexibel nach dem Grundsatz gehandhabt werden, daß eine Leistung jeweils da zu erbringen ist, wo sie der Sache nach und den jeweiligen Umständen nach besonders qualifiziert erbracht werden kann. So ist es beispielsweise vorstellbar, daß bestimmte Leistungen besser oder nur vor Ort zustande kommen und andere Leistungen zentral vollzogen werden, weil sie dort aus organisatorischen Gründen oder aus Gründen der Qualität zweckmäßigerweise erledigt werden.

Die Vielfalt der Gestaltung der Arbeitsorganisation im Hinblick auf moderne informationstechnische Systeme erschöpft sich nicht in der Arbeitsform des Mensch-Maschine-Dialogs und in den verknüpfbaren Alternativen zentraler und/oder dezentraler Aufgabenerledigung. Es gibt vielmehr eine große Vielfalt weiterer arbeitsorganisatorischer Aspekte, die allerdings den Rahmen dieses Vortrages sprengen würden. Als ein weiteres Beispiel zur Arbeitsorganisation soll das Kommunikationsdreieck beschrieben werden. Man stelle sich ein Dreieck vor, an dessen einer Ecke sich ein informationstechnisches System befindet, an jeder der beiden anderen Ecken sitzt je eine Person, die Dreieckskanten bedeuten Kommunikationsbeziehungen. Dann kann man sich folgenden Kommunikationsfluß vorstellen: Eine der beiden Personen ist Fachmann in der Bedienung des informationstechnischen Systems, die andere Person ist Fachmann auf einem bestimmten Sachgebiet. Beide beraten gemeinsam

mit Unterstützung des informationstechnischen Systems einen schwierigen Sachverhalt. Sie schauen gemeinsam auf den Bildschirm des Computers, führen gemeinsam einen Dialog mit dem Computer und führen untereinander ein der Klärung des Sachverhaltes dienendes Gespräch. Das Kommunikationsdreieck ist vermutlich eine besonders zweckmäßige Arbeitsform dann, wenn ein bestimmtes Sachwissen einerseits und ein bestimmtes Wissen über den detaillierten Umgang mit dem informationstechnischen System auf verschiedene Personen verteilt ist.

Generell sollte bei der Einführung informationstechnischer Systeme darauf geachtet werden, daß die Arbeitsorganisation sich stark auf den Menschen und seine Integration in den Arbeitsprozeß ausrichtet. Der Mensch sollte in seiner Rolle durch die Informationstechnik nicht in eine Erstarrung oder Verarmung getrieben werden, sondern umgekehrt Chancen erhalten zu einer flexiblen und dynamischen Arbeitsform auf der Grundlage einer die Kooperation und Kommunikation fördernden Arbeitsorganisation.

E) Einführungsstrategie

Die stürmische Entwicklung der Informationstechnologie erfordert eine umsichtige und zugleich zielstrebige Einführungsstrategie. Es ist zu empfehlen, in zunächst begrenzten Probeinstallationen schrittweise praktische Erfahrungen mit den neuen informationstechnischen Möglichkeiten zu gewinnen und parallel dazu in größerer Breite mit Fortbildungsveranstaltungen, welche ausführliche Erläuterungen konkreter Anwendungsbeispiele enthalten, ein inhaltlich untermauertes Verständnis zu verbreiten. Bei der Durchführung von Erprobungen neuer Techniken ist es wichtig, daß die Anwendungsbasis nicht zu schmal gewählt wird, d.h. es sind sowohl hinreichend viele Anwendungsfälle zu erproben als auch hinreichend viele Personen in den Versuch einzubeziehen. Es ist gewissermaßen eine "kritische Masse" erforderlich, damit die aus einem Versuch hervorgehenden Erfahrungen zugleich einigermaßen repräsentativ sind. Wichtig ist auch eine gute Beratungsbegleitung während der Erprobungsphase. Auftretende Unklarheiten oder Schwierigkeiten können dann durch die begleitenden Berater sofort behoben werden; dies ist entscheidend für die Entwicklung einer guten Akzeptanz des Systems und der Systemleistungen.

Sehr wichtig sind ferner, wie schon gesagt, Fortbildungsmaßnahmen. Die jetzige Arbeitstagung ist dafür ein positives Beispiel. Es ist wichtig, daß alle Anwenderschichten eine solche Fortbildung in hinreichend gründlicher Weise geboten bekommen. Dabei geht es nicht

nur um die Information über technische Systeme, sondern auch um eine Information über allgemeine Zusammenhangsfragen, damit so eine ganzheitliche Sicht sich bei den Anwendern entwickeln kann. Mit einer vordergründigen technischen Information ist es nicht getan. In diesem Zusammenhang möchte ich darauf hinweisen, daß erfreulicherweise eine größere Anzahl von Mitarbeitern des Bundeskriminalamtes Fortbildungskurse im Informatikkolleg der Gesellschaft für Mathematik und Datenverarbeitung Jahr für Jahr besucht haben und auch in diesem Jahr besuchen. Gleichwohl möchte ich anregen, die Fortbildungsmaßnahmen zu verstärken und weiter auszubauen, damit vermieden wird, daß die Leistungen informationstechnischer Systeme lediglich als "schwarze Kästen" empfunden werden können. Dies kann sonst Abwehrreaktionen und Technikfeindlichkeit erzeugen. Aus einer ganzheitlichen Sicht heraus kann der Mensch seine spezifische, ihn fordernde Rolle, auch wenn sie modifiziert ist, wiedererkennen. Erst dann wird für ihn sichtbar, daß er seine Kreativität und seine Verantwortungsbereitschaft weiterhin wirksam wird entfalten können, auch wenn informationstechnische Systeme seine Arbeit unterstützen.

Unter solcher Voraussetzung, ich möchte hier von "Informationskultur" sprechen, können wir der Informationstechnologie der Zukunft positiv und aufgeschlossen entgegengehen.

Literatur

Bunge, Ernst — Kriminaltechnische Forschung mit besonderer Behandlung der Sprecher-erkennung. Vortrag an der ETH Zürich (1979)

Proceedings of International Conference on Fifth Generation Computer Systems. Japan Information Processing Development Center (JIPDEC), Tokio (Oktober 1981)

Spaniol, Otto — Konzepte und Bewertungsmethoden für lokale Rechnernetze. Informatik-Spektrum (September 1982)

Unterberger, — Auf dem Wege zur automatischen Erkennung akustischer Sprachsignale. Angewandte Informatik (Heft 9, 1982)

Zuse, Konrad — Der Computer mein Lebenswerk. Verlag moderne Industrie (1980)

Das INPOL-System - Zielsetzungen und Ausbaustand 1982

Dieter Küster

1. Entstehung des INPOL-Systems

Die Polizei hat seit jeher der Aufgabenerfüllung dienliche Informationen gesammelt und verarbeitet. Für die Verarbeitung wurden und werden teils noch heute Karteien, Listen und Akten benutzt, in denen die Informationen aufbereitet, aufbewahrt und verwaltet wurden. Die Grenzen effektiver ebenso wie ökonomischer Informationshaltung und -auswertung mit solchen einfachen Hilfsmitteln wurden allerdings erreicht, als die Kriminalität mehr und mehr anstieg und in einigen Bereichen sogar Massencharakter annahm.

Mit den Möglichkeiten der Datenverarbeitung, massenhaft anfallende Informationen kompakt zu speichern und zugleich in vielfältiger Weise erschließen zu können, wurden die bisherigen Mengenprobleme bei gleichzeitig effektiverer Auswertbarkeit der Informationssammlungen lösbar. Zudem kamen die Möglichkeiten der Datenfernübertragung den polizeilichen Bedürfnissen besonders entgegen. Die schnelle und sichere Verbreitung und Nutzung aktuellerer und umfassenderer Informationen durch Ferneingabe und Fernabfrage trugen dazu bei, im Fahndungswettlauf mit den Straftätern wieder Schritt zu halten.

Die grundlegende Entscheidung für die gemeinsame Entwicklung der Polizeilichen Datenverarbeitung in Bund und Ländern brachte am 27.01.1972 ein Beschluß der Innenministerkonferenz über die Einrichtung eines "Elektronischen Datenverbundes" zunächst für den Bereich der Fahndung. Zu diesem Zeitpunkt hatte in einigen Ländern und beim Bundeskriminalamt der Aufbau eigener Datenverarbeitungssysteme bereits begonnen bzw. waren Systementscheidungen für die Beschaffung von Datenverarbeitungsanlagen getroffen worden. Die Innenministerkonferenz beschloß deshalb, das Vorhaben auf der technischen Basis eines Verbundsystems zwischen den Datenverarbeitungsanlagen der Länder und des Bundes zu verwirklichen.

Die weiterreichenden Zielsetzungen der Innenministerkonferenz gingen kurze Zeit später in das am 16.06.1972 beschlossene "Programm für die Innere Sicherheit in der Bundesrepublik Deutschland" ein: Danach war ein gemeinsames Informations- und Auskunftssystem für die gesamte Polizei in der Bundesrepublik mit dem Bundeskriminalamt als Zentralstelle zu schaffen, das für die Befriedigung sämtlicher Bedürfnisse der Polizei ausgelegt sein sollte.

Den ersten offiziellen Realisierungsschritt vollzog das Bundeskriminalamt, als am 13.11.1972 mit einer DV-Anlage und 35 angeschlossenen Terminals, die bei Polizeidienststellen an der Grenze, auf dem Flughafen Frankfurt a. Main und im Bundeskriminalamt aufgestellt waren, das Personenfahndungssystem mit dezentraler Abfrage in Betrieb genommen wurde. Dieser "Geburtsstunde" des heutigen INPOL-Systems lagen bereits mehrjährige, unter Beteiligung der Länder betriebene, Vorbereitungen für die Einrichtung eines elektronischen Fahndungssystems zugrunde, so daß bei Betriebsaufnahme schon ein DV-Bestand von rd. 116.000 aktuellen Fahndungsdatensätzen vorhanden war.

Der Kurzname INPOL als Ableitung aus der Bezeichnung Informationssystem der Polizei wurde 1973 eingeführt.

2. Grundlagen des INPOL-Systems

2.1 Konzeptionen für Aufbau und Fortentwicklung

Die organisatorisch-technische Konzeption des polizeilichen Fahndungssystems als Rechner-Verbundsystem war faktisch vorgegeben. In den Jahren nach 1972 schufen Bund und Länder dann die organisatorischen Grundlagen für den Zusammenschluß ihrer DV-Anlagen. Das Verbundsystem wurde erstmals Wirklichkeit, als am 14.10.1974 zwischen den DV-Systemen des Bundeskriminalamtes und des Bayerischen Landeskriminalamtes der Nachrichtenaustausch für die Personenfahndung über Datenfernübertragungsleitungen aufgenommen werden konnte (Siemens-Siemens-Verbund). Kurze Zeit später wurde der Verbundbetrieb mit dem DV-System des Kriminalpolizeiamtes Schleswig-Holstein verwirklicht (Siemens-IBM-Verbund). Zuvor hatte das Bundeskriminalamt am 20.05.1974 die Kraftfahrzeugfahndung als erste Stufe in der Sachfahndung in Betrieb genommen.

Die Fortschritte bei der technischen Realisierung des Fahndungsverbundes lösten bald die Forderung nach einem Gesamtkonzept für das Informationssystem aus. Als Fortschreibung der Aufgabenplanung wurde schließlich am 05.12.1975 von der Innenministerkonferenz das "Konzept für das polizeiliche Informations- und Auskunftssystem" verabschiedet. Das als INPOL-Gesamtkonzept bezeichnete Konzept ist durch die ab 1978 eingetretene Entwicklung als überholt anzusehen. Gleichwohl haben einige der damaligen Ziele und Aufgabenstellungen noch heute Bestand.

Als vorrangiges Ziel galten die Intensivierung und Beschleunigung des überörtlichen Informationsaustauschs, d.h. die bei einer am Verbund beteiligten Dienststelle eingehenden oder bereits vorhandenen Informationen sollten den anderen am Verbund beteiligten Dienststellen bei Notwendigkeit sofort über Stromwege zur Verfügung gestellt werden.

Als Aufgaben des Verbundsystems gab das Gesamtkonzept ferner eine Reihe von schrittweise zu verwirklichenden DV-Anwendungen vor, die im wesentlichen auch heute noch zum Aufgabenspektrum von INPOL gehören.

Als in der Aufbauphase besonders wichtige Vorgaben formulierte das Gesamtkonzept die polizeitaktischen Anforderungen an die DV-Technik, u.a. die grundlegenden Anforderungen an die Sicherheit und Schnelligkeit der Informationsverfügbarkeit, ferner, daß die Informationen für den unmittelbaren Vollzugsdienst ausfallsicher "rund um die Uhr" abrufbar sein müssen.

Mitte 1978 unternahm die Innenministerkonferenz den Versuch, das gesamte INPOL-System neu zu ordnen und inhaltlich und technisch zu vereinheitlichen. Die damaligen Vorschläge des Bundeskriminalamtes, die auf eine Ablösung des Verbundsystems durch ein vom Bund neu zu errichtendes, zentral geplantes und zentral organisiertes Gesamtsystem gerichtet waren, verfielen in der von Ende 1979 bis Mitte 1981 andauernden Prüfung der Ablehnung.

Am 12.06.1981 verabschiedete die Innenministerkonferenz dann

- das Konzept für Fortentwicklung des polizeilichen Informationssystems INPOL

und - darauf basierend -

- das Konzept für Aufbau und Führung des Kriminalaktennachweises (KAN).

Wenige Monate vorher hatte die Innenministerkonferenz am 23.01.1981 die "Richtlinien für die Errichtung und Führung von Dateien über personenbezogene Daten beim Bundeskriminalamt" verabschiedet, denen wegen der Bindungen für das Bundeskriminalamt mittelbar auch die Rolle einer Rahmenvorschrift für das INPOL-System zukommt.

Das Fortentwicklungskonzept spricht die ausdrückliche Widmung aus, daß das Gesamtsystem vorrangig der Unterstützung der Verbrechensbekämpfung zu dienen habe. Dementsprechend enthält das neue Konzept folgende Forderungen und Organisationsprinzipien:

- INPOL enthält alle bei den zuständigen Polizeidienststellen des Bundes und der Länder angefallenen einschlägigen Daten der Verbrechensbekämpfung und macht sie für weitere Ermittlungen verfügbar.

- Das Gesamtsystem besteht aus den Teilen INPOL-Bund und INPOL-Land, d.h. den Systemen des Bundes und der Länder.

- Zu INPOL-Bund (mit der Wirkung zentraler Speicherung der Daten beim Bundeskriminalamt) gehören:
  - -- der Kriminalaktennachweis
  - -- die Personenfahndung
  - -- die Haftdatei
  - -- die Sachfahndung
  - -- die erkennungsdienstlichen Daten
  - -- die zentralen Aktenerschließungs- und Spurendokumentationssysteme und Falldateien für Straftaten von bundesweiter Bedeutung
  - -- zentrale Tatmittelnachweise für bestimmte Kriminalitätsbereiche.

- Die Länder können ihre in INPOL-Bund eingespeicherten Daten auch jeweils in ihren INPOL-Land-Systemen speichern. Eine Parallelspeicherung von INPOL-Bund-Daten bei allen Ländern ist nur bei der Fahndung zulässig.

- INPOL-Land umfaßt Datenbestände, die jeweils von dem Land gespeichert werden, in dem sie angefallen sind, und zwar

-- Modus-operandi-Daten zu Personen und Fällen

-- Folgedaten zu Personen, die in INPOL-Bund erfaßt sind

-- Folgedaten zu Fällen mit unbekannten Tätern.

- INPOL-Bund-Rechner werden vom Bund, INPOL-Land-Rechner vom jeweiligen Land geplant, installiert, programmiert, betrieben und unterhalten.

- Die Verbundprogramme werden zwischen Bund und Ländern abgestimmt.

2.2 Technische Ausgestaltung

Alle DV-Systeme des Verbundes unterliegen im Prinzip gleichartigen Aufgabenstellungen. Die polizeitaktischen Anforderungen an die DV-Technik sind für alle DV-Systeme weitgehend identisch, lediglich das polizeiliche Aufgaben-Soll differiert aufgrund der Aufgabenteilung zwischen INPOL-Bund und INPOL-Land.

Die Autonomie der im Verbundsystem zusammenwirkenden Partner läßt es dabei zu, daß Bund und Länder das jeweilige Aufgabenspektrum mit systemtechnisch verschiedenen Betriebsmitteln realisieren. Die Länder Baden-Württemberg, Bayern, Berlin, Hamburg, Niedersachsen, Nordrhein-Westfalen und das Bundeskriminalamt betreiben Siemens-DVA'n, die Länder Hessen, Rheinland-Pfalz und Schleswig-Holstein hingegen IBM- oder IBM-kompatible DVA'n. Nur die Länder Bremen und Saarland haben für INPOL-Aufgaben auf eigene DV-Systeme verzichtet und benutzen im Einvernehmen mit dem Bund das BKA-System.

Im Verbundsystem werden somit Datenverarbeitungsanlagen verschiedener DV-Hersteller - aber auch desselben Herstellers - mit unterschiedlicher Hard- und Systemsoftware und daher z.T. systemimmanent inkompatibler DV-Technik eingesetzt. Die Verschiedenartigkeit der eingesetzten DV-Technik hat deshalb regelmäßig die Konsequenz, daß alle Systembetreiber für die gleichartigen DV-Anwendungen eigene, systemspezifische Anwendungsprogramme entwickeln müssen.

Der Nachrichtenaustausch im Gesamtsystem funktioniert dann reibungslos und störungsfrei, wenn sich alle angeschlossenen DV-Systeme an den Schnittstellen gleich verhalten. Das gleiche Systemverhalten wird deshalb über Schnittstellenabsprachen gewährleistet, die in den sogenannten Verbundkonventionen niedergelegt sind. In den Verbundkonventionen werden Vereinbarungen für den Nachrichtenaustausch zwischen den DV-Systemen getroffen, mit denen z.B. die einzelnen DV-Anwendungen strukturell und inhaltlich definiert, die Bestandsführung für die Daten aus den DV-Anwendungen festgelegt und die Abläufe des gesamten Nachrichtenaustausches zu diesen DV-Anwendungen, d.h. Eingaben, Veränderungen, Löschungen, Abfragen, einzeln verbindlich geregelt werden.

In dem Verbundsystem sind die Rechner der Länder mit dem BKA-System in einem sternförmigen Leitungsnetz gekoppelt. Das BKA-System nimmt als Zentrale Datenverarbeitungsanlage die Koordinierungsaufgaben wahr. Der Zentralrechner steuert den Verbundbetrieb technisch, empfängt Nachrichten, verteilt Nachrichten, gewährleistet die Synchronität der bei den DV-Systemen der Länder parallel geführten Bestände und gibt Bestandsauskünfte.

Bei den Polizeidienststellen in Bund und Ländern sind z.Z. rund 2.500 Terminals installiert. Dabei handelt es sich überwiegend um Datensichtgeräte, aber auch um Fernschreib- und Telexgeräte und um Datenfunkgeräte. Die Terminals der Länder bzw. des Bundes sind wiederum prinzipiell in sternförmigen Leitungsnetzen jeweils dem DV-System des betreffenden Landes bzw. des Bundeskriminalamtes angeschlossen. Zur Erhöhung der Betriebssicherheit werden die Leitungsnetze unter Einsatz von Netzknotenrechnern zusätzlich vermascht. Die Fortentwicklung der Übertragungstechnik hat es darüber hinaus ermöglicht, die Terminals wahlweise auch mit anderen DV-Systemen zu verbinden. Z.Z. betreibt das Bundeskriminalamt in Abstimmung und z.T. Kostenteilung mit den Ländern ein Datennetz von rd. 10.000 km Länge mit 1.024 Datensichtgeräten, darüber hinaus 220 Telexgeräte und 158 Datenfunkgeräte.

2.3 Der Begriff INPOL

Während der Begriff INPOL in der Öffentlichkeit für die gesamte Datenverarbeitung bei der Polizei gebraucht wird, ist doch anzumerken, daß die polizeilichen Informationssysteme der Länder eigene Namen bzw. Kurzbezeichnungen führen. Tatsächlich ist die Definition des Begriffs INPOL uneinheitlich und streitig, bereitet die Abgrenzung selbst den Experten immer wieder Schwierigkeiten.

Eine weite Begriffsbestimmung versteht unter INPOL die Gesamtheit der in Vollzug der gemeinsamen Aufgabenplanung in den DV-Systemen der Länder und des Bundes realisierten und zu realisierenden DV-Anwendungen, unbeschadet der systemspezifischen Ausgestaltung und etwaigen inhaltlichen Ergänzungen. Diese Interpretation berührt damit allerdings das "Selbstverständnis" der eigenhändigen Ländersysteme.

Der weiten Begriffsbestimmung steht die enge Begriffsbestimmung gegenüber, daß INPOL nur den Teil der gemeinsamen Aufgaben umfaßt, der im Rechner-Verbundbetrieb abgewickelt wird oder abgewickelt werden soll und somit in den Verbundkonventionen beschrieben ist oder wird. INPOL wäre danach lediglich die Summe des vereinbarten Nachrichtenaustausches zwischen den Rechnern des BKA und der Länder. Diese enge Definition würde die DV-Anwendungen PIOS, SPUDOK und COD aus dem INPOL-Aufgabenspektrum ausklammern, weil sie unmittelbar im BKA-System realisiert sind und ihr Betrieb im Rechner-Verbund nicht geplant ist. Ebenso würden dann auch die Landesaktennachweise und die Modus-operandi-Systeme der Länder nicht zu INPOL zählen.

Zwischen diesen Extrempositionen vermittelt die auch durch das INPOL-Konzept gestützte pragmatische Begriffsbestimmung, daß INPOL ohne Berücksichtigung der Art der dv-technischen Realisierung alle in der gemeinsamen Aufgabenplanung genannten, der Verbrechensbekämpfung dienenden DV-Anwendungen, unbeschadet der systemtechnischen Ausgestaltung, umfaßt.

3. Die Anwendungen des INPOL-Systems

Der Ausbaustand des Verbundsystems beschränkt sich bis heute noch auf die Personen- und Sachfahndung, während die Realisierung in mehreren Ländersystemen und im BKA-System bereits weiter fortgeschritten ist. Um hierüber einen Überblick zu geben, müßten eigentlich alle DV-Systeme des Bundes und der Länder mit ihren heutigen Anwendungen vorgestellt werden. Der gegebene Zeitrahmen läßt dies jedoch nicht zu. Statt dessen wird die Aufgabenplanung für INPOL im Rahmen des Fortentwicklungskonzeptes dargelegt und neben einer kurzen Erläuterung der Anwendungen jeweils der Realisierungsstand aufgezeigt werden. Dabei wird darauf verzichtet, die Inhalte der Anwendungen aufzulisten, die einzelnen Speicherfristen aufzuführen und die bestehenden Zugriffsregelungen zu nennen. Hierzu soll lediglich auf die für alle Anwendungen erlassenen Errichtungsanordnungen bzw. Feststellungsanordnungen des Bundeskriminalamtes hingewiesen werden, in denen die Einzelregelungen niedergelegt wurden.

3.1 INPOL-Bund-Anwendungen

3.1.1 Fahndung

Die Anwendungen Personenfahndung und Sachfahndung stellen - jede für sich - eine Reihe gleichstrukturierter Auskunftsdateien dar, die jeweils eigenen Fahndungszwecken, nämlich der Festnahme, der Aufenthaltsermittlung oder der Beobachtung von Personen bzw. der Sicherstellung, Einziehung oder Beobachtung von Sachen dienen. Gegenstand von Fahndungsausschreibungen sind die von Polizei-, Justiz- oder berechtigten Verwaltungsdienststellen in Strafverfahren oder in anderen behördlichen Verfahren gestellten Mitfahndungsersuchen, die sich in der Regel an alle Polizeidienststellen richten. In der Personenfahndung werden z.Z. ca. 200.000 Personen geführt, die Sachfahndung enthält ca. 2.000.000 Gegenstände.

Die Datenbestände der Personen- und Sachfahndung werden bei den Verbund betreibenden Ländern parallel gespeichert. Die Sachfahndung bedarf noch einer Optimierung des seit 1974 unveränderten DV-Verfahrens. Ein DV-Verfahren für die Fahndung nach nicht durch alphanumerische Kennzeichnungen wiedererkennbaren Gegenständen (nichtnumerische Sachfahndung) befindet sich in Vorbereitung.

3.1.2 Kriminalaktennachweis

Die Anwendung Kriminalaktennachweis wird als Kernstück der INPOL-Fortentwicklung durch das KAN-Konzept konkret mit ihrer Aufgabenstellung und mit detaillierten Vorgaben über Inhalte, Aufbau und Nutzung beschrieben.

Gegenstand des Kriminalaktennachweises sind die bei den Polizeidienststellen der Länder und des Bundes geführten Kriminalakten, in denen die im Zuge von Ermittlungsverfahren oder aus Anlaß anderer polizeirelevanter Ereignisse angefallenen, für künftige Verfahren bedeutsamen personenbezogenen Erkenntnisse aktenmäßig gesammelt werden. Es handelt sich in erster Linie um eine Auskunftsdatei, mit der der Erkenntnisstand der Sachbearbeiter vor Ort für die Bearbeitung anhängiger Ermittlungsverfahren verbessert werden soll. Wegen der überwiegend dienststellenbezogen angelegten Kriminalaktensammlungen fehlt der Polizei seit langem eine schnelle Auskunftsmöglichkeit zur Erschließung der bei anderen Polizeidienststellen vorhandenen Erkenntnisse.

Das KAN-Konzept unterteilt allerdings die Gesamtmenge der vorhandenen Kriminalakten nach der Bedeutung der Erkenntnisse für die Bearbeitung überregionaler Straftaten und macht hiervon die Führung im Kriminalaktennachweis und damit die bundesweite Verfügbarkeit der Aktenfundstellen für alle Polizeidienststellen abhängig.

Im einzelnen enthält es folgende Bindungen für die Errichtung des Kriminalaktennachweises:

- Der KAN als Verzeichnis der beim Bund und den Ländern nach den "Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen" in Fällen schwerer oder überregional bedeutsamer Straftaten über Beschuldigte und tatverdächtige Personen angelegten Kriminalakten gibt nur über folgende Daten Auskunft:
  - -- rechtmäßige und sonstige Personalien
  - -- Kriminalaktennummer(n), aktenführende Dienststelle(n) sowie Aktenaussonderungsdatum
  - -- ggf. Kurzhinweise auf das Vorhandensein von aktuellen Haftnotierungen und erkennungsdienstlichen Daten.
- Schwere Straftaten im Sinne des KAN-Konzepts sind
  - -- alle Verbrechen und zusätzlich
  - -- die in § 100a StPO aufgeführten Vergehen.

- Als überregional bedeutsame Straftaten skizziert das KAN-Konzept stichwortartig Delikte, bei denen bestimmte, dem Kriminalpolizeilichen Meldedienst entlehnte Kriterien gegeben sind:
  - -- gewohnheits-, gewerbs- oder bandenmäßige Begehung
  - -- Triebtäterschaft
  - -- planmäßige überörtliche Begehung
  - -- Verfolgung extremistischer Ziele
  - -- Mitführen von Schußwaffen
  - -- internationale Betätigung
  - -- erneute Straffälligkeit des Verdächtigen außerhalb des Wohn- oder Aufenthaltsbereichs.

Kriminalakten von Beschuldigten und tatverdächtigen Personen, deren Delikte nicht unter die KAN-Kriterien fallen, werden also nicht im KAN, sondern ggf. nur in den Aktennachweissystemen der jeweiligen Länder registriert. Die Aktenfundstellen stehen dann zwar den Polizeidienststellen des betreffenden Landes, nicht jedoch denen anderer Länder für Direktauskünfte zur Verfügung.

Der Kriminalaktennachweis soll im Verbund betrieben werden, ist aber noch nicht realisiert. Die zuständigen Gremien bereiten z.Z. die Realisierungsgrundlagen durch Überarbeitung des Manuals INPOL 3/4 (Handbuch der Verbund-Konventionen) vor. Die schrittweise Einführung durch Aufnahme des Nachrichtenaustauschs mit den ersten Ländern ist im dritten Quartal 1983 zu erwarten. Soweit möglich ist auch geplant, nach KAN-Kriterien selektierte Bestände der Länder zu übernehmen.

Das Bundeskriminalamt hatte seit 1975 den Aufbau des seinerzeit für das INPOL-System vorgesehenen zentralen Personenindex in Angriff genommen und in den Folgejahren einen Bestand von ca. 2.000.000 Personalien mit Aktenhinweisen erfaßt. Nunmehr ist vorgesehen, diesen Bestand nur als Aktennachweis des Bundeskriminalamtes vorübergehend weiterzuführen und den KAN-Bestand des BKA aus eigenen Ermittlungsverfahren am aktuellen Fall aufzubauen.

3.1.3 Haftdatei

Die Anwendung Haftdatei erfaßt gem. § 4 BKA-Gesetz die Personen, die aufgrund richterlich angeordneter Freiheitsentziehung in Justizvollzugsanstalten einsitzen. Die Haftdatei erfüllt einerseits die Aufgabe, Fahndungsausschreibungen nach Personen unbekannten Aufenthalts, die sich jedoch an anderen Orten in justitiellem Gewahrsam befinden, zu vermeiden. Die andere Aufgabe besteht darin, Auskünfte über Haftzeiten zu geben, um bei neuen Verdachtsfällen Anhaltspunkte für Alibiüberprüfungen zu gewinnen.

Die Haftdatei wird im Verbund betrieben und voraussichtlich zusammen mit dem Kriminalaktennachweis bundesweit eingeführt werden. Bisher nutzen sechs Bundesländer im Direktanschluß die zentrale Haftdatei des Bundeskriminalamtes, in der z.Z. ca. 27.500 aktuelle Notierungen gespeichert sind. Die anderen fünf Bundesländer führen z.T. eigene Haftdateien in ihren Landessystemen.

3.1.4 Erkennungsdienstdatei/Daktyloskopiedatei

Die Anwendung Erkennungsdienstdatei enthält künftig den Nachweis über solche Personen, die nach § 81b StPO oder entsprechenden anderen Gesetzesvorschriften bei den Polizeidienststellen durch Abnahme von Fingerabdrücken, Anfertigung von Lichtbildern und Aufnahme der Personenbeschreibung erkennungsdienstlich behandelt werden.

Die Erkennungsdienstdatei wird ebenfalls im Verbund betrieben und voraussichtlich zusammen mit dem Kriminalaktennachweis und der Haftdatei eingeführt werden. Nach Einführung wird sie mit der beim Bundeskriminalamt bereits bestehenden zentral geführten Daktyloskopiedatei gekoppelt werden.

Die Daktyloskopiedatei hat die Aufgabe, bereits erkennungsdienstlich behandelte Personen bei Neuauftreten anhand ihrer Fingerabdrücke wiederzuerkennen und zu identifizieren, bei Vorliegen daktyloskopischer Tatortspuren ggf. solche Personen auch als Tatverdächtige zu ermitteln und bestehende Tatzusammenhänge bei Straftaten mit unbekannten Tätern erkennen zu lassen. Grundlage bildet das beim Bundeskriminalamt und den Landeskriminalämtern eingeführte Bund-Länder-System zur Klassifizierung von Fingerabdrücken.

Das im BKA-System realisierte DV-Verfahren Daktyloskopiedatei ist vorrangig eine Rechercheanwendung und ermöglicht es, den Prozeß des Recherchierens im Datenbestand erheblich zu beschleunigen und ergebnissicherer zu gestalten.

Von den beim Bundeskriminalamt vorhandenen ca. zwei Millionen Fingerabdruckblättern ist etwa ein Drittel erfaßt, davon wiederum ein Drittel in dem für die Spurenrecherche erforderlichen Umfang. Die Nutzung der Daktyloskopiedatei ist so organisiert, daß das Bundeskriminalamt für die Personenidentifizierung zuständig ist und die Aufgabe der Spurenrecherche den Landeskriminalämtern obliegt. Die Landeskriminalämter sind deshalb direkt mit Datensichtgeräten für die Eingabe des Rechercheauftrages und Druckern für die Ausgabe der Rechercheergebnisse an das BKA-System angeschlossen.

3.1.5 Zentrale Falldateien

Das INPOL-Fortentwicklungskonzept weist den für die Unterstützung der Verfolgung und Aufklärung von Straftaten wichtigen Bereich der Falldateien, in der Konzeptterminologie "Modus-operandi-Bereich" genannt, grundsätzlich den INPOL-Land-Systemen zu. Damit wird die frühere Zielvorstellung einer bundesweiten Straftaten-/Straftäterdatei, die die Überleitung des heute z.T. noch mit Hilfe von Formularen und Karteien organisierten Kriminalpolizeilichen Meldedienstes in eine DV-Anwendung vorsah, aufgegeben.

Ausgenommen von der grundsätzlichen "Abschottung" des Modus-operandi-Bereiches der Ländersysteme gegenüber INPOL-Bund sind lediglich die Zentralen Falldateien für Straftaten von bundesweiter Bedeutung. Dabei handelt es sich um Auskunfts- und Recherche-Anwendungen nach dem abgewandelten Modell der sogenannten Straftaten-/Straftäterdatei. In Zentralen Falldateien werden voraussichtlich die Kriminalitätsbereiche Rauschgift, Falschgeld, Waffen/Sprengstoff und Wirtschaftskriminalität organisiert werden. Die seit 1980 betriebene Erprobung der Falldatei Rauschgift besitzt Pilotcharakter für die Übernahme dieser Kriminalitätsbereiche als Zentrale Falldatei.

Die Zentralen Falldateien sollen künftig im Verbund betrieben werden. Die Erstellung der entsprechenden Verbundkonventionen ist von den zuständigen Gremien kürzlich in Angriff genommen worden. Eine Realisierung im Verbund wird jedoch erst nach der Realisierung des Kriminalaktennachweises, der Haftdatei und der Erkennungsdienstdatei erfolgen können, so daß heute noch keine näheren Terminaussagen über die Verwirklichung abgegeben werden können.

3.1.6 Zentrale Aktenerschließungssysteme

Der Begriff "Aktenerschließungssystem" beinhaltet das beim Bundeskriminalamt geführte PIOS-System. Es handelt sich dabei um ein in die Grundinformationsbereiche Personen, Institutionen (= Organisationen), Objekte und Sachen gegliedertes Dokumentations- und Recherchierverfahren, das dazu dient, die relevanten Einzelfakten aus Ermittlungsakten mit ihren Querbezügen recherchierfähig darzustellen und für beliebige ermittlungsdienliche Fragestellungen erschließen zu können. Das PIOS-Verfahren hilft bei der Bearbeitung großer Ermittlungskomplexe damit dem Ermittlungsführer, eine bessere Nutzung der gesamten anfallenden Erkenntnisse für die Steuerung der weiteren Ermittlungen zu erreichen.

Das PIOS-Verfahren wurde 1975 zuerst zur Unterstützung der Bekämpfung der terroristischen Gewaltkriminalität entwickelt. Seit 1980 wird das - anwendungsneutrale - PIOS-Verfahren auch im Rauschgiftbereich eingesetzt. Ferner werden im Rahmen der Neuordnung des Kriminalpolizeilichen Meldedienstes in Staatsschutzsachen heute auch die PIOS-Arbeitsdateien Staatsgefährdung und Landesverrat aufgebaut. Schließlich betreibt das Bundeskriminalamt eine PIOS-Arbeitsdatei Waffen.

Das PIOS-System wird zentral betrieben und seitens der Landeskriminalämter über direkt angeschlossene Terminals genutzt. Z.Z. bereitet das Bundeskriminalamt eine Neuentwicklung des DV-Verfahrens PIOS vor, das voraussichtlich Mitte 1984 zum Einsatz kommen wird.

3.1.7 Zentrale Spurendokumentationssysteme

Spurendokumentationssysteme - abgekürzt SPUDOK - sind ein weiteres Hilfsmittel der Ermittlungsführung. SPUDOK-Systeme existieren sowohl beim Bundeskriminalamt als auch bei verschiedenen Ländern. SPUDOK wird vorzugsweise eingesetzt, wenn in einem Ermittlungsverfahren wegen eines Kapitalverbrechens oder einer ähnlich herausragenden Straftat eine große Zahl an Hinweisen und Spuren anfällt. Die Hinweise und Spuren werden in SPUDOK zunächst unbewertet registriert, um dann einzeln ermittlungsmäßig abgeklärt zu werden. SPUDOK-Verfahren dienen deshalb in erster Linie der temporären Dokumentation und Recherche, um dem Ermittlungsführer einen laufenden Überblick über das Aufkommen an Hinweisen und Spuren sowie den Stand der Bearbeitung zu geben. SPUDOK-Verfahren eignen sich darüber hinaus auch als ein der Erfassung in der eigentlichen Hauptanwendung vorgeschalteter Filter, z.B. im Zusammenhang mit PIOS. Dabei werden die angefallenen Hinweise und Spuren im ersten Schritt in SPUDOK registriert und nach Abklärung ihrer Relevanz im zweiten Schritt in PIOS übertragen. Die SPUDOK-Datei wird regelmäßig mit Abschluß der polizeilichen Ermittlungen geschlossen und gelöscht.

3.1.8 Zentrale Tatmittelnachweise

Bei der im Fortentwicklungskonzept genannten letzten INPOL-Bund-Anwendung Zentrale Tatmittelnachweise handelt es sich um ein projektiertes Vorhaben, für das die im BKA-System geführte Beweismitteldokumentation für den Terrorismus-Bereich als Modell dienen könnte.

3.1.9 Literaturdokumentationssystem COD

In Vollzug des Beschlusses der Innenministerkonferenz vom 14.06.1974, für die gesamte Polizei ein computergestütztes System zur Erschließung und Wiedergewinnung kriminalwissenschaftlicher Literatur als Bestandteil des polizeilichen Informationssystems aufzubauen, errichtete das Bundeskriminalamt das Literaturdokumentationssystem COD (Computergestützte Dokumentation). Im Gesamtkonzept von 1975 wurde das Literaturdokumentationssystem mit dem Ziel beschrieben, der polizeilichen Praxis, Lehre und Forschung aktuell und vollständig die Fundstellen der Literatur aus den Bereichen Krimi-

nologie, Kriminalistik und naturwissenschaftliche Kriminaltechnik zu vermitteln. Im Fortentwicklungskonzept von 1981 findet das Literaturdokumentationssystem keine Erwähnung mehr. Es dient im weiteren Sinne aber auch der Verbrechensbekämpfung. Heute nutzen neben dem Bundeskriminalamt alle Landeskriminalämter und die Polizeiführungsakademie mittels Direktanschluß das COD-System. Die Datenbank enthält u.a. 7.500 kriminologische/kriminalistische und 4.000 kriminaltechnische Dokumente.

3.2 INPOL-Land-Anwendungen

Das Fortentwicklungskonzept beschreibt die DV-Anwendungen von INPOL-Land in den stichwortartigen Zielsetzungen

- Modus-operandi-Daten zu Personen und Fällen
- Folgedaten zu Personen, die in INPOL-Bund erfaßt sind
- Folgedaten zu Fällen mit unbekannten Tätern

mit gewollter Unschärfe. Es spricht auch die Formulierung "Im übrigen speichern die Länder ihre Daten der polizeilichen Verbrechensbekämpfung nach eigenem Ermessen" für diese Auffassung. Die für INPOL-Land gegebenen Stichworte finden prinzipiell in den Konzeptionen aller Länder für den Endausbaustand ihrer DV-Systeme anwendungsseitige Entsprechungen. Durch die unscharfe Anwendungsbeschreibung im Fortentwicklungskonzept bleibt die Aufgabenplanung der Länder im Ergebnis unberührt. Da das Konzept auch keine Verpflichtung enthält, bis wann die INPOL-Land-Systeme verwirklicht werden sollen, haben die langfristig angelegten Realisierungspläne der Länder weiterhin Bestand.

Die Ländersysteme werden somit weitgehend unabhängig nach den eigenen Zielsetzungen, aufgabenbezogenen Prioritäten und vorhandenen Ressourcen in landesspezifischer Ausgestaltung ausgebaut werden. Im gemeinsamen Kern werden die Landessysteme den eigenen Landesaktennachweis einschließlich des Landesbestandes zum bundesweiten Kriminalaktennachweis und darüber hinaus in unterschiedlichen Ausgestaltungs- und Organisationsformen die Modus-operandi-Anwendung nach dem Modell der Straftaten-/Straftäterdatei umfassen. Die Aufgabe einer Auskunfts- und Recherche-Anwendung für den Modus-operandi-Bereich besteht im allgemeinen darin, die Personenerkenntnisse über Beschuldigte und Tatver-

dächtige mit Informationen über die ihnen zuzuordnenden aufgeklärten Straftaten anzureichern. Weitere Aufgabe ist es, im Wege der Recherche mit Daten zum Modus operandi registrierter aufgeklärter ebenso wie unaufgeklärt gebliebener Straftaten einschließlich der Personenbeschreibung der Verdächtigen Hinweise auf mögliche Personen- und Tatzusammenhänge zu gewinnen, um die Ermittlungen zur Aufklärung dieser Straftaten zu unterstützen. Bei konsequenter dezentraler Organisation wird die Modus-operandi-Anwendung den Dienststellen vor Ort als "Vorgangserfassungs- und nachweissystem" für alle einschlägigen Formen der täglichen Sachbearbeitung angeboten werden. Mit dieser sachbearbeiternahen Verfahrensorganisation ist erreichbar, daß neben dem Aufbau eines umfassenden Erkenntnispools für den Landesbereich zusätzlich alle Registrier-, Berichts- und Meldedienstpflichten durch jeweils einen Datenerfassungsvorgang abgedeckt werden können. Um die Verträglichkeit der landesbezogenen Modus-operandi-Systeme für landesübergreifenden Informationsaustausch zu gewährleisten, werden die für die Zentralen Falldateien von INPOL-Bund vorgesehenen Informationsstrukturen den Orientierungsrahmen für die Ländersysteme abgeben.

Die Realisierungsbestände der INPOL-Land-Systeme sind von Land zu Land sehr verschieden. In einem Land ist das Aufgabenspektrum von INPOL-Land einschließlich Vorgangsnachweis bereits verwirklicht. In mehreren anderen Ländern sind Teilkomponenten der INPOL-Land-Anwendungen realisiert, wobei die volle Verwirklichung im Rahmen des kontinuierlichen Ausbaus der Landessysteme geplant wird.

Polizeitaktische Aspekte des Einsatzes der Datenverarbeitung

Gerd Lehmann

1. Einleitung

1.1

Die Polizei hat modernen Kommunikationsmitteln und -techniken für ihren Einsatz schon immer ihre besondere Aufmerksamkeit gewidmet. Melde-, Fernsprech-, Fernschreib-, Funk- und Bildtechnik gehören seit langem zu den wesentlichen Stützen ihrer Tätigkeit. Auch die Bedeutung der Datentechnik wurde schnell erkannt. Nach bescheidenen Anfängen bei der adv-mäßigen Aufbereitung der Kriminalstatistik führte dies für die Verbrechensbekämpfung alsbald zur Installation des bundesweiten Informationssystems der Polizei (INPOL) mit Zentralrechnern beim Bundeskriminalamt und Rechnern in den Landeskriminalämtern der einzelnen Bundesländer. Die in diesem Zusammenhang von Bund und Ländern autonom organisierten DV-Systeme mit einmaligen, parallelen und teilparallelen Datenbestandsführungen in einem mehr oder weniger koordinierten Gesamtsystem bilden noch heute den Kern des Einsatzes der Datenverarbeitung bei der Polizei.

1.2

Im Bereich von Führung und Einsatz sowie der Bearbeitung von Vorgängen aller Art werden vielerorts aber noch immer keine oder äußerst primitive Hilfsmittel eingesetzt.
Dabei ist der Nutzen unbestritten, der mittels Datenverarbeitung gerade in diesen Bereichen zu erzielen ist.

1.3

Mehr als zehn Jahre Datenverarbeitung bei der Polizei haben die Notwendigkeit, die Zweckmäßigkeit und die Vorteile ihres Einsatzes, aber auch Unzulänglichkeiten, Probleme und neue Aspekte aufgezeigt. Im weiteren sollen nunmehr die wichtigsten Anwendungsmöglichkeiten der Datenverarbeitung bei der Polizei und die dabei zu berücksichtigenden taktischen Aspekte aus der Sicht der polizeilichen Praxis (Streifendienst/Ermittlungsdienst/

Führungsaufgaben) in Form eines Soll-/Istabgleiches dargestellt werden. Dabei wird Leistungsmerkmalen der Datenverarbeitung, die eine Optimierung der Verbrechens- und Verkehrsunfallbekämpfung ermöglichen, besondere Aufmerksamkeit gewidmet.

Hierzu gehören u.a.

- Bewältigung großer Informationsmengen,
- Beschleunigung des Nachrichtenflusses,
- Vermeidung von Doppel-/Mehrfacherfassungen,
- Entlastung von Routinearbeiten.

2. Polizeiliche Streifentätigkeit

2.1

Zur Erfüllung der Aufgaben im polizeilichen Streifendienst sind aktuelle und gesicherte Informationen über Personen, Sachen und Sachverhalte unerläßlich. Soweit sie vor Ort nicht vorliegen, müssen sie insbesondere beim Einschreiten schnell, d.h. in Sekunden, und auf einfache Art und Weise zu erlangen sein.

2.2

Mit der Errichtung und Führung der bundesweiten Personen- und Sachfahndungsdateien im Direktzugriffsverfahren von INPOL ging für den Streifendienst die Suche in unhandlichen und inaktuellen Fahndungsbüchern zu Ende. Über Funk oder Telefon erreicht der Streifendienst nunmehr eine Datenstation und kann auf einen höchst aktuellen Datenbestand sekundenschnell zugreifen. Der technische Fortschritt gewährleistet eine Systemverfügbarkeit von mehr als 98% rund um die Uhr. Aber auch für Systemausfälle ist vorgesorgt. Mit dem COM-Verfahren (Computer Output on Microfilm) steht ein aktuelles Auskunftssicherungssystem zur Verfügung. Es ermöglicht über entsprechende Lesegeräte einen Zugriff auf postkartengroße Mikrofilmkarten (Fiches), die einzeln bis zu 50.000 Index-Fahndungsnotierungen aufnehmen können, so daß der gesamte Personenfahndungsbestand auf nur 3-5 Fiches gesichert ist.

Trotz Beachtung nahezu aller polizeitaktischer Aspekte ergeben sich bei der Durchführung des Verfahrens einige Probleme wie z.B.

- Überlastung der Funk-/Drahtwege,
- Übermittlungsfehler,
- mangelnde Geheimhaltung,
- "Negativ"-Motivation,
- fehlende Nähe der Datenverarbeitung.

Die Probleme sind weniger dv-spezifisch; sie sind mehr organisatorischer Natur. Ansätze zu ihrer Überwindung ergeben sich durch den Einsatz neuerer Kommunikationsmittel wie des Funkmeldesystems (FMS) und des Datenfunks, der Entwicklung von mobilen Dateneingabe-/Datenlese- und Datenausgabegeräten, durch eine Verdichtung des ortsfesten Datenstationsnetzes sowie durch Zulassung weiterer, polizeirelevanter Informationsinhalte in den Datenbeständen. Andere Probleme, die auf menschlicher Nachlässigkeit oder dergleichen basieren, wie z.B. das nicht zeitgerechte Speichern, Ändern oder Löschen von Daten oder die noch immer äußerst häufige Wiederausgabe gesperrter Kraftfahrzeugkennzeichen, sind zwar nicht völlig vermeidbar, aber sicherlich in der Häufigkeit reduzierbar. Dies sollte im Interesse der Sicherheit des Einschreitens oberstes Gebot sein.

2.3

Als erheblicher Mangel sind für den Streifendienst die fast noch überall gegebenen herkömmlichen, z.T. anachronistisch anmutenden Zugriffsmethoden auf Melde-, Kraftfahrzeug- und Führerscheindaten anzusehen. Dieser Mangel wiegt um so schwerer, weil eine effektive Streifentätigkeit fast ausschließlich auf der Feststellung und Überprüfung von Personalien, Fahrzeughaltern und -führern beruht und die Freiheitsrechte der Bürger hierdurch nicht unwesentlich berührt werden. Aus der Sicht des Streifendienstes gehört der Realisierung einer DV-Unterstützung mit direktem Zugriff der Polizei auf Datenbestände aus diesem Bereich rund um die Uhr oberste Priorität. Während für das Meldewesen kaum Verbesserungen erkennbar werden, können die Informationsbedürfnisse der Polizei durch den fortschreitenden Aufbau des Zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrt-Bundesamt (KBA) in Flensburg alsbald besser als bisher befriedigt werden. Derzeit hält das KBA die Daten der Halter von Fahrzeugen aus den Zulassungsbereichen der Länder

- Baden-Württemberg,
- Berlin und
- Schleswig-Holstein

sowie die Daten aller Halter von Fahrzeugen mit Versicherungskennzeichen und alle Daten über Führerscheinentziehungen für Direktauskünfte über Datenfernverarbeitung zur Verfügung. In Baden-Württemberg haben bereits mehr als 50 Datenendgeräte des polizeilichen Auskunftsdienstes Zugriff auf diese Daten.

2.4

Im Land Nordrhein-Westfalen werden zur Unterstützung der Streifentätigkeit derzeit noch folgende DV-Verfahren mit zentraler bzw. dezentraler Rechnerkapazität eingesetzt:

- Verkehrsunfallfluchtdatei,
- Verkehrswarndienstdatei,
- Begleitschutzdatei für den Bereich Bonn,
- Einsatzsteuerung in den Bereichen Bonn, Düsseldorf und Köln mit dem System CEBI.

2.5

Weiterer Bedarf an Verfahrensautomatisierung für die polizeiliche Streifentätigkeit besteht u.a. für die Bereiche

- Personen- und Sachbeschreibungen,
- gefährliche Güter,
- Anzeigenaufnahme.

3. Polizeiliche Ermittlungstätigkeit

3.1

Zur Erfüllung der Aufgaben im polizeilichen Ermittlungsdienst sind aktuelle und gesicherte Informationen über Personen, Sachen, Sachzusammenhänge und Vorgänge unerläßlich. Soweit sie dem Ermittlungsbeamten nicht vorliegen, müssen sie schnell, d.h. für Ermittlungen im Minutenbereich und für Auswertungen im Stunden-/Tagesbereich, auf einfache Art und Weise in der Regel rund um die Uhr zu erlangen sein.

3.2

Mit der Errichtung und Führung der bundesweiten Personen- und Sachfahndungsdateien im Direktzugriffsverfahren von INPOL ging auch für den Ermittlungsdienst die Suche in unhandlichen und inaktuellen Fahndungsbüchern und -karteien zu Ende. Mit einer automatisierten zentralen Auskunftsdatei in Nordrhein-Westfalen und ähnlichen Datensammlungen in anderen Bundesländern, die Informationen über Personen mit Kriminalakten führen (künftiger Kriminalaktennachweis - KAN), der elektronischen Führung von Haftdaten, der edv-gestützten Erfassung und Dokumentation von Fakten aus umfangreichen Aktenbeständen der Ermittlungskomplexe Staatsschutz und Rauschgift im System PIOS (Personen, Institutionen, Objekte, Sachen), der computerunterstützten Daktyloskopie und nicht zuletzt mit den Möglichkeiten einer rechnergestützten Dokumentation von Spuren und Hinweisen in großen Ermittlungsverfahren durch das SPUDOK-System stehen dem Ermittlungsdienst eine Fülle von Hilfsmitteln zur Verfügung. Diese Verfahren weisen jedoch nicht immer eine einheitliche und abgestimmte Benutzeroberfläche auf. Es sind z.T. Insellösungen, auf die nicht immer mit akzeptablem Bedienungskomfort zugegriffen werden kann.

3.3

Für die polizeiliche Ermittlungstätigkeit ergeben sich - wie beim Streifendienst - Probleme beim Zugriff auf Melde-, Kraftfahrzeug- und Führerscheindaten sowie vergleichbare Konflikte im organisatorischen Bereich bei der Durchführung der ADV-Verfahren.

3.4

Die derzeitige ADV-Unterstützung bei der polizeilichen Ermittlungstätigkeit vermeidet nicht Doppel- und Mehrfacherfassungen und ist m.E. trotz oder gerade wegen der Vielzahl von Verfahren nicht in der Lage, den Anforderungen in ausreichender Weise gerecht zu werden. Auf der Suche nach neuen Wegen, insbesondere zur Kriminalitätsbekämpfung, - eine zwingende Notwendigkeit im Interesse der Sicherheit der Gesellschaft angesichts der permanent steigenden Tendenz der Kriminalitätsraten - wird man sich künftig besonders mit dem Problem der büro- und arbeitstechnischen Bewältigung der sehr erheblichen Mengen von polizeilichen Ermittlungsvorgängen auseinandersetzen müssen.

Alle polizeilich zu lösenden Aufgaben für die Verbrechens- und Verkehrsunfallbekämpfung lassen sich aus Ermittlungsvorgängen ableiten. Sie sind Grundlage allen polizeilichen Handelns, das aus Gründen der Eigenkontrolle der polizeilichen Maßnahmen und als Voraussetzung für die rechtliche Überprüfbarkeit durch andere aktenkundig zu machen ist. Die ordnungsgemäße Erfassung, Bearbeitung und Verwaltung (Registratur) der Vorgänge erfordert ein vielfältiges System von

- Tagebüchern und Personen-Indizes
- Zentralkarteien
- Sammlungen für Kriminalakten/Personen- und Fallbeschreibungen
- Karteien für körperliche Merkmale/Spitznamen/Spezialisten

und dergleichen mehr, eine Flut von Informationen, die manuell mit den herkömmlichen Mitteln der Büroorganisation und den bisherigen Arbeitsmethoden nicht mehr zu bewältigen sind.

3.4

Wege zur Optimierung der Ermittlung und Auswertung von Straftaten zeigen die Bemühungen in Berlin mit dem ADV-System ISVB und in Baden-Württemberg mit dem System PAD sowie das Konzept der automatisierten Vorgangsverwaltung in Nordrhein-Westfalen. Dabei wird angestrebt, alle Teilbereiche polizeilicher Ermittlungstätigkeit

- Vorgangsverwaltung
  (Tagebuchführung/Büro-Administration/Registratur)
- Vorgangsbearbeitung
  (Ermittlungen/Personen- und Sachfahndung/Aktualisierung kriminalpolizeilicher Dateien/Recherchen i.S. des KMD bzw. der SSD)
- Vorgangsauswertung
  (Polizeiliche Kriminalstatistik/kriminologisch-soziologische Forschung)

in einem System von Datenerhebung, -erfassung und -auswertung zusammenzufassen. Die automatisierte Vorgangsverwaltung soll die bisher vorhandenen erheblichen Belastungen der Sachbearbeiter durch Doppel- und Mehrfacherfassungen von polizeirelevanten Daten weitgehend ausschließen und die Belange der polizeilichen Fahndung, des Meldedienstes (KMD/SSD), der Sondermeldedienste (SOM) sowie der Polizeilichen Kriminalstatistik integrieren und zu einer einheitlichen Benutzeroberfläche führen.

3.5

Ähnliche Anforderungen bestehen für eine rechnergestützte Vorgangsverwaltung im Bereich Verkehr/Ordnungswidrigkeiten. Mit der Entwicklung der Verfahren HESOWi in Hessen und VoBi in Bayern ist hier bereits ein Stand erreicht worden, der, von geringfügigen Modifikationen abgesehen, eine Implementierung auch bei der Polizei anderer Länder zuläßt.

4. Polizeiliche Führungsaufgaben

4.1

Die Anwenderanforderungen an Systeme für Führung und Einsatz orientieren sich weitgehend an der Polizeidienstvorschrift PDV 100. Danach sind Datenverarbeitungsanlagen Führungsmittel zum

- Speichern von Informationen über Personen, Sachen und Sachverhalte,
- Speichern von Übersichten, Befehlen und Durchführungsplänen,
- Vorbereiten, Planen und Durchführen polizeilicher Einsätze,
- schnellen Erfassen und Verarbeiten aller verfügbaren Daten für eine Entscheidungsvorbereitung.

Im Mittelpunkt steht in allen Fällen die Gewinnung von ausreichenden und sachgerechten Informationen zur Bewältigung von Entscheidungsprozessen. Aufgabenschwerpunkte für den Einsatz der Datenverarbeitung ergeben sich bei der

- Erstellung und Aktualisierung von Lagebildern für die Verkehrsunfall- und Kriminalitätsbekämpfung,
- Einsatzsteuerung,
- Bewältigung der Informationsflut in Führungsstäben.

Daneben bestehen Anforderungen auch für andere Führungs- und Koordinationsaufgaben. Im täglichen Dienst und bei polizeilichen Maßnahmen aus besonderen Anlässen wird eine Rechnerunterstützung u.a. angestrebt bei

- Kräfteberechnungen,
- Überprüfung von Einsatzabläufen,
- Führung von Einsatztagebüchern,
- Aufbereitung von objekt- und raumbezogenen Sondermaßnahmen, z.B. bei Fahndungen.

Dabei haben operationelle Führungssysteme den Vorzug vor Logistikverfahren.

4.2

Für eine erfolgreiche Verkehrsunfall- und Kriminalitätsbekämpfung sind differenzierte Kenntnisse der Lage unerläßlich, weil jede wirkungsvolle Aktion eine begründete und systematische Konzeption voraussetzt. Durch den Einsatz der Datenverarbeitung bei der Erstellung der Verkehrsunfall- bzw. Kriminalstatistik konnten bereits in der Vergangenheit neue Einsichten gewonnen werden. Abgerundete, das polizeiliche Geschehen ganzheitlich und einheitlich betrachtende Lagebilder stehen jedoch noch immer aus. Für die Einsatzplanung sind sie aber unerläßlich.

Die zu erstellenden Lagebilder müssen mindestens über die örtlichen und zeitlichen Gegebenheiten des Geschehens sowie über die möglichen Adressaten polizeilichen Handelns (Verursacher, Täter, Opfer, Geschädigte) Aufschluß geben. Sie sollen auch Entwicklungen und Trends aufzeigen und Prioritätsfestlegungen erleichtern. Ihre Erstellung duldet keinen Aufschub; sie müssen zeitnah verfügbar sein und ständig aktualisiert werden. Von der Form her müssen Lagebilder u.a. übersichtlich, anschaulich und leicht handhabbar sein. Zahlenfriedhöfe bringen keine Hilfe; sie begrenzen nur den praktischen Nutzen.

Die von der Polizei bislang beim Verkehrsunfall- und Kriminalitätsgeschehen erhobenen Daten erfüllen zwar die meisten, aber nicht alle gestellten Anforderungen. Probleme ergeben sich bei der eindeutigen Stationierung/Lokalisierung von Unfallorten (bei Kriminalitätsdaten fehlen die Angaben zum Tatort und zur Tatzeit vollständig) und wegen mangelnder Repräsentativität der Datenbasis. Dagegen lassen sich die Richtigkeit der Datenbasis und die notwendige Schnelligkeit der Datenaufbereitung - auch in einem parallelen Auswertungsmodell - mit Hilfe von Ablauforganisationen und Verfahren, wie sie bei der Gewinnung und Auswertung der Unfalldaten im Land Nordrhein-Westfalen angewandt werden, sicherstellen.

4.3

Bei der Einsatzsteuerung mit herkömmlichen Mitteln ergeben sich - insbesondere in Spitzenzeiten - mannigfaltige Informations- und Kommunikationsprobleme. Es bestehen häufig große Schwierigkeiten, die an sich vorhandenen Informationen aufzufinden und sie schnell, vollständig und im richtigen Zusammenhang aufzubereiten.

Selbst in großen Einsatzzentralen werden eingehende Hilfeersuchen, Alarme und Meldungen noch immer handschriftlich protokolliert,in herkömmlicher Weise analysiert und ausgewertet. Ein Gesamtüberblick über die vorhandenen Einsatzmittel, die laufenden Ereignisse und eingeleiteten Maßnahmen ist nur schwer zu gewinnen. Dies führt häufig zu Zeitverzögerungen und Unsicherheiten bei der Bearbeitung. Besonders bei schwerwiegenden Ereignissen wie z.B. Überfällen, Unglücksfällen und Katastrophen können dadurch vermeidbare Folgen eintreten und der polizeiliche Erfolg in Frage gestellt werden.

Aufgabe und Zielsetzung einer computerunterstützten Einsatzsteuerung liegen daher bei der

- Schaffung eines umfassenden Informations- und Kommunikationssystems und der
- Automatisierung des Nachrichtenflusses

für den ersten Ansatz. Dazu müssen die benötigten Informationen mit hoher Zuverlässigkeit, sekundenschnell, rund um die Uhr, in einfacher Art und Weise abrufbar, zur Verfügung stehen.

Mit den bislang bei der Polizei eingeführten Einsatzleitsystemen in Bonn, Duisburg, Düsseldorf, Köln, Stuttgart, Koblenz, Mainz und Freiburg konnte die Machbarkeit und Effizienz des DV-Einsatzes für Führung und Einsatz nachgewiesen werden.

Bereits kurze Zeit nach Inbetriebnahme der nordrhein-westfälischen CEBI-Systeme konnten wesentliche mit der DV-Unterstützung bei der Planung, Durchführung und Überwachung von Einsätzen angestrebte Ziele erreicht werden:

- Optimierung des Kräfte- und Mitteleinsatzes,
- Beschleunigung der Einsatzvergabe und -abwicklung,
- Gewährleistung eines einheitlichen taktischen Grundkonzeptes,
- Erhöhung der Sicherheit beim Einschreiten,
- schnelle Bereitstellung aktueller Informationen,
- Verbesserung des Zusammenspiels der nachrichtentechnischen Mittel,
- Überwindung technischer Engpässe und arbeitsorganisatorischer Mängel u n d
- Entlastung der Einsatzbearbeiter von Routinetätigkeiten.

Dazu werden die bei der Ereigniserfassung weitgehend automatisch anfallenden Daten durch ein äußerst komplexes Einsatzleitprogramm mit den polizeispezifischen Dateien und über Dialoge mit den Bearbeitern in einen logischen Zusammenhang gebracht und im Rahmen der Ereignisbearbeitung zu entsprechenden Ausgaben verarbeitet. Ein den polizeitaktischen Gegebenheiten angepaßter Algorithmus wählt für jedes Ereignis geeignete Kräfte und Mittel unter Berücksichtigung der art-, orts- und objektspezifischen Gegebenheiten aus und schlägt zu veranlassende Maßnahmen vor.

Die Ereignisdokumentation wird quasi am Rande erledigt. Einsatzgeschehen und polizeiliche Aktivitäten werden kurz-, mittel- und langfristig ausgewertet, so daß z.B. umfassende Erkenntnisse über Einsatzschwerpunkte in zeitlicher und räumlicher Hinsicht gewonnen werden. MENSCH - KOMMUNIKATIONSMITTEL - KOMMUNIKATIONSTECHNIK werden bei CEBI als integrale Einheit betrachtet. Dadurch kann sich der Einsatzbearbeiter mehr als bisher der seiner Aufgabenstellung entsprechenden Tätigkeit des ENTSCHEIDENS UND ANWEISENS widmen.

An CEBI sind im wesentlichen vier Kommunikationseinheiten direkt angeschlossen:

- Funkmeldesystem (FMS),
- Überfall-/Einbruchmeldeanlage (ÜEA),
- Informationssystem der Polizei (INPOL/PIKAS NW) mit Zugang zum Fernschreibnetz der Polizei.

Über die Datenquellen FMS und ÜEA fließen der Einsatzleitung die manuell nur mit relativ hohem Aufwand zu gewinnenden Informationen automatisch zu. Durch den Verbund mit dem Informationssystem der Polizei wird der Zugriff auch auf die überörtlichen Fahndungs-, Führungs- und Einsatzdateien gewährleistet. Außerdem kann bei Bedarf die Nachrichtenübermittlung in das Fernschreibnetz der Polizei veranlaßt werden.

Besondere Programmteile unterstützen Fahndungsmaßnahmen sowie die Dienststärke- und Wachdienstplanführung.

Für den Bereich der computerunterstützten Einsatzsteuerung besteht noch ein weiterer Automationsbedarf hinsichtlich einer

- Funkortung als automatisierte Standortbestimmung

  u n d

- einsatzorientierten Stadtplanprojektion.

Die Entwicklung solcher Systeme erfordert jedoch heute noch Kosten, die in keinem Verhältnis zum Nutzen stehen. Ihre Realisierung muß daher der Zukunft überlassen bleiben.

4.4

Zur Bewältigung der Informationsflut in Führungsstäben und zur Unterstützung der Arbeit von Befehlsstellen werden neuerdings zumindest im Lande Nordrhein-Westfalen "SPUDOK-vergleichbare", rechnergestützte Arbeitsdateien für die unterschiedlichsten Zwecke eingesetzt. Als Standard steht eine Datei zur Ereignis- und Veranlassungsdokumentation zur Verfügung. Damit wird u.a. eine lückenlose, nach unterschiedlichsten Gesichtspunkten direkt abfragbare und auswertbare Dokumentation vorgenommen und die Arbeit z.B. des Führungsstabes bei der Nachrichten-, Informations- und Sammelstelle (LZ 01) und der Dokumentation (LZ 03) spürbar erleichtert werden. Weitere Dateien (z.B. eingesetzte Kräfte, Führungs- und Einsatzmittel) können auf Anforderung kurzfristig eingerichtet werden.

Die z.B. bei Großeinsätzen in Bonn und bei Demonstrationen um das Kernkraftwerk Kalkar gewonnenen Erfahrungen haben die Notwendigkeit und Zweckmäßigkeit einer solchen DV-Unterstützung aufgezeigt.

5. Schlußbetrachtung

5.1

Die Polizei benötigt für ihre Aufgabenerfüllung leistungsfähige Informations- und Kommunikationssysteme. Dazu gehört heute ohne Zweifel die Datenverarbeitung. Die vorstehenden Ausführungen haben gezeigt, daß die derzeitigen und absehbaren Anwendungsmöglichkeiten und taktischen Anforderungen hinsichtlich

- Datenintegrität,
- Antwortzeitverhalten,
- Verfügbarkeit,
- Bedienerfreundlichkeit,
- Datensicherung,
- Datenschutz,
- Ausbaubarkeit und
- Übertragbarkeit

im wesentlichen erfüllt, bzw. die erforderlichen Maßnahmen zur Beseitigung von Mängeln und Schwachstellen erkannt und z.T. auch eingeleitet sind. Dazu gehören insbesondere die Entwicklung einer automatisierten Vorgangsverwaltung, die Einführung von DISPOL und eines bundesweiten Datenfunksystems.

Der Einsatz der Datenverarbeitung findet allerdings dort seine Grenze, wo innerhalb der Polizei selbst die Bereitschaft zur Akzeptanz des neuen Mediums noch fehlt. Hier gilt es künftig verstärkt anzusetzen. Durch entsprechende "Hinführung" aller Mitarbeiter zur Datenverarbeitung und durch organisatorische Maßnahmen müssen die Nutzungsmöglichkeiten der Datenverarbeitung voll erschlossen werden.

5.2

Die Realisierung von DV-Vorhaben wird heute mehr und mehr bestimmt von der Randbedingung "Kosten". Bei den meisten polizeilichen Anwendungen läßt sich keine strenge Wirtschaftlichkeitsberechnung im Sinne einer Kosten-Nutzen-Analyse aufmachen. Das zu automatisierende Verfahren steht neben anderen Aufgaben der

Polizei und den dafür erforderlichen Aufwendungen. Seine Rangordnung ergibt sich aus den Haushaltsbeschlüssen der Gesetzgeber. Grundsätzlich sollte aber bereits der Anwender seine Anforderungen mehr am technisch Notwendigen als am technisch Machbaren orientieren.

Polizeiliche Datenverarbeitung in Schweden

Anna Greta Gehnich

Bei der schwedischen Polizei wurden die ersten EDV-Systeme schon 1967 in Betrieb genommen. Die nationale Zentralisierung des Polizeiwesens 1965 und die damalige Einrichtung des Reichspolizeiamtes hat den Einsatz der EDV bei der schwedischen Polizei wesentlich erleichtert. In den ersten Jahren wurden auch sehr viele Systeme entwickelt und vor 1975 war die Polizei in Schweden im Vergleich zu anderen Ländern in Europa im Bereich der EDV sehr weit gekommen. Nach 1975 sind jedoch nur wenige neue Systeme hinzugekommen, in den letzten 2 bis 3 Jahren fast keine, und heutzutage müssen viele von den polizeilichen EDV-Systemen in Schweden leider als sehr unmodern betrachtet werden. Es gibt keine eindeutige Erklärung für diese Entwicklung; zum Teil ist das Reichspolizeiamt selbst dafür verantwortlich, aber auch andere Faktoren haben indirekt die Entwicklung zurückgehalten. Ich werde später darauf zurückkommen. Zuerst möchte ich Ihnen aber eine kurze Übersicht über den aktuellen Stand der Datenverarbeitung bei der schwedischen Polizei geben und danach die geplante Weiterentwicklung unter besonderer Berücksichtigung nicht nur des Datenschutzes sondern auch einiger der übrigen beeinflussenden Faktoren behandeln.

Es gibt bei der schwedischen Polizei gegenwärtig etwa 40 EDV-Systeme, davon 10 on-line-Systeme, die über 445 Bildschirme den 118 Polizeibezirken zur Verfügung stehen. Außerdem gibt es einige Systeme, die nur vom Reichspolizeiamt benutzt werden können. Die ersten on-line-Systeme, Personenfahndung und Kraftfahrzeugfahndung, wurden schon 1968, als das Reichspolizeiamt die erste Computeranlage installierte, in Betrieb genommen; aber erst 1974, als der neue Computer beim Reichspolizeiamt installiert wurde, konnten die großen Dateien, die zum Teil schon aufgebaut waren, für on-line-Betrieb zugänglich gemacht werden. Abbildung 1 zeigt sämtliche on-line-Systeme, die wir gegenwärtig in Betrieb haben, und ich werde einige davon kurz vorstellen.

Die größte Datei, die von den Bezirken aus zugänglich ist, ist die Pässedatei, wo Informationen über fast 5 Mio. schwedische Paßinhaber gespeichert sind. Anfragen können mit vollständiger Personennummer, mit Paßnummer oder mit Geburtsdaten zusammen mit dem Namen als Suchbegriff erfolgen.

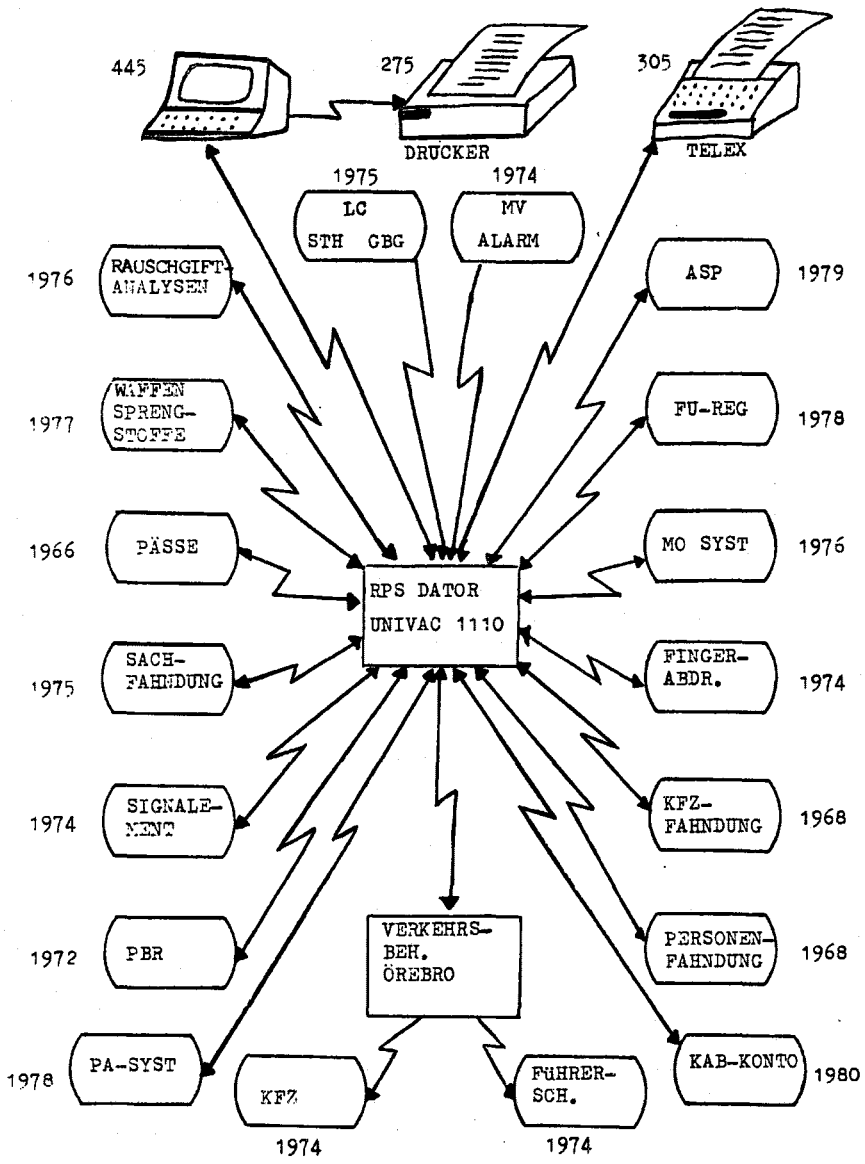

445
275
305
DRUCKER
TELEX
1975
LC
STH GBG
1974
MV
ALARM
1976
RAUSCHGIFT-
ANALYSEN
1977
WAFFEN
SPRENG-
STOFFE
1966
PÄSSE
1975
SACH-
FAHNDUNG
1974
SIGNALE-
MENT
1972
PBR
1978
PA-SYST
RPS DATOR
UNIVAC 1110
VERKEHRS-
BEH.
ÖREBRO
KFZ
1974
FÜHRER-
SCH.
1974
1979
ASP
1978
FU-REG
1976
MO SYST
1974
FINGER-
ABDR.
1968
KFZ-
FAHNDUNG
1968
PERSONEN-
FAHNDUNG
1980
KAB-KONTO

Abbildung 1

PBR ist die Abkürzung für die Personen- und Belastungsdatei, in der die Urteile, die Vollstreckungs- und die Tatverdachtsangaben betreffend mehr als 400 000 Personen registriert sind. Dieses System ist ein Teil des Informationssystems der Justiz und es bedient außer der Polizei auch die Staatsanwaltschaft und die Gerichte. Die beiden letzteren können jedoch nur über schriftliche Ersuchen Auszüge aus der Datei erhalten.

In das Sachfahndungssystem, in dem anfangs nur Gegenstände mit einer eindeutigen Herstellernummer registriert werden sollten, werden seit etwa zwei Jahren auch Gegenstände eingegeben, die eine solche Nummer nicht haben. Eine Nummer wird aus verschiedenartigen Kennzeichen des Gegenstandes konstruiert und als Herstellernummer betrachtet. Der Grund für diese Veränderung des Systems war, daß viele Hersteller, auch wenn es sich um teure Produkte handelt, die Gegenstände nicht mehr mit einer eindeutigen, eingeprägten Herstellernummer versehen.

ASP ist die Abkürzung für das allgemeine Fahndungssystem, das seit 1979 im Betrieb ist. Das System gibt schnelle Auskunft z.B. über Adressen, Kontakte usw., von aktiven Verbrechern. Da alle Polizeibezirke selbst ihre aktuellen Beobachtungen in das System eingeben, sind die Informationen immer aktuell und diese Tatsache hat, zusammen mit den vielen verschiedenen Suchbegriffen, die das System erlaubt, die Fahndungsarbeit der Polizei viel effektiver gemacht.

Zu den Systemen, die von den Polizeibezirken on-line zugänglich sind, gehört außer den Personen- und Kraftfahrzeugfahndungssystemen auch das Signalementsystem, in dem Daten über Untersuchungen auf dem Gebiet der Rauschgiftkriminalität gespeichert sind. Die Eingaben in die drei letzten Systeme erfolgen beim Reichspolizeiamt. Auch zwei administrative Systeme sind von den Bezirken aus für Anfragen on-line zugänglich, so ein Budgetsystem, das Auskunft darüber gibt, wieviel von den bewilligten Mitteln verbraucht ist und auch eine Prognose für den Rest des Rechnungsjahres stellt, und ein personaladministratives System, das aber noch nicht voll ausgebaut ist.

Für die Eingabe sämtlicher Informationen im Zusammenhang mit z.B. einem Mord oder irgend einem komplizierten Fall wird das besondere System für das Ermittlungsverfahren verwendet.

Ich möchte auch darauf hinweisen, daß es möglich ist, von allen Terminals in den Bezirken aus den Dateien der Verkehrsbehörde Auskunft über Autos und Führerscheinbesitzer zu bekommen.

Abbildung 2 zeigt die Entwicklung der Anwendungsfrequenz der Systeme von 1979 bis heute. Die Steigerung in den letzten Jahren hängt vor allem mit der Einführung von ASP (Allgemeines Fahndungssystem) zusammen, aber die Abbildung zeigt auch eine steigende Anwendung von anderen Systemen. Die Erhöhung der Anzahl der Bildschirme von 380 auf 445 während dieser Zeit hat natürlich auch zu der Steigerung beigetragen.

Wie sehen nun die Pläne für die Weiterentwicklung aus und welche Möglichkeiten hat das Reichspolizeiamt, diese Pläne durchzuführen? Dies hängt nicht nur mit dem Willen zusammen, neue Systeme einzuführen, sondern ist fast mehr eine Frage der Mittel und anderer beeinflussender Faktoren.

Wie ich schon erwähnt habe, müssen mehrere von den Systemen, die dem schwedischen Polizeiwesen zur Verfügung stehen, als ziemlich unmodern betrachtet werden. Das hängt nicht nur mit den technischen Lösungen, die teilweise einer vergangenen Zeit angehören, zusammen, sondern ist auch eine Folge der veränderten Anforderungen der Benutzer. Die ersten großen Systeme, die Anmelde- und Personenblattsysteme, die 1968 eingeführt wurden, hatten zwei Hauptziele: einerseits sollten sie zentrale Dateien über Straftaten und die dieser Straftaten verdächtigten oder derentwegen verurteilten Personen aufbauen, und andererseits sollten sie eine verbesserte Statistik produzieren. Diese Ziele sind auch erreicht worden. Aber in den letzten 4 bis 5 Jahren, mit einer stets steigenden Kriminalität ohne eine entsprechende Personalverstärkung bei der Polizei, sind die EDV-Pläne mehr darauf eingerichtet worden, Systeme zu entwickeln, die die tägliche Arbeit in den Polizeibezirken unterstützen und erleichtern können.

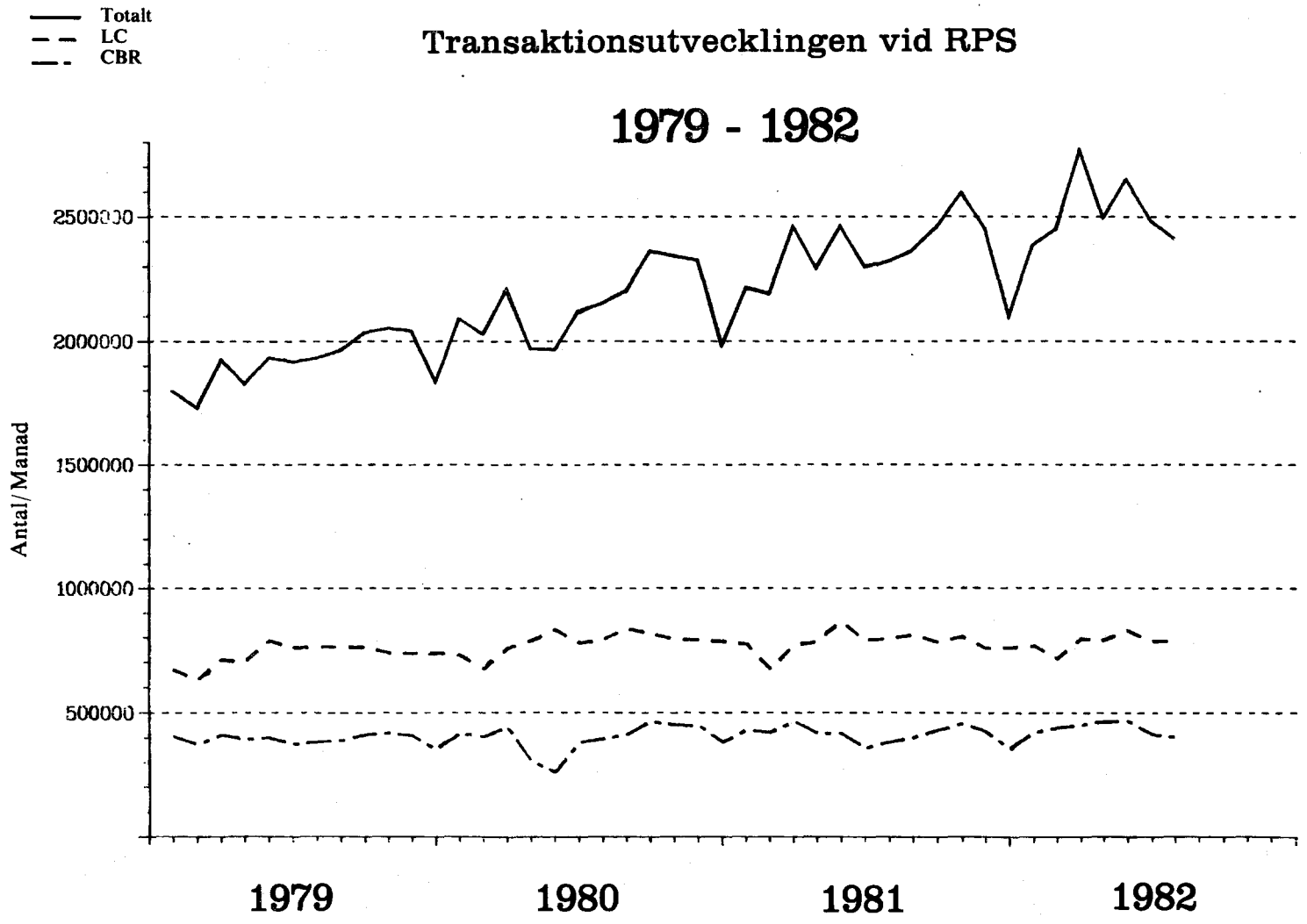

Totalt
LC
CBR
Transaktionsutvecklingen vid RPS
1979 - 1982
2500000
2000000
1500000
1000000
500000
Antal/Manad
1979
1980
1981
1982

Abbildung 2

Zu den Weiterentwicklungsplänen, die gegenwärtig vorliegen, gehört unter anderem eine völlige Neukonstruktion der Anmelde- und Personenblattsysteme. Bei den gegenwärtig benutzten Systemen werden alle Formulare zum Reichspolizeiamt geschickt und dort bearbeitet und die Polizeibezirke bekommen sehr wenig Informationen zurück. Das neue System hat als Hauptziel vor allem die Informationsbedürfnisse der Bezirke zu erfüllen und außerdem die manuellen Register überflüssig zu machen. Natürlich muß auch in der Zukunft eine ganze Menge an Informationen in zentralen Dateien erreichbar sein, aber die großen Datenmengen werden nur für den betreffenden Bezirk zugänglich gemacht werden.

Abbildung 3 zeigt in großen Zügen, wie das System, das in mehreren Etappen durchgeführt werden soll, geplant ist. Alle Formulare sollen direkt auf den Bildschirm geschrieben werden, und das Einschreiben soll vom System unterstützt werden, so daß alle Informationen, die für verschiedene Zwecke erforderlich sind, auch registriert werden.

In den lokalen Dateien wird alles gespeichert, und nur die Angaben, die für die Koordination zwischen den Bezirken und für die reichsdeckende Statistik nötig sind, werden in die zentrale Datei eingegeben. Das neue System wird in der ersten Etappe die heutigen Anmelde- und Kraftfahrzeugfahndungssysteme und zum Teil auch das Personenblattsystem ersetzen.

Außer den vielen Anfragearten, die das System ermöglichen wird, werden z.B. gewisse Mitteilungen an andere Behörden automatisch ausgedruckt werden, und die Bezirke können den Umfang und die Periodizität der statistischen Zusammenstellungen, die sie für ihre Tätigkeit benötigen, selbst bestimmen.

In den folgenden Etappen werden mehrere der heutigen Systeme hiervon beeinflußt werden, z.B. ASP (das Allgemeine Fahndungssystem), das Sachfahndungssystem und einige der Systeme, die zum Informationssystem der Justiz gehören. In dieser Etappe sind auch ein vereinfachter Informationsaustausch mit der Staatsanwaltschaft sowie erweiterte Möglichkeiten vorgesehen, Auskünfte aus den Dateien anderer Behörden zu erhalten.

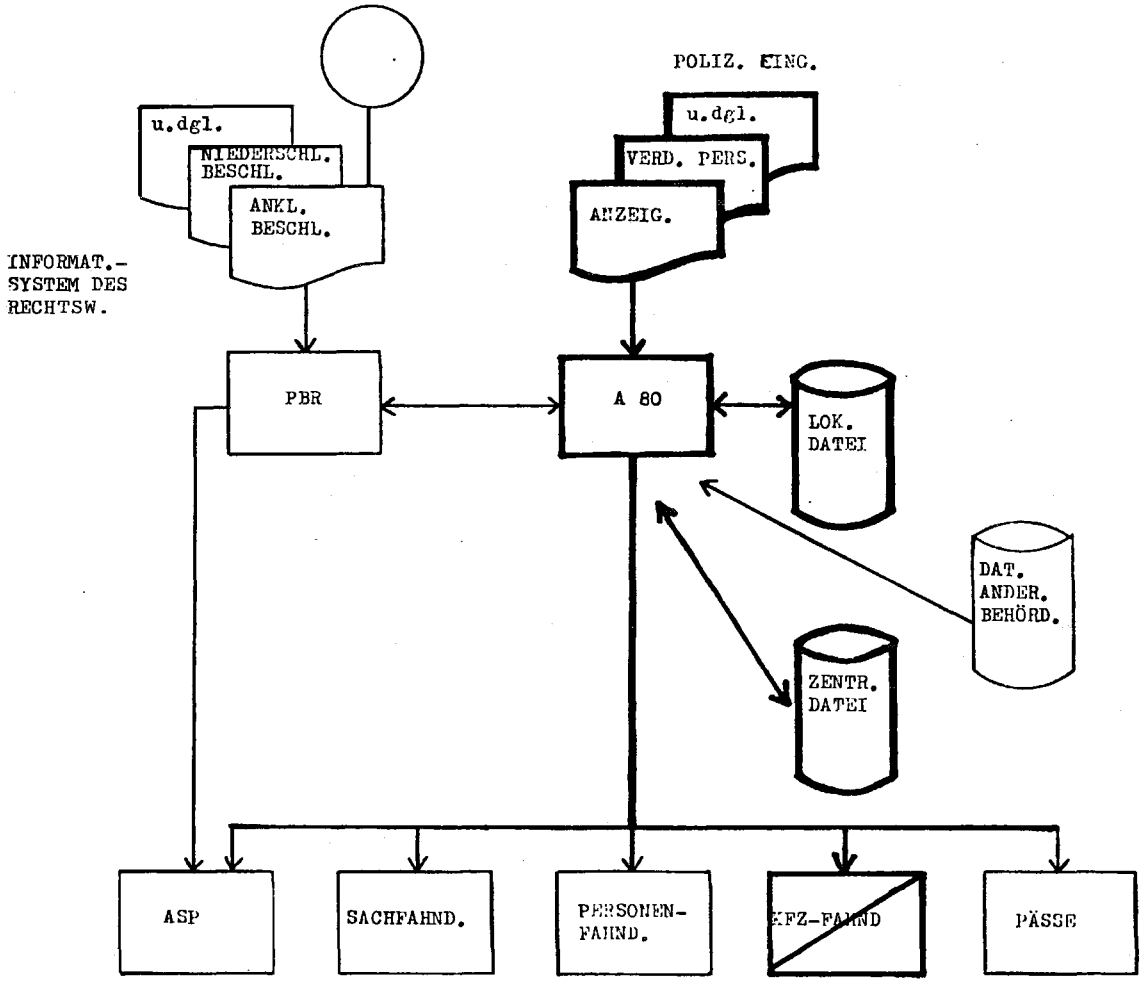

POLIZ. EING.
u.dgl.
VERD. PERS.
ANZEIG.
u.dgl.
NIEDERSCHL. BESCHL.
ANKL. BESCHL.
INFORMAT.-SYSTEM DES RECHTSW.
PBR
A 80
LOK. DATEI
DAT. ANDER. BEHÖRD.
ZENTR. DATEI
ASP
SACHFAHND.
PERSONEN-FAHND.
KFZ-FAHND
PÄSSE

Abbildung 3

Für die Einsatzleitstellen in Stockholm, Göteborg und Malmö, wo neue Funksysteme eingeführt werden sollen, ist auch ein neues, mit dem Funksystem integriertes Einsatzleitsystem geplant. Dieses System kann mit kleinen Änderungen auch in anderen Polizeibezirken eingeführt werden. Als Weiterentwicklung dieses Systems ist auch eine Verbindung zu dem zuvor beschriebenen System vorgesehen. Eine Anzeige, die als Folge eines Einsatzes ausgeschrieben werden soll, enthält zum Teil die Angaben, die beim Einsatz registriert wurden, und um dieselben Informationen nicht wieder eingeben zu müssen, werden die gemeinsamen Daten vom Einsatzleitsystem überführt werden.

Außer den obengenannten Systemen, die vor allem der polizeilichen Ermittlungs- und Überwachungstätigkeit dienen sollen, liegen auch für die administrativen Systeme verschiedene Neuentwicklungspläne vor. Um die stets steigende Arbeitsbelastung im kriminalpolizeilichen Bereich zu bewältigen, müssen neue Grundlagen für Planung, Prioritätensetzung und Auswertung entwickelt werden, damit die zur Verfügung stehenden Mittel optimal verwendet werden können. Deshalb wird ein neues, personaladministratives System entwickelt werden, das sowohl lang- und kurzfristige Planung wie auch eine Auswertung der Einsätze ermöglichen soll.

Natürlich stellen unsere Pläne große Anforderungen an z.B. die Computerkapazität. Ende nächsten Jahres wird eine neue Computeranlage installiert, die die doppelte Kapazität im Vergleich zu der jetzigen hat. Außerdem werden die größeren Polizeibezirke in einigen Jahren bestimmt eigene Computer haben, die mit der Zentralanlage verbunden sind. Die Einführung des neuen Anmelde- und Personenblattsystems setzt dies z.B. voraus, weil die lokalen Dateien der größeren Bezirke einen Umfang haben werden, der eine zentrale Anlage nicht belasten sollte. Eine starke Erhöhung der Anzahl der Terminals ist auch erforderlich, um eine effektive Benutzung der vorher beschriebenen neuen Systeme zu ermöglichen. Die Versuche, die wir mit mobilen Terminals bisher durchgeführt haben, deuten auch auf einen weiteren Ausbau auf diesem Gebiet hin.

Da es der Wunsch des Bundeskriminalamtes war, daß die geplante Weiterentwicklung unter besonderer Berücksichtigung des Datenschutzes behandelt werden sollte, will ich auf dieses Thema etwas gründlicher eingehen, obwohl das Datenschutzgesetz und mit diesem zusammenhängende Fragen auf unsere Weiterentwicklungspläne viel weniger Einfluß haben, als andere administrative und wirtschaftliche Regeln.

Das schwedische Datenschutzgesetz, das 1973 in Kraft trat, regelt die Einrichtung und Führung von personenbezogenen Registern im Zusammenhang mit EDV. Gleichzeitig mit dem Inkrafttreten des Gesetzes wurde auch das Datenschutzamt eingerichtet, dessen Aufgabe es unter anderem ist, Genehmigungen für die Einführung von EDV-Systemen mit personenbezogenen Daten zu erteilen, die Aufsicht über solche Systeme auszuüben und auch Beschwerdeinstanz in Fragen zu sein, die mit dem Datenschutzgesetz zusammenhängen.

Das Datenschutzgesetz, das sowohl im staatlichen wie im privatwirtschaftlichen Bereich gilt, schreibt vor, daß für EDV-Register mit personenbezogenen Daten eine Genehmigung des Datenschutzamtes erforderlich ist und daß jede Person das Recht hat, kostenlos bei einer Behörde oder einem Unternehmen darüber Kenntnis zu erhalten, ob sie in einem Register vorkommt oder nicht.

Es gibt bezüglich der Genehmigungen nur eine Ausnahme, und zwar dann, wenn die Regierung die Einrichtung eines Registers beschließt; aber auch in diesem Falle muß sich das Datenschutzamt dazu äußern. Dies bedeutet, daß auch die Polizei, genau wie andere Behörden innerhalb des Rechtswesens, für alle EDV-Systeme mit personenbezogenen Daten eine Genehmigung haben muß.

Das Recht, Auszüge aus verschiedenen Registern zu erhalten, kann durch andere Gesetze beseitigt werden. Das Gesetz zur Geheimhaltung regelt z.B. das Recht auf Auskunft aus den Polizei- und Kriminalregistern und mit Hinweis auf dieses Gesetz sind die Informationen in den meisten der beim Reichspolizeiamt geführten EDV-Register für die einzelne Person nicht zugänglich.

Eine Frage ist natürlich, ob das Datenschutzgesetz die Möglichkeiten der Polizei, die gewünschten Systeme zu entwickeln, eingeschränkt hat. Dies kann nicht eindeutig mit "ja" oder "nein" beantwortet werden. Bisher sind alle vom Reichspolizeiamt eingebrachten Anträge bewilligt worden, und das könnte ein Zeichen dafür sein, daß das Datenschutzgesetz kein Hindernis für die polizeiliche Datenverarbeitung gewesen wäre. Dies ist aber nicht der Fall. Die allgemeine Meinung im Polizeiwesen ist, daß das Datenschutzgesetz die Polizei gezwungen hat, die Wünsche betreffend den Inhalt jedes einzelnen Registers im Sinne des Datenschutzgesetzes genau zu überprüfen, ehe der Antrag an die Datenschutzbehörde überreicht wurde.

Außerdem hat das Reichspolizeiamt, ehe der formelle Antrag gestellt wird, normalerweise informelle Kontakte mit der Datenschutzbehörde gehabt, um gewisse Einzelheiten zu erläutern. Ohne Zweifel hat die Polizei in einigen Systemen wegen des Datenschutzgesetzes auf gewisse Informationen verzichten müssen; diese Fälle sind jedoch selten.

Zusammenfassend kann festgestellt werden, daß das Datenschutzgesetz bisher nur wenige negative Effekte auf die polizeiliche Datenverarbeitung gehabt hat. Als positiv wird dagegen erlebt, daß eventuelle Kritik gegen die Datenbestände der Polizei mit Hinweis auf die Genehmigungen der Datenschutzbehörde zurückgewiesen werden kann. Was in der Zukunft für die Polizei negativ werden könnte, ist die restriktive Einstellung der verschiedenen Behörden und auch zwischen verschiedenen Dateien innerhalb einer Behörde.

Das größte Hindernis für die Weiterentwicklung der polizeilichen Datenverarbeitung ist aber nicht das Datenschutzgesetz, sondern der Mangel an Mitteln und eine sehr komplizierte administrative Behandlung im Zusammenhang mit der Einführung neuer Systeme. Seit dem vorigen Jahr gilt für die Behörden eine Verordnung, die vorschreibt, daß die Einführung neuer EDV-Systeme von der Regierung überprüft werden soll, nicht nur einmal, sondern dreimal während der Systementwicklungsphase. Vor allem werden dabei die ökonomischen Konsequenzen beurteilt, aber auch andere Aspekte können die Beschlüsse der Regierung beeinflussen.

Unter anderen ist in den letzten Jahren die Frage der Dezentralisierung auch im EDV-Gebiet sehr aktuell geworden, teils aus politischen Gründen, aber auch unter dem Gesichtspunkt der Verletzbarkeit der bei den Behörden zentral geführten Dateien. Der Austausch der Computeranlage beim Reichspolizeiamt wurde z.B. um mehrere Monate verzögert wegen einer von der Regierung verlangten Untersuchung bezüglich der Möglichkeiten, die polizeilichen EDV-Systeme zu dezentralisieren. Es wurde jedoch festgestellt, daß unsere gegenwärtigen Systeme auch in der Zukunft zentral geführt werden müssen, weil sie Informationen enthalten, die, wenn sie nicht sämtlichen Polizeibezirken zur Verfügung stehen, ohne Wert sind. Eine Dezentralisierung der polizeilichen Datenverarbeitung ist aber auch von einem Ausschuß, der im Auftrag der Regierung die 1965 eingeführte neue Polizeiorganisation auszuwerten hatte, vorgeschlagen worden. Bis zu einem gewissen Grad wird sicherlich in der Zukunft eine Dezentralisierung durchgeführt werden.

Vor allem wird die gegenwärtige zentrale Datenerfassung bei Eingabe von den Terminals in den Bezirken ersetzt werden und für die größeren Bezirke ist die Einführung von lokalen EDV-Systemen auch zu erwarten.

Obwohl, wie aus dem Vorigen hervorgeht, eine ganze Menge außenstehender Faktoren die Weiterentwicklungspläne der Polizei im EDV-Gebiet beeinflussen, hoffen wir unsere Pläne durchführen zu können, um in einigen Jahren wieder auf ein hohes EDV-technisches Niveau zu kommen.

Rechtsgrundlagen polizeilicher Datenverarbeitung

Edwin Kube *)

1. Polizeiliche Verbrechensbekämpfung als Informationsproblem - eine Skizzierung der Situation

In der Alltagspraxis arbeitet die Polizei bzw. der einzelne Polizeibeamte häufig mit ungesicherten Informationen, mit sog. weichen Daten. Der Beamte schöpft Verdacht und schätzt Gefahrenlagen ein. Er stellt taktische Erwägungen an, wann und wie er vorgehen soll. Er befaßt sich mit Indizien, deren wirkliche Bedeutung im konkreten Fall zunächst unklar sein wird. Bei erheblichem Theoriedefizit der Kriminalistik bringt er vor allem seine Berufserfahrung, sein professionelles Vorwissen in die Fallbearbeitung ein. Er wertet (zum Teil unzureichend) aufbereitete bzw. abrufbare Informationen aus, die sich aus Akten, Karteien und Dateien ergeben. Der Beamte handelt auf der Basis ihn einengender organisatorischer und rechtlicher Gegebenheiten und - soweit überhaupt vorhanden - auch strategischer Konzepte.

Dabei deutet sich an:

- Wesentlichster Problembereich des polizeilichen Entscheidungsprozesses ist die effektive Informationsbeschaffung, -speicherung und -auswertung.

- Bei zunehmender Professionalisierung und Mobilität von Straftätern sowie bei zunehmender Komplizierung und Anonymisierung der Lebensverhältnisse ist die Polizei sowohl im Rahmen der repressiven wie auch der präventiven Verbrechensbekämpfung (1) gehalten, für die Informationssammlung und -verarbeitung extern den Informationsaustausch mit sonstigen Instanzen und deren Dateien, intern die Anwendungsmöglichkeiten der EDV möglichst zu optimieren.

- Rechtliche Vorschriften stellen für die Polizei bzw. den Beamten nicht "motivierende" Handlungsanleitungen dar, sondern sind Begrenzungen für kriminalistische Aktivitäten. Die Auseinandersetzung mit der Rechtsdogmatik liegt außerhalb des polizeilichen Selbstverständnisses.

---

*) Unter Mitwirkung von Heinz Leineweber

> Die Effizienz polizeilicher Verbrechensbekämpfung zeigt sich also primär in der Art und Weise der externen Informationsbeschaffung sowie der internen Datenspeicherung und Datenauswertung. Bei der Informationsbeschaffung geht es hierbei um das Problem des kriminaltaktisch zweckmäßigen Erhebens entscheidungsrelevanter und möglichst abgesicherter Informationen auf nicht unverhältnismäßig aufwendiger Grundlage. Bei der Informationsverarbeitung kommt es darauf an, das Wissen der Polizei als Organisation aufgabenadäquat zu speichern und zu aktivieren (z.B. schnell, zielgerichtet, vollständig, zuverlässig, benutzerfreundlich). Das bekannte Problem ist hierbei: Die Polizei weiß oft mehr, als sie aktuell tatsächlich weiß.

Die wissenschaftliche Betrachtung polizeilicher Arbeit setzt sich grundsätzlich kritisch mit der "Kontrollinstanz" Polizei auseinander. Zum einen betrachtet die sog. neue Kriminologie Verbrechensbekämpfung vorwiegend unter den Aspekten Selektion, Etikettierung und Stigmatisierung. Einzelne Rechtswissenschaftler stellen in jüngster Zeit - vor allem unter dem Vorzeichen eines sich offensiv (2) verstehenden Datenschutzes - legitimerweise, aber dennoch die Polizei deshalb nicht weniger hart treffend, Kernbereiche polizeilicher Arbeitsweisen in Frage. Dabei interessiert sich der Datenschutz für die vielfältigsten Fragen, die von Rechtsproblemen der Datenerhebung bis zu Kooperationsformen mit IKPO-Interpol reichen.

Nicht zuletzt ist der zentrale Begriff der Erforderlichkeit des Speicherns, Veränderns, Übermittelns und Löschens von Daten (vgl. §§ 9, 10, 11, 14 BDSG) (3) im konkreten Fall Anlaß zu erheblichen Konflikten. Die Polizeiführung hat es offenbar zunehmend schwerer, als notwendig erkannte Bekämpfungsansätze im Rahmen der Realisierungsphase des Entscheidungsprozesses (4) rechtlich und politisch durchzusetzen. Dies hängt insbesondere damit zusammen, daß die Polizei in der Vergangenheit zum einen ihre spezifischen Informationsbedürfnisse (5) zu wenig (öffentlichkeits)wirksam geltend gemacht hat; zum anderen hat sie es hingenommen, daß ihre juristischen Grundlagen nahezu ausschließlich von Dritten - neuerdings vor allem von Datenschützern - interpretiert werden (6).

Polizeiliches Verhalten wird anhand der extern vorgenommenen Auslegung von Rechtsvorschriften gemessen, kritisiert, und als rechtlich bedenklich oder gar als unzulässig bezeichnet. Nicht durch den Gesetzgeber oder die Rechtsprechung ausgefüllte "Spielräume" werden von Polizeivertretern höchst selten prononciert juristisch-dogmatisch analysiert und in der Fachliteratur erläutert. Die Polizei ließ sich in der Vergangenheit verschiedentlich in Rechtfertigungspositionen manövrieren, sie ließ sich sozusagen in das juristische Abseits stellen.

2. Rechtsgrundlagen

Polizeiliche Arbeit bei der Verbrechensbekämpfung besteht also in erster Linie in der Gewinnung, Sammlung und Verarbeitung von Daten über persönliche oder sachliche Verhältnisse von Personen. Dieses polizeiliche Handeln ist gesetzmäßig festgelegt und damit auch begrenzt und zwar je nach Zielrichtung in der StPO (hinsichtlich der Strafverfolgung) oder in den Polizeigesetzen der Länder (hinsichtlich der Gefahrenabwehr) (7). Erst die Anwendung der elektronischen Datenverarbeitung bei bestimmten polizeilichen Maßnahmen - wie etwa im Rahmen der Polizeilichen Beobachtung oder der Rasterfahndung - führte zu einer Problematisierung rechtlicher Befugnisse (vgl. etwa die Diskussion zur sog. Schwellentheorie bei § 163 StPO) (8).

Der Einfachheit halber und wegen der weitgehenden Ähnlichkeit des Bundes- und Landesdatenschutzrechtes beziehen sich die folgenden Ausführungen auf bundesrechtliche Regelungen.

a) Rechtmäßigkeit der Datenerhebung

Jüngste Bestrebungen und Gesetzesinitiativen (9) zielen darauf ab, bereits die Erhebung von Daten ausdrücklich in den Begriff der Datenverarbeitung im Sinne es § 1 BDSG einzubeziehen. Aus dem Tatbestandsmerkmal "für die rechtmäßige Aufgabenerfüllung" (§§ 9, 10, 11 BDSG) schließen Vertreter des Datenschutzes schon heute, daß sich die Rechtmäßigkeit der Aufgabenerfüllung von der Erhebung der Daten (10) bis zu deren Auswertung erstrecken müsse. Dazu der Bundesbeauftragte für Datenschutz Bull (11):

> "Es dient nicht der rechtmäßigen Aufgabenerfüllung, wenn Daten verarbeitet werden sollen, die rechtswidrig erhoben worden sind. Da die Erhebung von Daten beim Betroffenen durchgängig als Eingriff in dessen Rechtssphäre angesehen wird, der einer gesetzlichen Ermächtigungsgrundlage bedarf, ist die Feststellung, ob eine solche Erhebungsermächtigung im konkreten Fall besteht, auch für die Verarbeitung der erhobenen Daten von entscheidender Bedeutung. Für die Datenbeschaffung der Sicherheitsbehörden gilt darüber hinaus, daß auch die "Erkundigung" bei Dritten einer gesetzlichen Grundlage bedarf, weil auch dadurch in den geschützten Rechtskreis des Betroffenen eingegriffen wird."

Abgesehen davon, daß zuweilen der Begriff des Eingriffs (im Verhältnis zur bloßen Beeinträchtigung) für bestimmte polizeiliche Aufgaben, wie beispielsweise die Polizeiliche Beobachtung, zu Unrecht bejaht wird (12), ist diese Tendenz der Einbeziehung der Datenerhebung bedenklich. Das Datenschutzrecht würde faktisch in bereits geregelte und den Bürger ausreichend vor Mißbrauch schützende Rechtsbereiche eingreifen: nämlich vor allem in Strafverfahrensrecht und Polizeirecht. So kann es offensichtlich keine Aufgabe des Datenschutzes sein festzustellen, ob beispielsweise eine Vernehmung formell und materiell rechtmäßig durchgeführt wurde oder ob vertrauliche Hinweise rechtmäßig erlangt und in das Verfahren eingeführt wurden, m. a. W. ob also die Polizei nach den Rechtsgrundlagen der StPO die Informationen rechtmäßig gewonnen hat.

Die Einbeziehung der Datenerhebung in das BDSG erscheint daher weder zum Schutz des Bürgers erforderlich, noch würde eine größere Rechtsklarheit erreicht.

Daß insbesondere Strafverfahrensrecht und Polizeirecht an Entwicklungen angepaßt und die Abgrenzungen zum Datenschutz verdeutlicht werden sollten, ist einleuchtend und notwendig. Dies ist jedoch kein originär datenschutzrechtliches Problem.

Folgerung

Die Polizei sollte rechtspolitisch initiativ werden, soweit durch eine einengende Gesetzesauslegung (vgl. etwa § 163 StPO) die Basis für polizeilich notwendige Maßnahmen (z.B. Rasterfahndung) (13) in Frage gestellt wird. Die Kontrolle der Datenerhebung ist - wie schon § 1 BDSG zeigt - keine Aufgabe des Datenschutzes. Diese Regelung muß auch bei einer Änderung des Datenschutzrechts beibehalten werden.

b) Datenverarbeitung als Eingriff

Bei der Frage der Zulässigkeit der Datenverarbeitung sehen Vertreter der sog. Eingriffstheorie (14) in jeder Verarbeitungsform personenbezogener Informationen einen Eingriff in Freiheitsgrundrechte des einzelnen. Dieser Eingriff bedürfe - sofern er nicht durch die Einwilligung des Betroffenen gedeckt ist - der formell gesetzlichen Ermächtigung.

Obgleich diese Auffassung durch den Wortlaut der §§ 3, 9 Abs. 1 BDSG gestützt zu werden scheint, muß sie in dieser pauschalen Formulierung abgelehnt werden. § 3 BDSG ist im Zusammenhang mit § 1 Abs. 1 BDSG zu interpretieren. Danach sind personenbezogene Daten (vgl. § 2 Abs. 1 BDSG) nur vor Mißbrauch bei ihrer Verarbeitung geschützt, nicht jedoch vor einer Verarbeitung schlechthin. § 3 BDSG enthält - bezogen auf Datenverarbeitung - keinen generellen Gesetzesvorbehalt (15), auch nicht hinsichtlich der im BDSG überhaupt geschützten Daten (vgl. § 1 Abs. 2 BDSG).

Die Datenverarbeitung vollzieht sich zudem - ebenso wie die Datenerhebung -, wenn sie von staatlichen Instanzen vorgenommen wird, oft nicht in Form nach außen dringender behördlicher Akte (16) oder von Zwangsmaßnahmen; diese sind eher bei "Begleitmaßnahmen" zur Erlangung von Informationen festzustellen; insoweit ist etwa auf den körperlichen Eingriff bei zwangsweiser ed-Behandlung oder die zwangsweise Entnahme einer Blutprobe zu verweisen. Die Datenverarbeitung ist in den meisten Fällen für den Betroffenen nicht erkennbar und somit unbeeinflußbar. Dennoch- oder gerade deshalb - fühlt sich der einzelne evtl. durch die Übermacht an Wissen und Herrschaft auf seiten des

Staates eingeengt oder gar bedroht. Dieses eher emotionale Unbehagen gegenüber modernen Technologien kann aber nicht zur Folge haben, daß der Datenschutz de facto zur generellen Beeinträchtigung effektiver staatlicher Tätigkeit führt, zumal diese eben personenbezogene Daten essentiell voraussetzt (17).

In diesem Zusammenhang ist mit Kloepfer festzustellen (18):

> "Generelle Konzeptionen von staatlichen (und privaten) Informationseingriffen, d.h. die Fassung im Prinzip aller Datenerhebungs- und -verarbeitungsvorgänge als Eingriffe, beeindrucken zwar durch ihre gerade Einfachheit, siedeln aber notwendig an der Grenze zur Simplizität des Zirkelschlusses, der von den gewünschten rechtlichen Eingriffskonsequenzen her auf den Eingriffscharakter schließt. Kann sich der Staat dann überhaupt noch mit dem einzelnen befassen, ohne "einzugreifen"? Wird damit der Gesetzesvorbehalt nicht in untragbarer Weise zum Befassungsvorbehalt ausgedehnt, mit der Folge, daß wesentliche Garantiegehalte des Gesetzesvorbehalts bei klassischen Grundrechtseingriffen verwässert werden? Hierin liegt ja ein Grundproblem extensiver Verfassungsinterpretation: die auf besondere Problemlagen zugeschnittenen Verbürgungen werden so stark ausgedehnt, daß ihre konkreten Garantiegehalte zur Vermeidung unhaltbarer und unrealistischer Ergebnisse abgeschwächt werden müssen, wodurch dann im Ergebnis die Ursprungsverbürgungen ausgehöhlt werden."

Die strikte Anwendung der Eingriffstheorie ist also abzulehnen. Die konzeptionelle Unsicherheit des BDSG sowie die fehlende Definition des darin geschützten Rechtsgutes haben dazu beigetragen, nach sonstigen Kriterien für die Zulässigkeit der Verarbeitung personenbezogener Daten zu suchen.

Ein differenzierender Ansatz macht den Eingriffscharakter und die daraus resultierende Notwendigkeit einer Eingriffsbefugnis vor allem von der zu erfüllenden Aufgabe und damit von der Art der zu verarbeitenden Daten abhängig (19). Nach dieser Literaturmeinung sollte es dabei jedoch weniger darauf ankommen, ob die Informationen öffentlich

zugänglichen Quellen entstammen oder nicht (20), sondern auf die Sensibilität der Daten. Datenspeicherung, -veränderung und -übermittlung durch staatliche Stellen haben nach dieser Auffassung zumindest dann als Eingriff zu gelten, wenn Umfang und Sensibilität der Daten einen solchen Grad erreichen, daß das ungezielte und unkontrollierte Streuen der Daten den Betroffenen in der Bewertung durch seine Mitmenschen herabsetzen kann (21). Dabei wird auf die Frage abgehoben, ob nicht etwa schon die Speicherung wegen der Zweckbestimmung der Datei die Ehre des Betroffenen mindert (22) und dieser damit ein Interesse an der Geheimhaltung der Speicherung hat (23). Diese Voraussetzungen sind bei staatlichen Datenverarbeitungsmaßnahmen in sehr unterschiedlicher Weise erfüllt; doch wird man nach Maßgabe dieser Kriterien der Speicherung und Veränderung personenbezogener Daten in polizeilichen EDV-Systemen vielfach Eingriffscharakter zubilligen müssen (24).

Nach solcher Literaturmeinung wird sich der Verdächtige/Beschuldigte hier mehr als bloß "erfaßt" fühlen und er wird zumeist nicht nur hinsichtlich der Inhalte, sondern auch schon hinsichtlich der Tatsache der Speicherung ein hochgradiges Geheimhaltungsinteresse haben. Derartige Zweckmäßigkeitsgrundsätze dienen bislang als "Ersatzkriterien" für eigenständige Datenschutzmaßstäbe.

Nach meiner Auffassung eignen sich solche Grundsatzüberlegungen höchstens für die Frage des Eingriffs gegenüber Verdächtigen/Beschuldigten. Soweit Dritte - wie etwa Anzeigeerstatter und Hinweisgeber - in Dateien als solche erkennbar gespeichert werden - und zwar vorübergehend wie in SPUDOK (25) - kommt diesen Maßnahmen keine Eingriffsqualität zu. Überhaupt sollte bei der Frage nach dem Eingriffscharakter der Speicherung und der Veränderung von Daten eines Bürgers die Antwort vorrangig von der objektiven Erheblichkeit der Maßnahme abhängig gemacht werden. Die Intensitätsschwelle im Sinne eines Eingriffs wäre dann überschritten, wenn durch die Datenmenge und die Datenqualität der Betroffene "durchleuchtet" und "bewertet" werden kann. Ist dagegen der Datenbestand so "dünn", daß praktisch keine Aussage gemacht werden kann, handelt es sich um eine bloße Beeinträchtigung, die jeder gemeinschaftsbezogene und -gebundene Bürger (26) dem allgemeinen Lebensrisiko zurechnen muß (27).

Folgerung:

Nicht jede Verarbeitung (und auch nicht schon jede Erhebung) personenbezogener Daten durch die Polizei stellt einen grundrechtsrelevanten Eingriff dar und ist daher an eine besondere Ermächtigung geknüpft. Der Eingriffsbegriff ist hier weitgehend strittig. Kommt einem polizeilichen Datenverarbeitungssystem generell bzw. Datenverarbeitungsmaßnahmen bezogen auf einen bestimmten Betroffenen Eingriffscharakter zu, so stellt sich die Frage nach der Befugnisnorm.

c) Befugnisnorm im Bundesdatenschutzgesetz?

Nach § 3 BDSG ist die Verarbeitung personenbezogener Daten nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt. Geht man von dem Eingriffscharakter einer polizeilichen Datenverarbeitungsmaßnahme aus, so stellt sich nun die Frage, ob für die Speicherung, Veränderung bzw. Übermittlung personenbezogener Daten die für den öffentlichen Bereich einschlägigen §§ 9 und 10 BDSG als selbständige Eingriffsbefugnisse für Maßnahmen der polizeilichen Datenverarbeitung herangezogen werden können.

Einmal werden die §§ 9 und 10 BDSG für nahezu überflüssig angesehen, wollte man sie nicht als Ermächtigungsnormen und somit als Erlaubnisnorm im Sinne des § 3 BDSG anerkennen (28). Dagegen spricht, daß dann - abweichend von den üblichen Anforderungen an gesetzliche Ermächtigungsnormen - völlig konturlose, praktisch unbegrenzte Eingriffsnormen existierten (29). Darüber hinaus stellt sich die wesentlichere Frage, ob es denn dem Bundesgesetzgeber hätte gestattet sein können, in einem Gesetz, das in seinem ersten und zweiten Abschnitt bestimmte Aspekte des Verwaltungsverfahrens regelt, materielle Eingriffsbefugnisse zu formulieren, die inhaltlich auch noch in den dem Landesgesetzgeber obliegenden Materien zum Tragen kämen (30).

Folgerung:

Soweit für Maßnahmen polizeilicher Datenverarbeitung Eingriffsbefugnisse notwendig sind, können diese nicht dem Bundesdatenschutzgesetz entnommen werden (31).

d) Befugnisnorm aus anderen Gesetzen?

Bejaht man im Einzelfall den Eingriffscharakter von Maßnahmen der Datenverarbeitung, so muß man scheinbar zu dem Ergebnis kommen, daß polizeiliche Datenverarbeitung eigentlich ohne Rechtsgrundlage ist, da ausdrückliche rechtliche Regelungen von Datenverarbeitungsmaßnahmen in der StPO und in den Polizeigesetzen fehlen. Dies Ergebnis wäre sicherlich unbefriedigend.

Die bekannte Rechtsprechung des Bundesverwaltungsgerichts zur Aufbewahrung von ed-Unterlagen bietet jedoch Ansätze zur rechtlichen Argumentation:

Es ist heute unstrittig, daß die Frage der Rechtsgrundlage für die Aufbewahrung von ed-Unterlagen und die bestimmte Bezeichnung in Akten und Sammlungen, also die Speicherung und Verarbeitung der erlangten Informationen, ebenfalls anhand der Befugnisnorm für die ed-Behandlung (§ 81b StPO) zu beurteilen ist. Mit anderen Worten: Ist die Polizei berechtigt, sich Informationen zu beschaffen, so muß es für sie auch zulässig sein, diese Informationen zu verarbeiten.

Folgerung:

Für die polizeiliche Datenverarbeitung bedeutet dies, daß die Befugnisse für Eingriffe in das allgemeine Persönlichkeitsrecht in Form der Speicherung, Veränderung und Übermittlung personenbezogener Daten den prozessualen und polizeirechtlichen Befugnissen als "Folgeeingriff" zu entnehmen sind (32). Die Datenverarbeitungsbefugnis ist also den polizeilichen Ermächtigungsnormen als "Annex" zuzuordnen, solange keine audrücklichen Vorschriften für Datenverarbeitungsmaßnahmen vorhanden sind (33). Allerdings besteht für die Datenverarbeitung im BKA eine Rechtsgrundlage im BKA-Gesetz. Insoweit ist insbesondere auf § 2 Abs. 1 Ziff. 1 zu verweisen, der bestimmt, daß das Amt alle Nachrichten und Unterlagen für die polizeiliche Verbrechensbekämpfung zu sammeln und auszuwerten hat (34).

e) BKA-Gesetz und Inpol - Bund -

Nach der vom Bundesbeauftragten für den Datenschutz vertretenen Rechtsauffassung ist es dem BKA unter anderem nicht erlaubt, die Daten aller Straftäter oder Tatverdächtigen zentral zu speichern. In seinem zweiten Tätigkeitsbericht vom 18. Januar 1980 heißt es (35):

> "Eine zentrale Speicherung von Straftätern oder vermuteten Straftätern in polizeilichen Informationssystemen des Bundeskriminalamtes ist bereits nach dem Wortlaut des BKA-Gesetzes nur für überregionale Täter möglich. Das ergibt sich aus der Grundsatzvorschrift des § 1 Abs. 1 Satz 2 BKAG, aus dem Begriff der Erforderlichkeit für die Übermittlung von Daten an das BKA durch die Landeskriminalämter i. S. § 3 BKA-Gesetz und aus dem Vergleich mit § 4 BKA-Gesetz, der allein für Freiheitsentziehungen ... eine umfassende Meldepflicht vorsieht. Eine totale Erfassung polizeilich relevanter Vorgänge würde im übrigen gegen den Grundsatz der Verhältnismäßigkeit verstoßen, so daß auch deshalb der Begriff "alle Nachrichten" i.S. des § 2 Abs. 1 Nr. 1 BKAG einschränkend ausgelegt werden muß."

Die Auffassung des Datenschutzbeauftragten wird im 3. und 4. Tätigkeitsbericht wiederholt (36).

Diese Rechtsmeinung, die im Rahmen der Konzeptualisierung des Kriminalaktennachweises zum Tragen gekommen ist, hätte in anderen vom Datenschutz ebenfalls bereits angesprochenen Bereichen - wie den daktyloskopischen Daten - unter polizeilichen Gesichtspunkten nicht akzeptable negative Folgen. Hier zeigt sich deutlich, daß eine offensive Strategie des Datenschutzes nicht nur rechtlich zum Teil angreifbar ist, sondern auch für die Polizeipraxis tief einschneidende Wirkungen zur Folge haben kann (37).

§ 1 BKA-Gesetz und die Zentralstellenbefugnisse des Amtes wurden unlängst von dem BKA-Mitarbeiter Kubica eingehend behandelt (38). Dabei wurde deutlich gemacht, daß eine Fülle von Gründen gerade für eine wörtliche Auslegung des § 2 Abs. 1 Nr. 1 sprechen,wonach das Amt als Zentralstelle

alle Nachrichten und Unterlagen für die polizeiliche Verbrechensbekämpfung zu sammeln und auszuwerten hat. Der wesentliche Grund ergibt sich aus der amtlichen Begründung der Novelle von 1973. Darin heißt es u.a., daß das Bundeskriminalamt seine Aufgabe als Zentralstelle für den elektronischen Datenverbund nur wahrnehmen könne, "wenn ihm sämtliche Unterlagen über Straftaten und Straftäter zur Verfügung stehen" (39) . Es wurde also ausdrücklich der Zusatz gestrichen, der lautete: "... soweit die Nachrichten und Unterlagen nicht eine lediglich auf den Bereich eines Landes begrenzte Bedeutung haben". Bereits aus den Gesetzesmaterialien ergibt sich also eindeutig, daß die Streichung mit dem Ziel der Erweiterung der Zentralstellenbefugnis erfolgte, zumal die Notwendigkeit des Ausbaues des BKA als Informations- und Kommunikationszentrale für die gesamte Polizei besonders betont wird. Außerdem wird im Hinblick auf die Änderung des § 2 Abs. 1 Nr. 1 hervorgehoben, daß die Frage einer überregionalen Bedeutung von Nachrichten und Unterlagen sich in der Mehrzahl der Fälle abschließend erst nach einem Vergleich mit anderen vorliegenden Erkenntnissen beurteilen lasse (39a).

Auch ein Blick auf die einzelnen Aufgaben, die im § 2 Abs. 1 niedergelegt sind, verdeutlicht, daß § 1 Abs. 1 Satz 2 keine erschöpfende Aufgabenbeschreibung darstellen kann, sondern nur eine Kernfunktion des Amtes voranstellt. § 2 Abs. 1 Nr. 1 enthält im Hinblick auf die Aufgabenbeschreibung (§ 1 Abs. 1 Satz 2) ein Mittel, wie dieser erwünschte Zustand erreicht werden soll (40).

Im einzelnen kann also nachgewiesen werden, daß durch die Änderung des BKA-Gesetzes im Jahre 1973 auch eine veränderte Definition des Aufgabenbereiches im rechtlichen Sinne bezweckt und bewirkt worden ist und daher der Aufgabenumschreibung in § 1 Abs. 1, S. 2 BKA-Gesetz, wonach das Amt den Straftäter zu bekämpfen hat, "soweit er sich international oder über den Bereich eines Landes hinaus betätigt oder voraussichtlich betätigen wird", keine die Vorschrift des § 2 Abs. 1 Nr. 1 einschränkende Funktion zukommt.

Folgerung:

Rechtlich vertretbar erscheint, daß das BKA alle Nachrichten und Unterlagen über Straftaten sammelt und auswertet. Ein anderes Problem ist, daß aus politischen Gründen - vgl. etwa die prinzipielle Regionalisierung des Kriminalaktennachweises - die rechtlichen Möglichkeiten nicht voll ausgeschöpft werden.

Eine weitere Folgerung:

Nach meiner Auffassung wäre eine notwendige Konsequenz aus dem Gebot der Transparenz, die im politischen Bereich Wirkung erzeugenden Tätigkeitsberichte des Bundesdatenschutzbeauftragten so abzufassen, daß bei differierenden Rechtsmeinungen die eigene Auffassung des Datenschutzbeauftragten in der Auseinandersetzung mit den anderen Meinungen kundgetan wird. Die Interpretation der §§ 1 Abs. 1 Satz 2 und 2 Abs. 1 Nr. 1 BKA-Gesetz stellt ein Beispiel dar, welches das Spannungsverhältnis zwischen Rechtsmeinung des Datenschutzes einerseits und offenkundigen polizeilichen Praxiserfordernissen sowie erheblich abweichenden "verschwiegenen" Rechtsmeinungen andererseits offenkundig macht.

f) Datenübermittlung anderer Behörden an Polizeidienststellen

Einen diffizilen und strittigen Problembereich, der hier nur kurz erwähnt werden kann, stellt die Übermittlung von Daten anderer Behörden dar. Der Bundesdatenschutzbeauftragte ging bisher offensichtlich davon aus, daß § 10 Abs. 1 BDSG für die Zulässigkeit der Übermittlung personenbezogener Daten stets eine Aufgaben- und Befugnisnorm voraussetze und daß wegen der Zweckbindung der Daten und wegen der vorzunehmenden Prüfung der Erforderlichkeit der Übermittlung insoweit on-line-Verbindungen etwa zum Kraftfahrt-Bundesamt oder zum Ausländerzentralregister grundsätzlich unzulässig seien (41). Dies gelte dann, wenn die Datei im Sinne eines Zentralregisters genutzt werden soll.

Dieser Rechtsauffassung wird von polizeilicher Seite insbesondere entgegengehalten (42), daß § 161 StPO - unbeschadet Sonderregelungen wie §§ 35 und 68 ff. SGB X - der Staatsanwaltschaft die Befugnis einräume, von allen Behörden Auskunft zu verlangen und Ermittlungen jeder Art entweder selbst vorzunehmen oder durch die Behörden oder Beamten des Polizeidienstes vornehmen zu lassen. Allerdings wird vereinzelt inzwischen von Justizvertretern geltend gemacht, daß "Strafverfolgungsdaten" prinzipiell "Justizdaten" seien, über die die Polizei nicht ohne weiteres verfügen könne.

Hier wird offenbar die Furcht vor einer "Verselbständigung" der Polizei heraufbeschworen und der Forderung nach eigenem exekutivem Unterbau der Staatsanwaltschaft Nachdruck verliehen (42a).

Dabei wird jedoch verkannt, daß die im Rahmen der Strafverfolgung von der Polizei erhobenen und gesammelten Daten - soweit sie dateimäßig gespeichert und ausgewertet werden - ihre bloß straftat- und straftäterbezogene Qualität verlieren; die Nutzung der Dateien verfolgt nämlich auch originär-polizeiliche Zwecke. Dazu zählt einmal das Ziel der Gefahrenabwehr im Rahmen zukünftiger polizeilicher Lagen; nicht zu vernachlässigen ist des weiteren der meist von Polizeiexternen übersehene Zweck, der sich in der Erstellung polizeilicher Lagebilder, Kriminalitätsanalysen sowie Einsatz- und Organisationsplanungen zeigt. Als sog. Hilfsbeamte der Staatsanwaltschaft kommt die Polizei ihrer Pflicht zur Übersendung ihrer Verhandlungen (§ 163 Abs. 2 StPO) durch Zuleiten der Ermittlungsakten an die Staatsanwaltschaft nach. Seit langem führt die Polizei Kriminalaktensammlungen, hat die Polizei einen kriminalpolizeilichen Meldedienst aufgebaut und sammelt sonstige Daten, die zwar im Rahmen der Strafverfolgung anfallen können, jedoch polizeiinternen Charakter aufweisen (z.B. Darstellung und Auswertung eines operativen Einsatzes unter kriminaltaktischen Gesichtspunkten). Die prinzipiell

einzelfallbezogene Sachleitungsbefugnis der Staatsanwaltschaft würde überdehnt, wollte man durch Definition der Daten als "Justizdaten" die Zugriffsbefugnis der Staatsanwaltschaft auf alle polizeilichen Daten, die nicht "reine Präventivdaten" sind, erstrecken.

Als weiteres Problem im Rahmen der (erweiterten) Amtshilfe wird von der Datenschutzseite gesehen, daß nach § 2 Abs. 2 Nr. 2 BDSG das Bereithalten von Datenbeständen zum Abruf bereits als Übermittlung des Gesamtbestandes gilt. Allerdings weiß jeder Sachkenner, daß die Polizei nicht die Übermittlung aller Daten - etwa vom Kraftfahrt-Bundesamt die Namen aller Kfz-Halter wünscht -, sondern nur jeweils Daten zu der Person, deren Namen sie in das System eingeben würde.

Bei rechtsdogmatischer Betrachtung ist auch hier offen, wann eine Datenübermittlung überhaupt einen Rechtseingriff darstellen würde. Nach der Kommentierung von Gallwas u.a. hat eine Übermittlung jedenfalls dann Eingriffscharakter, "wenn sie besonders umfassend oder besonders intensiv ist, also vielfältige oder sensible Informationen über den Betroffenen einschließt" (43). Diese Voraussetzungen sind m. E. offensichtlich prinzipiell nicht bei Datenübermittlungen der negativen Rasterfahndung erfüllt. Im Kommentar von Gallwas u.a. heißt es weiter, daß beim Bejahen eines Eingriffs mindestens die Aufgabenzuweisung der empfangenden Stelle auf einer Rechtsnorm beruhen müsse(44).

Folgerung:

Das Problem der Zulässigkeit der Datenübermittlung an die Polizei ist einerseits ganz wesentlich für die effektive Aufgabenerfüllung. Andererseits besteht gerade auch zu diesem Fragenkomplex eine erhebliche Unsicherheit in juristisch-dogmatischer Hinsicht. Mehr Klarheit sollte auch hierzu im Rahmen der Novellierung des Bundesdatenschutzgesetzes geschaffen werden.

3. Resümee

Mit meinem Beitrag wollte ich an verschiedenen Beispielen aufzeigen, daß manche Rechtsfragen im Bereich der polizeilichen Datenverarbeitung rechtsdogmatisch noch weitgehend ungeklärt sind, auch wenn eine solide rechtsstaatlich geprüfte Grundlage für die automatisierte Datenverarbeitung vorhanden ist (45). Dieses Defizit besteht unabhängig von zuweilen strittigen, ich möchte sagen "normalen" Problemen, nämlich ob ein bestimmtes Verhalten - wie etwa der Umfang des Datenbestandes einer speziellen Datei oder die Verweigerung des Auskunftersuchens eines Betroffenen - unter dem Gesichtspunkt des Datenschutzes rechtlich vertretbar ist oder nicht. Allerdings darf die Klärung der Rechtsfragen nicht zu einer Überstülpung der polizeilichen Ablauforganisation mit einem feinmaschigen Netz rechtlicher Detailregelungen führen. Der Polizei muß - insbesondere im Rahmen neuer Bekämpfungsansätze - ein angemessener Bewertungsspielraum sowie eine gewisse Experimentierfreiheit zugebilligt werden. Nur dann kann sie der sich ständig wandelnden Kriminalität wirksam begegnen.

Außerdem war es mir ein Anliegen aufzuzeigen, daß im Interesse einer rationalen rechtlichen Diskussion die unterschiedlichen Meinungen offen ausgetragen werden und der Diskussionsstand mit in die eigene Begründung einfließen sollte. Während beim Datenschutz eine offensive, auch offenbar bewußt die Öffentlichkeit einbeziehende Strategie festzustellen ist, ist bei der Polizei zu konstatieren,

daß sie sich weitgehend der rechtsdogmatischen Auseinandersetzung, aber auch schon der öffentlichen, vor allem aber der im politischen Raum wirksamen Darstellung ihrer Informationsinteressen entzieht. Es ist daher nicht verwunderlich, daß zuweilen beide Seiten durch ihr Verhalten zu Spannungen beitragen, die durch mehr Transparenz vermieden werden könnten.

Anmerkungen

(1) Zu der juristisch nicht unbestrittenen Aufgaben- bzw. Befugniszuweisung für die präventive Verbrechensbekämpfung Bull, Rechtsprobleme der polizeilichen Informationssammlung und -verarbeitung, Datenverarbeitung im Recht 1/1982, S. 4 m.w.H. und Schwan, Die Abgrenzung des Anwendungsbereiches der Regeln des Straf- und Ordnungswidrigkeitenverfolgungsrechtes von dem des Rechtes der Gefahrenabwehr, Verwaltungsarchiv 1979, S. 109 ff.

(2) Vgl. etwa Bull, Ziele und Mittel des Datenschutzes, Königstein 1981, S. 8 m.w.H. und auch Schomerus, Datenschutz oder Datenverkehrsordnung?, Zeitschrift für Rechtspolitik 1981, S. 293.

(3) Erforderlichkeit bedeutet, daß das Mittel geeignet ist, nicht durch ein anderes, vor allem milderes ersetzt werden kann und in einem angemessenen Verhältnis zum angestrebten Erfolg steht.

Die Speicherung nicht erforderlicher Daten ist datenschutzrechtlich nur dann unzulässig, wenn dadurch schutzwürdige Belange beeinträchtigt würden. "Sie werden nicht beeinträchtigt, wenn eine Rechtsvorschrift die Speicherung oder Übermittlung ausdrücklich vorschreibt"; so Schomerus, Datenschutz oder Datenverkehrsordnung? a.a.O., S. 292. In diesem Zusammenhang vgl. insbesondere § 2 Abs. 1 Nr. 1 BKAG.

(4) Polizeiliche Entscheidungsprozesse kann man - bei Verwendung eines entscheidungstheoretischen Ansatzes - in verschiedene, sich überlappende und durch Rückkoppelungsprozesse gekennzeichnete Phasen unterteilen (generell für die öffentliche Verwaltung vgl. Kube, Den Bürger überzeugen. Stil, Strategie und Taktik der Verwaltung, Stuttgart, Berlin, Köln, Mainz 1973, S. 15 ff. m.w.H.).

(5) Dazu Stümper, Datenschutz und Sicherheitsprobleme, Kriminalistik 1982, S. 234 ff.

(6) In diesem Zusammenhang interessant: Evers, in: Polizei-Führungsakademie (Hrsg.), Recht und Praxis des Datenschutzes im Bereich der Inneren Sicherheit, Münster 1980, S. 121 ff. Vgl. auch Riegel, Datenschutz bei den Sicherheitsbehörden, Köln, Berlin, Bonn, München 1980, etwa S. 12 ff.

(7) Zum Problem der sog. doppelfunktionalen polizeilichen Maßnahmen und zur sog. Ergänzungslehre vgl. Schwan, a.a.O., S. 109 ff. Vgl. auch Riegel, Probleme des Datenschutzes im Bereich der polizeilichen Tätigkeit, Die Polizei 1978, S. 273.

(8) Riegel, Datenschutz bei den Sicherheitsbehörden a.a.O., S. 7 ff. Zur Schwellentheorie Schwan a.a.O., S. 116 f.

(9) Vgl. z.B. Simon/Taeger, Rasterfahndung, Baden-Baden 1981, S. 37 ff. sowie Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (jüngster Referentenentwurf des BMI).

(10) Festzustellen ist, daß keine einheitliche Auffassung über den Begriff der Erhebung (z.B. deren Beginn) besteht; vgl. etwa Schoreit, Problematische Informationssammlung und -verarbeitung durch die Polizei, Datenverarbeitung im Recht 1/1982, S. 39.

(11) Rechtsprobleme der polizeilichen Informationssammlung und -verarbeitung a.a.O., S. 14.

(12) In diesem Zusammenhang Steinke, Die Rechtmäßigkeit von polizeilichen Fahndungsmaßnahmen unter Berücksichtigung des Datenschutzes, Deutsches Verwaltungsblatt 1980, S. 433 ff.

(13) Vgl. Ermisch, Die systematisierte Fahndung - Rasterfahndung -, in: Kube/Störzer/Brugger, Wissenschaftliche Kriminalistik - Grundlagen und Perspektiven, Bd. 1, Wiesbaden 1983; Riegel, Rechtsprobleme der Rasterfahndung, Zeitschrift für Rechtspolitik 1980, S. 300 ff.

(14) Ein Hauptvertreter ist Schwan; vgl. ders., Datenschutz, Vorbehalt des Gesetzes und Freiheitsgrundrechte, Verwaltungsarchiv 1975, S. 120 ff. Differenzierter Bull, Verfassungsrechtlicher Datenschutz, in: Gedächtnisschrift für Sasse, Das Europa der zweiten Generation, Kehl, Straßburg, Bd. 2, 1981, S. 877 ff. (insbs. S. 879). Ablehnend z.B. Kloepfer, Datenschutz als Grundrecht, Königstein 1980, S. 22 und Evers, Rechtsfragen des Datenschutzes bei der Informationsübermittlung zwischen Polizei und Nachrichtendiensten, Die Polizei 1980, S. 237; vgl. auch BVerfG 47, S. 46 (78 ff.) und Schomerus, Datenschutz oder Datenverkehrsordnung? a.a.O., S. 292 m.w.H.

(15) So Ordemann/Schomerus, Bundesdatenschutzgesetz mit Erläuterungen, München, 3. Aufl. 1982, Anm. 1 zu § 3.

(16) Dazu Louis, Grundzüge des Datenschutzrechts, Köln, Berlin, Bonn, München 1981, Rdnr. 96 m.w.N.

(17) So Kloepfer a.a.O., S. 22.

(18) Kloepfer a.a.O., S. 23.

(19) Vgl. Wiese, Grundsatzfragen des Datenschutzrechts, Deutsches Verwaltungsblatt 1980, S. 866.

(20) Krüger, Verfassungsrechtliche Grundlagen des Datenschutzes, Die Polizei 1980, S. 231.

(21) Gallwas/Schneider/Schwappach, Bundesdatenschutzrecht, Stuttgart, Berlin, Köln, Mainz, Stand: Dez. 1981, § 9 Rdnr. 13, § 10 Rdnr. 25.

(22) Gallwas/Schneider/Schwappach a.a.O., § 1 Rdnr. 18.

(23) Simitis/Dammann/Mallmann, Kommentar zum Bundesdatenschutzgesetz, Baden-Baden, 3. Aufl. 1981, § 10 Rdnr. 30 ff.

(24) Riegel, Datenschutz bei den Sicherheitsbehörden a.a.O., S. 5.

(25) In diesem Zusammenhang vgl. auch Dateienrichtlinien 4.2.

(26) BVerfG 34, S. 238 (246) und 35, S. 202 (220 f.).

(27) In diesem Zusammenhang ausführlich - vor allem auch zur Anlegung und Führung von Kriminalakten - Ahlf, Der Begriff des "Eingriffes" insbesondere bei kriminalpolizeilicher Tätigkeit und die sog. "Schwellentheorie" zu § 163 Abs. 1 StPO (in Druck).

(28) Schmid, Zulässigkeit und Notwendigkeit polizeilicher Datenverarbeitung, Die Neue Polizei 1979, S. 167 ff. Auernhammer, Bundesdatenschutzgesetz, Köln, Berlin, Bonn, München, 2. Aufl. 1981, Einf. Rdnr. 37 und § 9 Rdnr. 2.

(29) Riegel, Probleme des Datenschutzes im Bereich der polizeilichen Tätigkeit a.a.O., S. 272; Burhenne/Perband, EDV-Recht, Bd. 3 (Komm. zum BDSG), Bielefeld, Stand: 1982, § 9 Rdnr. 13.

(30) Burhenne/Perband a.a.O., § 9 Rdnr. 17.

(31) Riegel, Datenschutz bei den Sicherheitsbehörden a.a.O., S. 5 f. Schomerus, Datenschutz oder Datenverkehrsordnung? a.a.O., S.293.

(32) Schwan a.a.O., S. 138 f.

(33) Zu weitgehend Schoreit, der die Strafverfolgungsdaten als "Justizdaten" klassifiziert: vgl. Schoreit, Datenschutz und Informationsrecht im Bereich der Strafverfolgung unter Berücksichtigung der Dateien des Bundeskriminalamtes, Zeitschrift für Rechtspolitik 1981, S. 74 ff., ders. Datenverarbeitung im Bereich der Strafverfolgung und "gesamtpolizeilicher Auftrag", Deutsche Richterzeitung 1982, S. 403 f. mit Vorschlägen zu einer gesetzlichen Regelung der polizeilichen Datenverarbeitungsmaterie . Siehe auch Bull, Rechtsprobleme der polizeilichen Informationssammlung und -verarbeitung a.a.O., S. 16, und Ernesti, EDV bei der Staatsanwaltschaft, Deutsche Richterzeitung 1982, S. 258 f.

(34) Ordemann/Schomerus, Bundesdatenschutzgesetz mit Erläuterungen a.a.O., Anm. 1.2 zu § 9.

(35) Bundestagsdrucksache 8/3570, S. 47.

(36) Bundestagsdrucksache 9/93, S. 49 und 9/1243, S. 26.

(37) Vgl. auch Ordemann/Schomerus a.a.O., Anm. 1.2 zu §9: "Das Bundeskriminalamt könnte seine Funktion als zentrale Auskunftsstelle nur noch partiell erfüllen."

(38) Kubica, § 1 BKA-Gesetz und die Zentralstellenbefugnisse des Bundeskriminalamtes, Öffentliche Verwaltung und Datenverarbeitung 3/1982, S. 109 ff. Zu demselben Ergebnis gelangte auch Hessel, Gesetz über die Einrichtung eines Bundeskriminalpolizeiamtes (BKA-Gesetz), Kommentar, Wiesbaden 1979, S. 21. Anderer Ansicht Riegel, Zur verfassungs- und datenschutzkonformen Auslegung der Zentralstellenbefugnis nach § 2 BKAG, Öffentliche Verwaltung und Datenverarbeitung 1-2/1980, S. 20 ff. sowie ders., Stellung und Aufgaben des Bundeskriminalamtes: Überblick und Probleme, Deutsches Verwaltungsblatt 1982, S. 723 f.

(39) Bundestagsdrucksache 7/178, S. 8. Zum Folgenden vgl. auch Stenographischer Bericht der 36. Sitzung v. 24.05.1973, S. 2028.

(39a) Als Entgegnung auf Riegel in Deutsches Verwaltungsblatt 1982, S. 720 ff. überzeugend und mit weiteren Argumenten aus den Gesetzesmaterialien Dietel, Zur Zentralstellenkompetenz des Bundeskriminalamtes, Deutsches Verwaltungsblatt 1982, S. 939 f.

(40) Kubica a.a.O., S. 110.

(41) Bull, Fahndung und Datenschutz, in: Bundeskriminalamt, Möglichkeiten und Grenzen der Fahndung, Wiesbaden 1980, S. 57 ff.

(42) Etwa Herold, Aussprache in: Bundeskriminalamt a.a.O. S. 73 f.

(42a) Vgl. außer Fußnote 33 auch Schoreit, Staatsanwaltschaft und Polizei im Lichte fragwürdiger Beiträge zur Reform des Rechts der Staatsanwaltschaft, Zeitschrift für Rechtspolitik 1982, S. 288 ff. sowie Ernesti, Informationsverbund Justiz - Polizei, siehe in diesem Band S. 121 .

(43) Gallwas/Schneider/Schwappach, Bundesdatenschutzrecht a.a.O., § 10 Rdnr. 26.

(44) Gallwas/Schneider/Schwappach a.a.O.

(45) So Bull, Rechtsprobleme der polizeilichen Informationssammlung und -verarbeitung a.a.O., S. 9 f. allerdings mit der Forderung nach weiteren Rechtsnormen, um nicht zuletzt "den großen technisch-organisatorischen Apparat überhaupt für die Leitungsinstanzen voll beherrschbar und verantwortbar zu machen".

Informationsverbund Justiz - Polizei

Günter Ernesti

Bei einem Informationsverbund Justiz - Polizei geht es um bessere Arbeitsmittel für die erfolgreiche und reibungslose Zusammenarbeit von Justiz und Polizei im Interesse der gemeinsamen Aufgaben. Auch müssen Justiz und Polizei im Datenschutzrecht ihren Platz finden und einnehmen.

Informationsverbund wird hier verstanden als Austausch von Daten unter den berechtigten Teilnehmern zu gemeinsamen Zwecken in einem Rechner-Rechner-Verbund, d.h. zwischen elektronischen Datenspeichern der Justiz und der Polizei(1).

Tendenzen für und gegen den Verbund

Der Gedanke einer solchen Verbindung ist nicht neu. Die Befürwortung beginnt demonstrativ mit den Leitsätzen der Gemeinsamen Konferenz der Justiz- und Innenverwaltungen aus dem Jahre 1975. Leitsatz 1 fordert gegenseitige Unterrichtung durch Beteiligung an den Informations- und Kommunikationssystemen der Polizei und Justiz. Das übernehmen fortan die Konferenzen der Justizminister und -senatoren (2). Auch der Generalbundesanwalt und die Generalstaatsanwälte der Bundesrepublik fordern parallel ständig die Verwendung modernster technischer Mittel auf dem Gebiet der Strafrechtspflege und verlangen, über eigene Anlagen Daten selbst eingeben oder abrufen zu können, jedenfalls aber, weil unerläßlich, Zugriff der Staatsanwaltschaften auf die Personen- und Sachfahndung von INPOL. Das sind Stimmen der höchsten für die Strafverfolgung verantwortlichen Stellen des Staates.

Der Innenbereich ist über die ersten Ansätze nicht hinausgegangen. Er hat den am 17. November 1978 zugesagten Erfahrungsbericht nicht erstattet. Er neigt bisher zur Abkapselung und Isolierung(3). Es liegen aber Anzeichen dafür vor, daß nunmehr eine ernsthafte Überprüfung aller anstehenden Fragen stattfinden wird.

Verbundfähige Dateien und Daten

a) Polizei

Im Polizeibereich fällt der Blick auf die Erschließungs- und Informationssysteme wie Kriminal-

aktennachweis (KAN), Personenfahndung, Haftdatei, Sachfahndung und PIOS. Von der Verbundfrage werden hier ausgenommen z.B. die Straftaten/Straftäter-Datei wegen ihrer Entwicklungsstufe, die Datenbank Daktyloskopie, weil sie offenbar nicht verbundfähig ist, die an sich bedeutsame Literaturdokumentation sowie das vergleichbare Justizsystem JURIS, weil für diese Untersuchung der Verkehr mit personenbezogenen Daten im Vordergrund steht, und die Spurendokumentationssysteme oder zentralen Tatmittelnachweise für bestimmte Kriminalitätsbereiche, da hier die Kriminaltechnik überwiegt (4).

Am Beispiel KAN und PIOS treten bereits bestimmende Merkmale hervor. Der KAN enthält Akten von kriminalpolizeilicher Relevanz über vermutete bevorstehende oder zu verhütende sowie über begangene und aufzuklärende Straftaten (5). Gespeichert werden also beieinander präventiv-polizeiliche und repressive Daten. PIOS enthält gleichermaßen bewertete wie unbewertete Daten. Die Justiz wird aber grundsätzlich Abstand halten von präventivpolizeilichen Daten, da diese anderen Zwecken als Justizzwecken dienen, und von unbewerteten Daten, da diese forensisch nichts tragen. Dies gilt für jeden Informationsverbund zwischen Justiz und Polizei.

b) Justiz

Auf Seiten der Justiz steht als vollständige Datei das Bundeszentralregister mit Erziehungs- und Gewerbezentralregister bereit. Leider ruht die gemäß § 10 Abs. 2 der 1. BZR VwV zulässige Planung der direkten Fernabfrage berechtigter Behörden zum BZR (6). Jedenfalls aber bahnt sich das Modell Fernübertragung Staatsanwaltschaft - BZR an. Die Datenzentrale Schleswig-Holstein als Rechenzentrum übersendet dem BZR ab November 1982 auf dem Postweg Magnetbänder mit Strafregisteranfragen der beiden Staatsanwaltschaften des Landes, die mit ihrer EDV die Daten eingegeben hatten. Die Bänder werden beim BZR teilautomatisch, nämlich durch Aufruf am Bildschirm bearbeitet. Die erarbeiteten Auskünfte gehen ausgedruckt an die Staatsanwaltschaften. Der nächste Schritt wird die Einschaltung des Leitungsweges zur Übermittlung der Anfragen sein, wenn auch bei weiterer intellektueller Prüfung der Trefferfrage. Dies ist zwar keine

automatische Datenverarbeitung, aber in einem komplexen Bereich ein erster Schritt. Die Ergebnisse eines verschiedentlich vervollständigten Probelaufs der schleswig-holsteinischen Staatsanwaltschaften mit dem BZR sollten vor weiteren Erörterungen abgewartet werden.

Im Bereich der Strafjustiz gibt es - abgesehen von den 1976/1977 eingerichteten Probeanschlüssen des Generalbundesanwalts sowie der Staatsanwaltschaften Frankfurt/Main und München I an INPOL zur Abfrage bei der Personen- und Sachfahndung- für eine EDV der Staatsanwaltschaften verschiedene Pläne der Bundesländer, teils im Rahmen von Sicherheitsplänen, und auch die praktische Anwendung der EDV als Dauereinrichtung.

Ein arbeitendes Registersystem auf EDV-Basis wird soeben schrittweise bei den Staatsanwaltschaften in Schleswig-Holstein aufgebaut und steht als fertiges Konzept den übrigen Bundesländern zur Verfügung. Es ist ein Verfahren zur Geschäftsstellenautomation der Staatsanwaltschaften (GAST). Es enthält Daten, die das BZR nicht zur Verfügung stellen kann und ist daher rechtlich selbständig. GAST begleitet als elektronisches Register die Anzeige oder Akte nach Erfassung der Personendaten über die Stationen Ermittlungsverfahren, gerichtliches Verfahren und Strafvollstreckung bis zur Aktenvernichtung. Es besteht keine Verbindung zur Polizei. Die Logik von GAST ist aufgebaut wie die der Datenbank INPOL mit Gruppenbildung, Gruppenvorspann, vergleichbaren Zugriffsmerkmalen und Zugriffsbeschränkungen; es besitzt Haft-, Fahndungs- und Fristenkontrollen. Bei allem handelt es sich um "verdateten" Akteninhalt und um die Übertragung von Bestimmungen der bundeseinheitlichen Aktenordnung und StA-Statistik auf die EDV (7).

Die Staatsanwaltschaft als Repräsentant der Justiz

Fragen nach einem Informationsverbund stellen nicht nur die Staatsanwaltschaften, sei es für einen Verbund mit der Polizei oder untereinander oder mit den Gerichten, auch die Justizvollzugsanstalten - diese wegen der Haftdaten - und ebenso die Justizministerien wegen der Auslieferungssachen. Es gibt insoweit einen

logischen Gegenpart zum Datenverbund im Polizeibereich und mit dem Polizeibereich. Die ganz unterschiedlichen Verbundfragen prüfe ich in dem Ausschnitt Staatsanwaltschaft - Polizei. Sollte nämlich zwischen Staatsanwaltschaft und Polizei aus tatsächlichen oder rechtlichen Gründen ein Inforamtionsverbund nicht zustande kommen, so wäre er mit anderen Stellen der Justiz kaum mehr zu erwarten. Diese würden sich dann höchstens intern verbinden.

Die Staatsanwaltschaft als datenverarbeitende Stelle

Will die Staatsanwaltschaft selbständig in einen Verbund eintreten, muß sie sich als datenverarbeitende Stelle (§ 2 Abs. 3 Nr. 1 BDSG) legitimieren. Dies ist für die Staatsanwaltschaft eine neue Frage. Für die Erörterung wird als Muster das BDSG zugrunde gelegt, obwohl das Gesetz in den Bundesländern mit eigener Datenschutzgesetzgebung nicht gilt (§ 7 Abs. 2 BDSG). Die Zulässigkeit eigener Datenverarbeitung bemißt sich im BDSG nach den §§ 1, 3 und 45.

Die Bedeutung der StPO im Hinblick auf §§ 1, 3, 45 BDSG

§ 1 BDSG muß am Anfang der Prüfung stehen, weil diese Bestimmung den Rechts- und Schutzbereich des BDSG bestimmt. Das Gesetz will den Mißbrauch zum Nachteil des einzelnen, nicht aber die Datenverarbeitung als solche verhindern; denn ohne Datenverarbeitung wären Staat und Wirtschaft nicht mehr funktionsfähig. Das bekräftigt der Regierungsentwurf zum BDSG mit der ausdrücklichen Absage an jede Maschinenstürmerei (8).

§ 3 BDSG spricht ein Verbot mit Erlaubnisvorbehalt aus, um den genannten Zweck des § 1 - Schutz vor Mißbrauch - durch die Kontrolle der Datenverarbeitung zu sichern. Da Rechtsvorschriften, die die Datenverarbeitung in diesem Sinne gestatten, nicht nur Gesetze im formellen Sinne sind, sondern auch Verordnungen, ja selbst Satzungen oder autonome Statuten oder Tarifverträge und Betriebsvereinbarungen (9), gehört ganz zweifellos die Strafprozeßordnung nach Charakter und Regelungsmaterie hierhin.

In der StPO geht es ständig und ausschließlich um die Verarbeitung personenbezogener Daten. Ermitteln heißt Daten erheben und verarbeiten. Die StPO, eingebettet in das GVG, hält für Zwecke der Datenverarbeitung ein

in sich geschlossenes System von geschriebenen und ungeschriebenen Rechtsgrundsätzen bereit, in dem ineinandergreifend in einem jahrelangen Entwicklungsprozeß die widersprüchlichen Interessen zwischen dem für die Gemeinschaft wahrgenommenen staatlichen Strafanspruch und dem individuellen Persönlichkeitsrecht als Datenschutzrecht des einzelnen ausgewogen geregelt sind. Der Datenverarbeitungsprozeß verläuft nach der StPO unter den gesetzlich geordneten und vom Verhältnismäßigkeitsgrundsatz gesteuerten Bedingungen des Ermittlungsverfahrens, der Anklage, der Hauptverhandlung, des Urteils und der Strafvollstreckung. Hier präsentiert sich die Vorentscheidung des Gesetzgebers in der Gestalt eines geschlossenen Rechtssystems, wo Geheimhaltung und Offenbarung, Öffentlichkeit und Veröffentlichung die Beteiligung von unmittelbar und mittelbar Betroffenen, wo Beginn, Umfang und Ende des Datenschutzes abgewogen und im Ergebnis abschließend geregelt sind. Hierdurch ergibt sich eine Eigengesetzlichkeit des Rechtspflegeverfahrens, die sich im Bereich des Datenverkehrs und des Datenschutzes ständig bemerkbar machen muß.

Den Vorrang derartiger Bestimmungen, ja Regelungskomplexe, achtet § 45 BDSG. § 45, die Subsidiaritätsklausel, ist von extremer Bedeutung (10). Durch § 45 verzichtet das BDSG auf seinen Ausschließlichkeitsanspruch (11). Er macht das BDSG zum subsidiären Auffanggesetz (12). § 45 hatte schon im Gesetzgebungsverfahren die Aufmerksamkeit der Gesetzgebungsorgane erregt und wurde erst im Gesetzgebungsverfahren auf den jetzigen Stand gebracht. Als weitergeltende Bestimmung, die der § 45 in einigen wenigen Beispielen zitieren will, wurden nicht nur Datenschutzbestimmungen festgeschrieben. Der Begriff des Datenschutzes wurde gestrichen, und als weitergeltend wurden nun auch verschiedene andere Vorschriften, z.B. die §§ 52 bis 55 und 161 StPO, benannt (13).

Durch diese Systematik des BDSG werden die Strafverfolgungsorgane in der Anwendung der auf Datenverarbeitung bezogenen geschlossenen Teile der StPO vom BDSG freigestellt. In diesem Sinne verstehe ich auch die Stellungnahme der Bundesregierung 1981 (14).

Was das Bayerische Datenschutzgesetz in seinem Artikel 2 Abs. 2 ausdrücklich geregelt hat, nämlich den Vorrang von Verfahren der Rechtspflege vor den Vorschriften des Bayerischen Datenschutzgesetzes mit dem Ergebnis, daß nicht die Einzelbestimmung der StPO, sondern das Verfahren der StPO insgesamt von den Beschränkungen der Datenschutzgesetze ausgenommen ist, weil es in der StPO um einen geschlossenen Regelungskomplex geht und daher nicht die eine Bestimmung getrennt von der anderen existiert oder betrachtet werden kann - dieses Ergebnis ist nur eine Deklaration dessen, was § 45 BDSG bei sinngemäßer Auslegung ebenso ergibt. Im Landesbereich überdies folgt der Vorrang der StPO bereits aus Artikel 31 GG. Die StPO ist ein Bundesgesetz, dessen Anwendung durch ein Landesdatenschutzgesetz nicht gebrochen oder eingeengt werden darf.

Ergebnis: Die StPO genügt dem Erlaubnisvorbehalt des § 3 BDSG. Die Staatsanwaltschaft ist grundsätzlich an der Datenverarbeitung nicht gehindert.

Speicherung

Da das BDSG die Regeln der Datenverarbeitung in einzelne Akte zerlegt, nun zur Datenspeicherung nach § 9 Abs. 1 BDSG. Auch dieser Bestimmung wird die Staatsanwaltschaft gerecht, da das Speichern und Verändern personenbezogener Daten zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben erforderlich ist. Das folgt aus dem Legalitätsprinzip (§ 152 Abs. 2 StPO) d.h. aus der Verpflichtung, wegen aller verfolgbaren Straftaten einzuschreiten. Die Staatsanwaltschaft muß demgemäß Daten erheben und verarbeiten und besitzt insoweit also ausdrückliche Erhebungs- und Erfassungskompetenz.

Benötigt die Staatsanwaltschaft wegen des Eingriffscharakters der Speicherung ein Sondergesetz? Die den Gesetzesvorbehalt wahrende Bestimmung des § 9 BDSG kann im Grunde nur am Einzelfall geprüft werden. Die sogenannte Eingriffstheorie vertritt demgegenüber die Ansicht, daß jede Stufe der Informationsbeschaffung und Datenverarbeitung unterschiedslos ein Eingriff sei (15). Sie reißt sich damit vom Zügel des § 1 BDSG los und verselbständigt sich, obwohl der Gesetzgeber in § 1 BDSG durch die Einführung der Mißbrauchsgrenze Unterscheidungen eröffnen will (16).

Die Eingriffstheorie ist in ihrer geraden Einfachheit beeindruckend, birgt aber die Gefahr in sich, zu nivellieren und hat wohl schon den Schritt vom Gesetzesvorbehalt zum Befassungsvorbehalt getan (17). Vor allem arbeitet sie mit der Fiktion des ausnahmslosen Eingriffs, während der Gesetzgeber, der Fiktionen durchaus kennt (§ 2 Abs. 2 Nr. 2 BDSG), eine solche Fiktion hier gerade nicht aufgestellt hat. Durch diese Fiktion wird die Theorie für Unterschiede blind. Der beachtenswerte Kern der Eingriffstheorie ist die Rolle des Persönlichkeitsrechts und somit die Frage des Grundrechtseingriffs durch Datenverarbeitung (18). Hierbei ergeben sich Abwägungsfragen, die sich in der Gemeinschaftsgebundenheit und -bezogenheit des einzelnen als Teil des Ganzen treffen müssen. Dazu gehört, daß sich Kriterien wie Eingriff oder Erforderlichkeit nicht verselbständigen, sondern nur im Kontext mit der Mißbrauchsformel des § 1 BDSG angewandt werden dürfen. Datenverarbeitung ist nicht schon per se ein Grundrechtseingriff, der einer gesetzlichen Ermächtigung bedarf (19).

Der Gesetzesvorbehalt des § 9 BDSG ist erfüllt, wenn fachspezifische Vorschriften vorliegen, die der jeweiligen öffentlichen Stelle Aufgaben übertragen, die nur auf der Grundlage bestimmter Informationen erfüllbar sind (20). Gesetzliche, an personenbezogene Voraussetzungen anknüpfende Eingriffs- und Leistungsermächtigungen beinhalten die akzessorische Kompetenz zur Erhebung, Bearbeitung und Verwertung derjenigen personenbezogenen Daten, die zur rechtmäßigen Gesetzesausführung erforderlich sind (21).

Diese Aufgaben- und Befugniszuweisung (22) hat der Gesetzgeber durch die StPO mit Generalklausel und Einzelregelungen, verbunden mit dem auf konkrete Straftatbestände zugreifenden Legalitätsprinzip, vorgenommen. Der Gesetzgeber hat in der StPO mithin - wie oben dargelegt - über das Recht des einzelnen, allein gelassen zu werden, d.h. über den status negativus des Artikels 2 Abs. 1 i.V.m. Artikel 1 Abs. 1 GG entschieden (23). Die Anwendung der StPO bringt Eingriffe. Die Datenverarbeitung ist akzessorischer Begleitumstand der Eingriffe. Datenverarbeitung im Rahmen und für Zwecke der StPO ist keine Beeinträchtigung schutzwürdiger Belange des einzelnen, ist kein Mißbrauch (§ 1 BDSG), sondern ist Ausführung des Gesetzes.

Der Rechtsgüterschutz der StPO als Ausprägung des verfassungsmäßigen Individualrechtsschutzes führt zu keiner anderen Beurteilung (24). Bis zur Grenze der Sonderregelungen wie Blutentnahme, Durchsuchung, Telefonüberwachung usw., also bis zu Maßnahmen, die nicht akzessorisch sind, sondern eigenes Gewicht besitzen, wird im Ermittlungsverfahren zu Recht die Generalklausel des § 161 StPO angewandt, wie z.B. bei der strafprozessual erforderlichen Rasterfahndung und polizeilichen Beobachtung (25).

Genügt mithin die StPO dem Gesetzesvorbehalt des § 9 BDSG, so kommt es nicht mehr auf die Erforderlichkeit einer Speicherung in einer ganz bestimmten Form, nämlich gerade in einer Datei, an. Entscheidend ist vielmehr die Notwendigkeit, die Daten überhaupt festzuhalten (26).

Ist eine Speicherung überhaupt erforderlich, so gestattet § 9 BDSG, daß dies in Form einer Datei geschieht und stellt die Wahl des Verfahrens, ob manuell oder automatisiert, frei. Es fragt sich also nicht, ob die Anlegung einer Datei vermieden werden kann, sondern ob das Festhalten der Daten durch die Aufgabe gefordert wird. Alle Daten, auf die das zutrifft, dürfen in automatisierten oder sonst rationalisierten Verfahren in einer Datei gespeichert werden (27).

Datenstatut

Allerdings bedeutet dies, um nochmals auf den Gesichtspunkt der Erforderlichkeit einzugehen, nicht, daß die Staatsanwaltschaft nach der StPO ungebunden Datenverarbeitung betreiben dürfte. Einer solchen Auffassung müßte ausdrücklich widersprochen werden. Die aus der StPO heraus zulässige elektronische Datenverarbeitung hat die Staatsanwaltschaft nach dem verfassungskräftigen Übermaßverbot zu begrenzen (28). Dies betrifft Dateninhalt, Datenmenge, Zugriffs- und Übermittlungskontrolle. Es bedarf eines Datenstatuts mit Arbeitsanweisungen, Richtlinien und Kontrollen. Das bedeutet z.B. Einführung von Codewörtern, Einschränkung der Zugriffsberechtigung, Einrichtung von Schutzstufen, Protokollierung des Datenverkehrs durch Logband, aber auch Datenreduzierung und frühzeitige Löschung. Hier gelten die 10 Anforderungen der Anlage zum BDSG über die Datensicherung (29). Durch das Datenstatut wird also auch die Verbuchung der Daten im Kontext gesteuert und minimalisiert.

Ergebnis: Die Staatsanwaltschaft kann, nach § 3 BDSG zugelassen, gemäß § 9 BDSG Daten speichern, d.h. gemäß § 2 Abs. 2 Nr. 1 BDSG Daten erfassen, aufnehmen oder aufbewahren und hierzu eine eigene elektronische Datei benutzen, kann also in einem Datenverbund selbständig mitwirken.

Datenübermittlung

In der Datenübermittlung konzentrieren sich Verbundfragen spezieller und genereller Natur.

Schon das Bereithalten zum Abruf gilt nach § 2 Abs. 2 Nr. 2 BDSG als Übermitteln (30). Diese Bestimmung, die bei Direktanschlüssen praktisch wird, blockiert jeden vernünftigen Datenverkehr; denn sie stellt die Fiktion auf, daß bei einem on-line-Verkehr der Datenbestand übermittelt sei. Das führt zu realitätsfernen Annahmen. Dann wären schon durch einen Verbund als solchen Millionen von Daten als übermittelt anzusehen. Dergleichen ist eine vom Gesetzgeber nicht gewollte Folge. Der Datenverkehr verlangt lediglich die Erforderlichkeit, die sich auf den einzelnen Abruf bezieht. Die Formulierung des § 2 Abs. 2 Nr. 2 BDSG muß daher in dem Sinne verstanden werden, daß die Einräumung einer Abrufbefugnis für Daten, deren Kenntnis bereits abstrakt erforderlich ist, nicht generell unzulässig ist (31).

Ständiger Verbund Staatsanwaltschaft - Polizei

Werden bei Einführung eines ständigen Informationsverbundes unzulässigerweise gesetzliche, auch verfassungsmäßige funktionale Trennungen überspielt?

Offenbar muß Ausgangspunkt einer solchen Untersuchung § 10 BDSG sein. Er fragt nach Erforderlichkeit, rechtmäßiger Aufgabenerfüllung und Zuständigkeit als den Voraussetzungen jeder Datenübermittlung und somit auch einer Übermittlung im Dauerverbund. Die Antwort darauf ergibt sich aus dem Rechtsverhältnis Staatsanwaltschaft - Polizei. An diesem Rechtsverhältnis läßt sich der Charakter der Daten bestimmen, die im Verbund zu bewegen sind. Hiernach beantwortet sich auch die Kardinalfrage der Zweckbestimmung und -bindung der Daten im Datenverbund.

Das Grundverhältnis Staatsanwaltschaft - Polizei

Maßgebend sind die §§ 152 GVG, 152, 160, 161, 163 StPO. Sie sind die Antwort des Reichsgesetzgebers von 1879 auf bis dahin unbefriedigende Zustände. Der Gesetzgeber beendete die Doppelrolle des Richters. Er legte die Ermittlungen in die Hände des Staatsanwalts. Er beschnitt auch die Befugnisse der Polizei, die, jedenfalls in Preußen, zuletzt Aufgaben anderer Stellen an sich gezogen hatte (32).

Um der Staatsanwaltschaft für ihre Ermittlungen den fehlenden Unterbau zu verschaffen - ein in den Beratungen als schwerer Übelstand bezeichneter Mangel -, wurde im Hinblick auf die gleichgerichteten Zwecke der Sicherheitspolizei das Institut des Hilfsbeamten der Staatsanwaltschaft geschaffen und die Leitung der Ermittlungen dem Staatsanwalt übertragen. Das Muster war die französische Police Judiciaire. § 152 GVG sollte erklärtermaßen die Organisation der Staatsanwaltschaft und Polizei regeln. Der Einsatz der Polizei wurde als eine Prozeß- und Verfahrensvorschrift in § 161 Satz 2 StPO geregelt (33).

Nur in Kenntnis dieser Vorgeschichte tritt die Bedeutung der §§ 152 GVG, 160, 161, 163 StPO für das Ermittlungsverfahren hervor. Staatsanwaltschaft und Polizei stehen im Ermittlungsverfahren nicht als gleichermaßen kompetente Behörden nebeneinander, sondern das Ermittlungsverfahren läuft in der ausschließlichen Kompetenz der Staatsanwaltschaft. Das wird einerseits an der Sachleitungsbefugnis des Staatsanwalts deutlich - Verfahrensverbindung und -trennung, Bildung von Sammelverfahren, Anforderung von Auskünften oder ständiger Unterrichtung (34) - und zeigt sich andererseits an dem Recht, das Verfahren abzuschließen, nämlich im eigenen Namen selbständig, entscheidungskräftig und unter Ausschluß anderer Behörden über den Ausgang des Verfahrens zu befinden, was den Inbegriff der Kompetenz ausmacht (35).

§ 163 StPO, von der Polizei in der Praxis mit Duldung der Staatsanwaltschaft fortentwickelt zu selbständigem Vorgehen auf dem Gebiete der Strafverfolgung, ändert an dieser Rechtslage nichts. Die Erforschungspflicht der Polizei nach § 163 entspricht nur derjenigen der Staatsanwaltschaft nach § 160 und bleibt eine Durchgangszuständigkeit. Die Kriminalpolizei handelt hier als ein

Organ der Staatsanwaltschaft, als Bevollmächtigte, und dient den Zwecken, deren Trägerin die Staatsanwaltschaft ist. Die Tätigkeit der Polizei ist kein behördliches Beistandleisten im Sinne des Artikels 35 GG (36), denn die Polizei kann einerseits ohne Ersuchen Ermittlungen anstellen, hat aber andererseits nicht nachzuprüfen, ob die Staatsanwaltschaft des geforderten Beistandes bedarf. "Die Polizei ist zwar organisatorisch und ressortmäßig keine Justizbehörde wie die Staatsanwaltschaft, wird aber durch die StPO der Strafjustiz dienstbar gemacht. Die Behörden und Beamten des Polizeidienstes sind als verlängerter Arm der Staatsanwaltschaft nicht nur bei der Ausführung einer Weisung dieser Behörde tätig, sondern auch dann, wenn sie nach § 163 Abs. 1 StPO von sich aus handeln. Die Polizeiorgane werden als Justizbehörden im funktionellen Sinn tätig" (37).

Charakter der Repressivdaten

In dieser Beleuchtung wird der Charakter der Daten sichtbar, die im Ermittlungsverfahren bewegt werden. Die im Zuge repressiver Tätigkeit erlangten Daten sind Justizdaten. Das betrifft nicht nur Haftdaten, die allein im Justizbereich erwachsen und gilt auch nicht nur für die etwa 30% jener Ermittlungsverfahren, die bei der Staatsanwaltschaft durch Anzeigen der Ämter und Rechtsanwälte oder anderer Stellen beginnen, sondern ebenso für die übrigen ca. 70% der Verfahren, die mit Anzeigen bei der Polizei oder dem Amtsgericht (§ 158 StPO) ihren Anfang nehmen oder von der Polizei selbständig in Gang gesetzt werden; denn hier erwachsen Daten aus repressiver Tätigkeit, und das sind Justizdaten.

Der Bereich der Justizdaten darf nicht verundeutlicht werden, etwa indem man den Begriff der Prävention und vorbeugenden Verbrechensbekämpfung ausdehnt. Das BZRG spricht in zutreffender Unterscheidung von der Verhütung und der Verfolgung von Straftaten (§ 39 I Nr. 5). Der Begriff der präventiv-polizeilichen Tätigkeit ist offenbar beweglich. Wählt man § 8 ME als Beispiel, so betrifft er zunächst die Abwehr einer konkreten Gefahr. Mit diesem Inbegriff präventiv-polizeilicher Zwecke verbindet sich die vorbeugende polizeiliche Aufgabe der Verhütung von Straftaten als Gefahrenabwehr. Die Poli-

zei empfindet die Generalklausel des § 8 als zu eng (38). Auch bei abstrakter Gefahr gibt es polizeiliches Einschreiten als Vorbeugungsmaßnahme (39). Die vorbeugende Verbrechensbekämpfung - ein Ausdruck des § 5 BKAG - wird zur Gefahrenvorsorge. Andererseits gibt es auch den Begriff der Vorbeugungsarbeit (§ 2 Abs. 1 Nr. 7 BKAG). Sie stellt etwas anderes dar und greift doch wieder in den Bereich zurück, soll nämlich auch Abschreckung und Sozialisierung umfassen (40).

Verbindet man das mit der Vorstellung, daß das BKA nach § 2 Abs. 1 Nr. 1 BKAG als Nachrichtensammelstelle das Recht habe, bei allen in Betracht kommenden Stellen, z.B. bei der Justiz, Daten zu erfassen, also Auskünfte von der Justiz zu fordern (41), so entsteht der Gedanke an einen gesamtpolizeilichen Auftrag mit dem Bestreben, ein Spektrum der Vorbeugung weit auszudehnen (42). Möglicherweise liegt dem ein Ausspruch zugrunde, wie er in den Thesen der Innenminister des Jahres 1975 formuliert worden war und wo es unter Abschnitt I.2.1.1 hieß, daß der Sicherheitsauftrag der Polizei den gesamten Bereich der Verbrechensbekämpfung umfasse, also die Verbrechensbekämpfung und die Strafverfolgung (43). Solche Ausweitungen müssen auf Rechtsbedenken stoßen, wenn sie nicht begrenzt werden (44).

Die Trennung der vorbeugenden von der strafverfolgenden Tätigkeit der Polizei ist unbedingt erforderlich, um Zuständigkeit, Datencharakter und Datenverkehr abzugrenzen. Ausgangspunkt ist die Einsicht, daß die Begehung einer Straftat das Scheitern der Prävention anzeigt. Hier endet die Prävention, und was bis dahin Prävention war, wird zur Repression. Wo beides ausnahmsweise zusammentrifft, weil breit angelegte polizeiliche Maßnahmen laufen, muß gleichwohl nach dem Zweck der konkreten Maßnahme entschieden werden. Der Zweck gibt Aufschluß über die Ermächtigungsgrundlage und damit über die Rechtmäßigkeitsvoraussetzungen und beantwortet übrigens auch die Frage des Rechtsweges (45). Die abstrakte Amtsbefugnis ist also nicht entscheidend. Im etwaigen Zweifel entscheidet vielmehr das Schwergewicht der Tätigkeit. Es kommt auf den Teil des Vorgehens an, der dem Einschreiten das Gepräge gibt (46). Nochmals: Sobald der Beamte zureichende tat-

sächliche Anhaltspunkte für eine Straftat sieht, ist der Zweck seines Handelns selbstverständlich, weil pflichtgemäß, Ermittlungstätigkeit (§§ 160, 161, 163 StPO). Dann hat der Polizeibeamte den präventiven Bereich verlassen und übt funktionelle Justiztätigkeit aus. Im Zweifel schlägt die weiterreichende repressive Tätigkeit durch. So hat das OVG Münster (a.a.O.) in der Anwendung der damaligen PDV 384.1 eine regelmäßig repressive Tätigkeit gesehen.

Konzentration der Justizdaten

Der beständigen Klarstellung im Rechtlichen muß im Tatsächlichen die Bezeichnung der erlangten Daten als Justizdaten entsprechen. Dies geschieht in der elektronischen Datei durch besondere Kennung. Das ist zu praktizieren nach Art der jetzt verwendeten polizeilichen Kennungen der Länder, Ämter und Daten. Auch jetzt findet z.B. keine weitere automatisierte Ausgabe von Folgedaten statt, wenn die Zielinformation auf Daten stößt, die nicht in verbundfähigen INPOL-Bereichen enthalten sind.

Entgegenwirkende Umstände

Die Justizdaten müssen für den Staatsanwalt verfügbar sein, denn er trägt die Verantwortung für die Strafverfolgung im Ermittlungsverfahren, und er ist Herr der anfallenden Daten (47). Dem widersprechen einzelne Tätigkeiten des BKA als Zentralstelle in Anwendung des BKAG und BDSG, dem widersprechen Regeln aus den Dateien- und KpS-Richtlinien, dem widerspricht in mehrfacher Hinsicht die Praxis.

a) Die Kompetenzabgrenzung des BKA als Zentralstelle nach § 2 BKAG ist nicht eindeutig, wenn auch von einer Grundverantwortung des BKA auszugehen ist und das BKA grundsätzlich datenverarbeitende Stelle sein soll und ist (48). Als demnach speichernde Stelle im Sinne von § 2 Abs. 3 Nr. 1 BDSG trifft das BKA Verfügungen über Daten und verarbeitet sie, soweit Repressivdaten betroffen sind, anstelle des Herrn der Daten, d.h. anstelle der Staatsanwaltschaft, und dies selbständig ohne oder bei nur beschränkter Beteiligung der Staatsanwaltschaft.

b) Dem Charakter der Justizdaten und der Sachleitungsbefugnis des Staatsanwalts widersprechen auch Teile der KpS- und Dateienrichtlinien. In den Dateienrichtlinien (5.3; 5.6) wird dem Staatsanwalt nur grundsätzlich Auskunft aus den polizeilichen Daten in Aussicht gestellt. Außerdem muß er die Rechtmäßigkeit seines Auskunftsbegehrens belegen, das BKA behält sich die Entscheidung vor. Ferner ist die Sachleitungsbefugnis des Staatsanwalts vor Übermittlung von Daten vom BKA an andere Stellen ebensowenig abgesichert wie bei Auskünften an den Betroffenen oder bei Aussonderung oder Löschung von Daten.

c) Der Datenumfang, der sich aus Nr. 2.3 der KpS-Richtlinien ergibt (49), ist nicht mit der StPO (§ 163 Abs. 2 StPO) zu vereinbaren. Nach dieser Bestimmung hat die Polizei (unverzüglich) ihre Verhandlungen der Staatsanwaltschaft zu übersenden. Dies ist ein typischer Ausdruck der Sach- und Datenherrschaft des Staatsanwalts gemäß §§ 152 GVG, 160, 161 StPO.

Anstelle der Durchgangszuständigkeit der Polizei, die sich aus § 163 Abs. 2 StPO ergibt, besteht aber in der Praxis und nach den KpS-Richtlinien eine Durchgangszuständigkeit der Justiz: Einerseits werden gemäß Nr. 2.3 "Doppelakten" zu den Ermittlungsakten gebildet, andererseits die darauf bezogenen Daten nach Nr. 7.5 der Dateienrichlinien über lange Zeit gespeichert, weil die Mitziehensklausel bei jedem von den Anlieferern gemeldeten neuen Speicherungsanlaß die Speicherungsfrist nochmals mitzieht. Zu den gespeicherten Daten gehören nach Nr. 5.6 Dateienrichtlinien auch getilgte und tilgungsreife Daten, die nach § 49 BZRG für die Justiz, weil gelöscht oder zu tilgen, nicht mehr verfügbar sind (50).

§ 163 Abs. 2 StPO zwingt dazu, die repressiven Daten als Akten und in sinngemäßer Anwendung auch als gespeicherte Daten an die Staatsanwaltschaft abzugeben (51). Was Ermittlungsmaterial war und nicht als unerheblich ausgeschieden wird, wird Bestandteil der Ermittlungsakten und entsprechendes gilt für Daten (52). § 163 Abs. 2 StPO kann weder durch das BDSG außer Wirksam-

keit gesetzt werden (§ 45 BDSG) noch durch das BKA-Gesetz, das nach seiner Regelungsmaterie eine Datenverkehrsordnung für den Polizeibereich ist, nach Beratungs- und Regelungsgegenstand aber kein Änderungsgesetz zu GVG und StPO (§§ 152 GVG, 160, 161, 163 StPO) (53).

d) Im Fahndungsbereich hat die in Teil 2.1.1.3 der PDV 384.1 fortgeschriebene Praxis dazu geführt, daß Haftbefehle, die die Staatsanwaltschaft den örtlichen Polizeidienststellen mit Vollstreckungsersuchen ohne Antrag auf Ausschreibung im INPOL-System (KP 21) übersandt hat, nach erfolglosem Vollstreckungsversuch von der Polizei in eigener Entschließung als nunmehr polizeiliche Ausschreibung in das INPOL-System, wenn auch beschränkt auf die Fahndungsregion des Landes und für eine beschränkte Laufzeit, eingegeben werden. Sowohl bei Haftbefehlen wie bei Vollstreckungshaftbefehlen muß es jedoch der Staatsanwaltschaft und allein ihrer Entscheidung im Rahmen von Zweckmäßigkeit und Übermaßverbot vorbehalten bleiben, ob und wie gefahndet wird. Es ist daher mit dem Gesetz nicht vereinbar, daß, wenn die Staatsanwaltschaft nach Erlaß eines Haftbefehls bewußt von einem Antrag auf Ausschreibung im INPOL-System absieht, die Polizei den Haftbefehl in das System eingibt. Umgekehrt ist es offenbar StPO-widrig, wenn dem ungehinderten Zugriff der Staatsanwaltschaften auf das Fahndungssystem Beschränkungen entgegengesetzt werden.

Korrektur durch den Verbund

Bei einem elektronischen Datenverbund Justiz - Polizei werden die Dateienrichtlinien an Bedeutung verlieren, weil die Übermittlung dann regelmäßig nicht von Entscheidungen, sondern von der Organisation des Systems abhängt, worüber es gemeinsame Konventionen geben wird (54). Alle Ordnungserwägungen müssen hier zu einer Regelung führen, die der typischen justitiellen Entstehung und Bestimmung von Daten im Justizbereich Rechnung trägt, der gesetzlichen Sachleitungsverantwortung des Staatsanwalts entspricht sowie dem Willen des § 163 Abs. 2 StPO voll gerecht wird.

Diese Bestimmung verlangt, daß anstelle einer Materialkonzentration bei der Polizei in Form von zurückgebliebenen Justizdaten diese Daten an den Herrn des Ermittlungsverfahrens, die Staatsanwaltschaft, gelangen. Dem muß durch Eingabe- und Abrufbefugnis in der Personen- und Sachfahndung sowie in der Haftdatei Rechnung getragen werden. Entsprechendes muß für bewertete Daten in KAN und PIOS gelten.

Was wird durch die Konzentration der Justizdaten bei der Justiz erreicht? Es wird die Zweckbindung der Justizdaten und damit ein beherrschendes Prinzip des Datenschutzgedankens voll zur Wirkung gebracht. Dabei muß allerdings einer Fehldeutung vorgebeugt werden. Wenn Justizdaten und Justizakten gemäß § 163 Abs. 2 StPO so deutlich für die Staatsanwaltschaft angefordert werden, so ist unverkennbar, daß die Polizei hinreichende Unterlagen zur Gefahrenabwehr und Verhütung von Straftaten, wenn nicht besitzen, so in Reichweite haben muß. Offenbar ermöglicht es aber gerade der elektronische Informationsverbund Staatsanwaltschaft - Polizei, daß die Justizdaten - sprich Repressivdaten - hier für die Polizei zur Verfügung gehalten werden (55).

Verfassungsrechtliche Gesichtspunkte

Im weiteren Sinne berührt ein Informationsverbund Staatsanwaltschaft - Polizei das Informationsgleichgewicht, sei es speziell als Persönlichkeitsschutz, den die Datenschutzregelungen des BDSG im Auge haben, sei es als verfassungsmäßiger Datenschutz, der das Informationsgleichgewicht zwischen staatlichen Bereichen betrifft. Zugrunde liegt allen Erwägungen die Erkenntnis, daß die Einschaltung der Elektronik geeignet ist, Grenzen aufzuheben, etwa Zuständigkeiten durch elektronische Verknüpfungen zu ändern. Die Technik erleichtert es, Aufgabengebiete neu zu verteilen oder Aufgaben zu übernehmen, die nicht den ursprünglichen gesetzlichen entsprechen. Gefördert wird dies durch Anpassung des Rechts oder des Rechtsganges an die EDV, was im Rückbezug zu einer Strukturveränderung des Rechts führen kann.

Der verfassungsmäßige Datenschutz als Ausdruck des Informationsgleichgewichts der staatlichen Stellen ist in einzelnen Bundesländern förmlich in Gestalt der ADV-Organisationsgesetze geregelt (56).

Nach der Rechtsprechung des BVerfG ist ein Verstoß gegen den Grundsatz der Teilung der Gewalten in Betracht zu ziehen, wo in den Kernbereich einer der Gewalten eingegriffen wird und dadurch das zum Schutze des einzelnen bestehende Kräftegleichgewicht betroffen wird (57). Bei der Regelung des Informationsgleichgewichts geht es vorrangig um die Ausbalancierung zwischen Legislative und Exekutive durch Gewährung eines Auskunfts- oder Zugriffsrechts der Legislative. In die Erwägung, daß bei der Justiz eine verfassungsbedenkliche Datenmenge gespeichert werde, ist man insoweit noch nicht eingetreten. Dies wird verständlich im Hinblick auf den Verfassungsgrundsatz richterlicher Unabhängigkeit (Art. 97 GG).

Bei einem ständigen Informationsverbund Staatsanwaltschaft - Polizei erhalten solche Fragen Auftrieb, weil der Personenkreis, dem die Informationen elektronisch zugänglich werden, sich vergrößert. Von Seiten des Datenschutzes wird als Grundsatz gefordert, daß jede Dauerverbindung der Entscheidung des Gesetzgebers vorbehalten werden müsse (58). Von anderen wird anerkannt, daß on-line-Anschlüsse nicht generell unzulässig sind (59). Das wird aber mit Einschränkungen versehen für Angaben über strafbare Handlungen oder für die Übermittlung aus dem Sicherheitsbereich an andere Stellen. Es geht bei allem um die Eindämmung eines Datenflusses durch sachgerechte Teilung, Steuerung und Kontrolle.

Nun ist es offenbar unzulässig, Sicherheitsbehörden und Justiz gleichzustellen (60), da dies die entscheidende rechtliche Besonderheit verwischt. Die Besonderheit ist die vom Gesetzgeber bewirkte Verkoppelung von Staatsanwaltschaft und Polizei in der repressiven Tätigkeit als funktioneller Justiztätigkeit. Es handelt sich nach den geschilderten Erwägungen des Gesetzgebers um ein Sonderverhältnis innerhalb der Gewaltenteilung, es läßt diese im Kern unberührt und ist vom Verfassungsgesetzgeber so übernommen worden. Der Verfassungsgesetzgeber hat diese gesetzliche Verkoppelung, die mit nichts verglichen werden kann, akzeptiert (61). Der Personenkreis, der für Justizdaten zuständig ist, vergrößert sich bei einem Datenverbund Staatsanwaltschaft - Polizei nicht, sondern der Datenverbund führt die Informationen in die Hände der entscheidungskompetenten Stelle. In diesem Verbund werden also gerade

keine Zweckbindungen unterlaufen. Der Zweckbindung entspricht die Abgrenzung der Justizdaten und in der Rückkoppelung möglicherweise eine deutlichere Abgrenzung der präventivpolizeilichen Daten im Polizeibereich.

Informationsverbund als Forderung

Der Informationsverbund Staatsanwaltschaft - Polizei ermöglicht es, das justizförmige Ermittlungsverfahren real zu verbessern. Der Staatsanwaltschaft und Polizei diese modernen Ermittlungsmethoden vorzuenthalten, wäre andererseits das Gegenteil von verfassungsmäßiger Ordnung. Auf diesen Zusammenhang muß das G 10-Urteil des Bundesverfassungsgerichts (62) aufmerksam machen. Das Gericht hat unter Abwägung aller in Betracht kommenden Interessen des einzelnen wie der Gemeinschaft und der insoweit bestehenden verfassungsrechtlichen Schranken darauf erkannt, daß der Staat mit der Aufgabe von Verfassungsrang auch die Mittel zu stellen habe. Und in mehr als einem Urteil hat das BVerfG auf die unerläßliche Gewährleistung einer effizienten Strafrechtspflege als der Aufgabe des Rechtsstaats hingewiesen (63).

Anmerkungen:

(1) Die technische Seite, die Kommunikation, wird vorausgesetzt (z.B. Postnetz und elektronischer Postpaketdienst).

(2) In den folgenden Jahren, also auch nach Inkrafttreten des BDSG am 01.01.1978 (§ 47 BDSG), drängen sie die Innenverwaltung nachdrücklich, den Anschluß der Staatsanwaltschaften an INPOL, sei es mit eigener Eingabe- und Abrufbefugnis, sei es nur als Abrufbefugnis im Bereich der Personen- und Sachfahndung, herzustellen. So die 49. Konferenz 1978, die 50. Konferenz 1979, die 51. Konferenz 1980 und die 53. Konferenz 1982.

(3) Das zeigen u.a. die Ausführungen unter Nr. 13 und 14 des 2. Berichts des BMI über Dateien im Bereich des BKA vom 19. März 1978. Im Jahre 1981 erläßt das BMI die KpS- und Dateien-Richtlinien, Erlasse vom 26. Februar 1981 - GMBl. 1981, 114 ff., 119 ff. - mit rechtsbedenklichen Regelungsanteilen.

(4) Solche Dateien bleiben gleichwohl in dem konkreten Ermittlungsverfahren ein wichtiges Führungsinstrument in der Hand des Staatsanwalts.

(5) BfD, 4. TB, Drucksache 9/1243 S. 25.

(6) Die Gerichte und Behörden, denen unbeschränkte Auskunft aus dem Zentralregister zusteht (§ 39 Abs. 1 BZRG), können mit der Registerbehörde Auskunftserteilung durch unmittelbare Fernabfrage vereinbaren (§ 10 II BZR VwV i.d.F. vom 19. Dezember 1979, Beilage BAnz. Nr. 20 vom 30. Januar 1980).

(7) Vgl. zu den Punkten, die zur Einführung eines solchen Systems aus tatsächlichen und rechtlichen Gründen drängen, wie etwa der Strafklageverbrauch durch Kommunikationsmängel, Verf., EDV bei der Staatsanwaltschaft, DRiZ 1982, 253 ff.

(8) Gesetzentwurf der Bundesregierung, Bundestagsdrucksache 7/1027, S.14, 18, 22.

(9) Simitis in Simitis/Dammann/Mallmann/Reh, BDSG, 3. Aufl., Einl. Rn 49; Reh, a.a.O., § 3 Rn 5 m.w.N.

(10) Riegel, Datenschutz bei den Sicherheitsbehörden, 1980, S. 2, hält § 45 für die wichtigste Bestimmung der Datenschutzgesetzbebung. In ihrer Bedeutung müssen aber § 1 und § 45 wetteifern.

(11) Simitis, a.a.O., § 45 Rn 8.

(12) Auernhammer, Kommentar zum BDSG, 1977, § 45 Rn 2.

(13) Man kann darüber streiten, ob die Beispielsfälle des § 45 unschwer auf 100 oder auf 1000 erhöht werden könnten, worauf Simitis a.a.O. § 45 Rn 22 hinweist.

(14) Antwort des Staatssekretärs Dr. Fröhlich vom 3. Dezember 1981 auf eine Anfrage des Deutschen Bundestages, Plenarprotokoll 9/70, S. 4102 = DRiZ 1982, 115: "Das geltende Datenschutzrecht behindert die Verfolgung von Straftaten nicht. Die Vorschriften des BDSG gelten gemäß dessen § 45 im Rahmen der Strafverfolgung nur, soweit nicht die Strafprozeßordnung vorrangig ist ...". Die Ansicht, daß § 45 BDSG zu einer Einzelprüfung zwinge, die jeweils wieder die Kongruenzen der kollidierenden Bestimmungen festzustellen habe, so Smitis, a.a.O., § 45 Rn 15, 17 f.m. w.N., findet Rückhalt in der Aufzählung der §§ 52 ff. StPO und des § 161 StPO in getrennten Ziffern des § 45 Satz 2. Eine solche Einzelprüfung bei Anwendung der StPO würde ohnehin praktisch zu denselben Ergebnissen wie die Gesamtübernahme führen. Die Einzelfallprüfung wird dem Sonderstatus der StPO aber nicht gerecht, würde das Ermittlungsverfahren aus dem Zusammenhang reißen und Ermittlungen auf das stärkste behindern. Die Auseinandersetzung entspannt sich indessen weitgehend dadurch, daß in Gestalt von § 161 StPO die Generalklausel für die gesamte Ermittlungstätigkeit der Staatsanwaltschaft vom BDSG ausgenommen ist.

(15) So z.B. Riegel, Datenschutz bei den Sicherheitsbehörden, S. 5.

(16) Schomerus, Datenschutz oder Datenverkehrsordnung? ZRP 1981, 291 ff., II 1.

(17) Vgl. hierzu Kloepfer, Datenschutz als Grundrecht, 1980, S. 23. Die Eingriffstheorie ist eine Ausprägung des Grundsatzes der Verhältnismäßigkeit und ist wie letzterer geeignet, bei Übersteigerung ein Gesetz aus den Angeln zu heben; dazu Schäfer in Löwe/Rosenberg, StPO, 23. Aufl., Einl. Rn 12 Kap. 6.

(18) Zum Persönlichkeitsrecht des Art. 2 I GG als status negativus vgl. Maunz/Dürig/Herzog/Scholz, GG, Art. 2 I Abschn. IV 1; zur Schließung der Wertschutzlücken, dieselben, Art. 2 I 33; zusammenfassend auch Dammann, a.a.O., Rn 31 ff. Ausgangspunkt müssen die in § 1 BDSG genannten schutzwürdigen Belange des Betroffenen bleiben. Der Begriff entspricht und entspringt dem Persönlichkeitsrecht (Wertung der Rechtsprechung mit Nachweisen zum Freiheitsrecht, BVerfG B.v. 3. Juni 1980, JZ 1980, 719, 720).

(19) Dammann, a.a.O., § 10 Rn 31. - Es bedeutet eine der wesentlichsten Gesetzesveränderungen, wenn der BfD die Voraussetzung des Mißbrauchs als Tatbestandsmerkmal und Einstieg des Datenschutzrechts streichen lassen möchte, 4. TB, Drucks. 9/1243, S. 54.

(20) Ordemann/Schomerus, BDSG, 2. Aufl., § 9 Anm. 1.1.

(21) Kloepfer, a.a.O., S. 25; Ordemann/Schomerus, a.a.O., § 3 Anm. 3; Wiese, Grundsatzfragen des Datenschutzrechts, DVBl. 1980, 861, 867, bildet das Beispiel der akzessorischen Natur einer Weitergabe von Mitteilungen aus dem Strafverfahren an das Disziplinargericht zur Berücksichtigung im Disziplinarverfahren nach §§ 14, 17 BDO. Hierin sieht er neben dem Strafverfahren zutreffenderweise keinen datenschutzrechtlich erheblichen weiteren Eingriff.

(22) Die Aufgaben- und Befugniszuweisung ist ein Kind des Verwaltungsrechts, wobei die Betonung auf der Aufgabenzuweisung liegt. Knemeyer, Funktionen der Aufgabenzuweisungsnormen in Abgrenzung zu den Befugnisnormen, DÖV 1978, S. 11 ff. m.w.N., verweist darauf, daß zahlreiche Eingriffsgesetze zwar Eingriffskataloge, aber keine entsprechende Aufgabenstellung enthalten und die Verwaltungsbehörden aus ihren Befugnissen auf ihre Aufgaben zurückschließen und dann wieder ihre Befugnisse anwenden. Es geht also um die Steuerung der Verwaltungstätigkeit durch die Auftragsnorm. Den Rückschluß von der Befugnis auf die Aufgabe findet man auch im Polizeirecht, wo Heise/Riegel, Musterentwurf eines einheitlichen Polizeigesetzes, 2. Aufl. 1978, S. 27, Anm. 2, letzter Absatz, die zumindest mißverständliche Auffassung vertreten, in jedem Falle

habe die Polizei die Aufgaben, die sich aus ihren Befugnissen ergäben. Die Unanwendbarkeit der Idee des Regelverbundes von Aufgaben- und Befugniszuweisung auf das Ermittlungsverfahren folgt aus dem Unterschied zwischen Opportunitätsprinzip und Legalitätsprinzip. die Auftragszuweisung ist typischerweise verknüpft mit bestehender Ermessensfreiheit. Das Legalitätsprinzip schließt die Ermessensfreiheit aus. Die Strafverfolgungsorgane handeln nicht nach Ermessen, sondern sind verpflichtet, einzuschreiten, und ihr Einschreiten ist bereits konkretisiert bezogen auf einen Tatbestand des StGB (§§ 152 Abs. 2, 160, 161, 163 StPO):

(23) Wer wie Riegel, Spezifisches Datenschutzrecht im Bereich der öffentlichen Sicherheit und Ordnung, ÖVD 1981, 16 ff., auf die Wesentlichkeitstheorie verweist - BVerfGE 41, 251, 259 und 47, 46, 78 -, muß ebenso die Schrankentheorie erwähnen, die Individualrechte im Gemeinschaftsinteresse eindämmen kann. Dazu etwa Maunz/Dürig/Herzog/ Scholz, GG Art. 4, Rn 75, 88 f., 111; Art. 5 Abs. 3 Rn 50, 62; Art. 20, Rn 53 mit Art. 19 II Rn. 28.

(24) Vogel, Verfahrensrecht und Terrorismus - eine Bilanz, NJW 1978, 1218, 1225, der sich allgemein mit Eingriffsfragen befaßt, unterliegt im Ausgangspunkt seiner Prüfung einem Versehen, wenn er in der StPO entgegen dem präventiv-polizeilichen Bereich eine Generalklausel vermißt. § 161 StPO: "Zu dem im vorstehenden Paragraphen bezeichneten Zweck (Ermittlungsverfahren) kann die Staatsanwaltschaft Ermittlungen jeder Art ... vornehmen oder ... vornehmen lassen". Seine Folgerungen dürften dadurch beeinträchtigt sein.

(25) Die Entscheidung darüber, ob das Gewicht des Anlasses die Maßnahme erforderlich macht, obliegt dem Staatsanwalt, R. Müller, Karlsruher Kommentar, § 161 Rn 34. Zur Rasterfahndung usw. ablehnend BfD, 3. TB, Drucks. 9/93, S. 50; 4. TB, Drucks. 9/1243, S. 52.

(26) Dammann, a.a.O., § 9 Rn 18; Auernhammer, a.a.O., § 9 Rn. 4.

(27) Dammann, a.a.o., 3. Aufl., § 9 Rn 19.

(28) Der Regelungsgehalt "erforderlich" und der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit entsprechen einander (Antwort der Bundesregierung v. 3. Dezember 1981, BT-Protokoll 9/70, S. 4102 = DRiZ 1982, S. 115).

(29) Die 10 Anforderungen sind Zugangs-, Abgangs-, Speicher-, Benutzer-, Zugriffs-, Übermittlungs-, Eingabe-, Auftrags-, Transport- und Organisationskontrolle.

(30) Gemeint ist, daß der Adressat im Bedarfsfalle nicht mehr einen rechtlichen Prüfungsvorgang des Datenbesitzers auslöst, sondern bereits eine technische und organisatorische Konstellation besteht (Abrufprozedur), kraft deren der Empfänger Zugang zu den Daten hat, vgl. Dammann, a.a.O., § 2 Rn 94.

(31) BfD, 4. TB, BT-Drucks. 9/1243, S. 56; Dammann a.a.O. § 10 Rn 12.

(32) In Preußen war das ursprünglich ausgewogene Verhältnis zwischen Polizeigerichtsbarkeit, Kriminalgerichtsbarkeit und Zivilgerichtsbarkeit verloren gegangen: Die Polizei, aus politischen Gründen verstärkt, hatte sich der verkümmernden Ermittlungsmöglichkeiten der Kriminalgerichte und ihres Ermittlungsapparates bemächtigt. Hatte sie, von der Wohlfahrtspolizei abgegrenzt, als Sicherheitspolizei, ausgerüstet mit der bekannten Generalklausel des § 10 II 17 Pr ALR, die nötigen Anstalten zur Erhaltung der öffentlichen Ruhe, Sicherheit und Ordnung und zur Abwendung der dem Publikum oder einzelnen Mitgliedern desselben bevorstehenden Gefahr zu treffen und stand ihr gemäß § 12 II 17 ALR bei jedem Vorfalle, wodurch die unter der besonderen Obsorge der Polizei stehende öffentliche Ruhe und Sicherheit gestört wurde, das Recht des ersten Angriffs und der vorläufigen Untersuchung zu, so war daraus ein tatsächliches Bestimmungsrecht der Polizei über die Einschaltung selbst der Kriminalgerichtsbarkeit erwachsen. Vgl. Eb. Schmidt, Die Rechtsstellung der Staatsanwälte im Rahmen der rechtsprechenden Gewalt und ihre Einbeziehung in das Richtergesetz, 1957, 4 ff.; Schäfer in Löwe/Rosenberg, 23. Aufl., GVG, § 152 Rn 2; Görgen, Strafverfolgungs- und Sicherheitsauftrag der Polizei, ZRP 1976, 59 ff.; Maunz/Dürig/Herzog/Scholz, GG, Art. 20 VI 59.

(33) Hahn, Die gesamten Materialien zu dem Gerichtsverfassungsgesetz, Berlin 1879, Erste Abteilung, S. 152 ff.

(34) Meyer-Goßner in Löwe/Rosenberg, 23. Aufl., § 163 StPO Rn 9 m.N.

(35) Zur Abgrenzung von Aufgabe, Kompetenz und Zuständigkeit vgl. Wolff/Bachof, Verwaltungsrecht II, 4. Aufl., 1976, § 72 I c.

(36) Von Mangoldt/Klein, Art. 35 V 2 c; Maunz in Maunz/Dürig/Herzog/Scholz, GG, Art. 35 Rn 6, 10; Drews/Wacke/Vogel/Martens, Gefahrenabwehr, Allgemeines Polizeirecht (Ordnungsrecht) des Bundes, 8. Aufl., S. 51, Bd. II.

(37) BverwGE 47,255 = NJW 1975, 893 ff. Wenn Bull, Rechtsprobeleme der polizeilichen Informationssammlung, DVR 1982, Bd. 10, 1, 16, von einer Monopolisierung der Informationsverarbeitung bei der Justiz spricht, ist das offenbar unzutreffend und unverständlich, da er alsbald, a.a.O. S. 21, die Regel der Nr. 5.5 1 Dateienrichtlinien im Hinblick auf die Sachleitungsbefugnis des Staatsanwalts als mögliche Provokation bezeichnet. Den Ansichten von Bull ist Schoreit, Problematische Informationssammlung durch die Polizei, DVR 1982, Heft 19, 39 ff.,entgegengetreten.

(38) Heise/Riegel, Musterentwurf, 2. Aufl., S. 44, § 8 Abs. 2, Anm. 23 Abs. 3.

(39) Riegel, Probleme der polizeilichen Beobachtung und Observation, JZ 1980, 224 Nr. 1: bei abstrakter Gefahr als Fall der sog. Gefahrenvorsorge. Anders Riegel, Datenschutz bei den Sicherheitsbehörden, S. 16 Abs. 2: streng im Rahmen der polizeilichen Generalklausel zur Abwehr einer konkreten Gefahr.

(40) Hessel, Kommentar zum BKAG, 1979, § 2 Anm. 18.

(41) Hessel, a.a.O, § 2 Anm. 5 Abs. 1 und 2.

(42) Stümper, Datenschutz und Sicherheitsprobleme, Kriminalistik 1982, 234 ff.

(43) Vgl. ablehnend Ulrich, Das Verhältnis Staatsanwaltschaft - Polizei, ZRP 1977, S. 158 ff.

(44) Wenn das Bundesverwaltungsgericht, BVerwGE 26, 169, 171 präventive Tätigkeit in der Aufbewahrung von ed-Akten zur künftigen schnelleren Überführung des Straftäters sieht, weil schneller Erfolg weitere Straftaten verhindere, so trägt das nicht dazu bei, die Abgrenzung von Kompetenzen der Präventivpolizei zu klären. Es wird nicht angesetzt, daß mit der Straftat die Prävention gescheitert ist. Die Formulierung "Die Aufbewahrung erkennungsdienstlicher Unterlagen dient hauptsächlich der repressiven Verbrechensbekämpfung. Sie ist keine Maßnahme auf dem Gebiet des Strafprozesses" (a.a.O. S. 170) fördert die Unterscheidung zwischen repressiver und präventiv- polizeilicher Tätigkeit ebenfalls nicht; hierzu Foerster, Allgemeines Verwaltungsrecht für das Land Schleswig-Holstein, LVwG, S. 178, Anm. 2 c.

Eine wohl nicht angemessene Rolle im Bereich der Zuständigkeit spielen die sogenannten Mischbefugnisse. Vgl. etwa bei Heise/Riegel, Musterentwurf, 2. Aufl. 1978, S. 27 Anm. 2; Riegel, Neueste Entwicklungstendenzen im Polizei- und Strafverfahrensrecht, ZRP 1978, 14 ff.; derselbe, Polizeigesetz Nordrhein- Westfalen, 1980, Einl. 9; Bull, Rechtsprobleme der polizeilichen Informationssammlung und -verarbeitung, DVR 1982, Heft 10, S. 1 ff. - Bei einer Razzia oder ed-Behandlung stellt sich die Frage, ob präventive oder repressive Maßnahme oder beide parallel stattfinden. Die Genannten wollen die Maßnahmen verbunden sehen. Es liegen anderweitige Äußerungen vor, die eine Trennung zu erschweren scheinen, z.B. Vogel, a.a.O., NJW 1978, 1225 f.: Überschneidungen und Regelungsbedarf; Meyer-Goßner, LR, a.a.O., § 163 Rn 30: Mögliche Überschneidungen, flüssige Grenzen im Einzelfall; Kleinknecht, StPO, 35. Aufl., § 163 Rn 31: Kombinierte Maßnahmen; R. Müller in Karlsruher Kommentar, § 163, Rn 22, 23: Maßnahmen nebeneinander; OVG Münster, U.v. 13. September 1979, JZ 1979, 806: Verfolgung bereits begangener Straftaten und "auch gleichzeitig ein doppelgleisiges Tätigwerden" zur Gefahrenabwehr und Verhütung von Straftaten. Ablehnend Schoreit, vgl. FN 37.

(45) Zutreffend Drews/Wacke/Vogel/Martens, Gefahrenabwehr, Allgemeines Polizeirecht (Ordnungsrecht) des Bundes, 8. Aufl., Bd. II, S. 43, 45, 47.

(46) OVG Münster, a.a.O., JZ 1979, 806.

(47) Riegel, Datenschutz bei den Sicherheitsbehörden 1980, S. 14 ff.

(48) Vgl. dazu Schoreit, Problematische Informationssammlung durch die Polizei, DVR 1982, Heft 10, S. 46 unter Hinweis auf das Dateienkonzept des BMI; Riegel, Datenschutz bei den Sicherheitsbehörden, 1980, S. 14.

(49) 2.3 KpS-Richtlinien benennt für die polizeiliche Sammlung: Hinweis von Auskunftspersonen, Tatortberichte, Fundberichte, Untersuchungsberichte, Gutachten, Durchsuchungsprotokolle, Beschlagnahmeprotokolle, Zwischen- und Schlußberichte, Aktenvermerke, Ermittlungs- und Auskunftsersuchen, Erledigungsunterlagen, Ausschreibungsunterlagen, Fahndungshinweise und -ergebnisse, Registerauszüge, Straf- und Haftmitteilungen, Verfahrenseinstellungen und Verurteilungen, Freisprüche und ed-Unterlagen und weiteres.

(50) Auch Bull geht davon aus, daß die Polizei - insoweit nicht im Rechtsverkehr - Unterlagen über schon getilgte oder zu tilgende Straftaten auswertet, a.a.O., DVR 1981 Heft 10, S. 30, Fußnote 66.

(51) Schoreit, Datenschutz und Informationsrecht im Bereich der Strafverfolgung unter Berücksichtigung der Dateien des BKA, ZRP 1981, S. 73 ff.

(52) Zu dem komplexen Thema am Beispiel der Spurenakten Meyer-Goßner, Die Behandlung kriminalpolizeilicher Spurenakten in Strafverfahren, NStZ 1982, 353, 354; seine Zweifel, § 163 Abs. 2 StPO auf Daten anzuwenden - im Gegensatz zu der umfassenden Forderung von R. Müller, KK, § 163 Rn 27 - führen zu einer von ihm selbst nicht gewünschten Aufspaltung des Ermittlungsmaterials.

(53) Bull verkennt § 163 Abs. 2 StPO, wenn er meint, die Polizei arbeite erst ab Übergabe der Verhandlungen an die Staatsanwaltschaft im Auftrage derselben, a.a.O., DVR 1982, Heft 10, S. 21 f.

(54) Unabhängig davon muß eine Rechtsform für die Datenherrschaft der Staatsanwaltschaft auch im BDSG gefunden werden. Ein äußerer Anlaß oder Abschnitt könnte nach § 163 Abs. 2 StPO der Zeitpunkt sein, in dem das Verfahren an die Staatsanwaltschaft abgegeben wird. Hiermit könnte in Verfahren, die bei der Polizei begonnen haben, der Charakter als speichernde Stelle (§ 2 Abs. 3 Nr. 1 BDSG) von der Polizei auf die Staatsanwaltschaft übergehen. Die Eigenschaft als speichernde Stelle geht aber bei einer Übermittlung von Daten nicht verloren. - Andererseits biete sich die Rechtsform des § 8 BDSG, die Auftragsverarbeitung, an. In diesem Bereich gilt die Weisung an eine nachgeordnete Behörde, wenn man den Ermittlungsauftrag rechtlich als solchen ansehen will, als Auftrag im Sinne des Gesetzes. Kein Auftrag, sondern eine Übermittlung, liegt jedoch vor, wenn die durchführende Stelle (mit-) zuständig ist, Dammann, a.a.O., § 8 Rn 3, und es besteht Mitzuständigkeit der Polizei für die Ermittlungsaufgabe als funktionellem Organ der Justiz. Denkt man an Datenmitbesitz als Lösung, so entspricht dieser nicht der rechtlichen Kompetenz und Datenherrschaft der Staatsanwaltschaft. Die gemeinschaftliche Datenverarbeitung schließlich ist im BDSG bisher nicht vorgesehen.

(55) Die parallele Prüfung hinsichtlich der zugrunde liegenden Akten führt zu dem gleichen Ergebnis. Prävention durch Anlegung polizeilicher Akten und Speicherung entsprechender Daten kann wirksam werden bei Delikten wie Terrorismus, Banden-, Waffen-, Rauschmittel-, und Falschgeldkriminalität, also in dem engeren Bereich der Schwer- und Bandenkriminalität. Regelmäßig unwirksam sind solche Maßnahmen in dem großen Bereich der kleinen und mittleren Kriminalität.

(56) Z.B. in N-W durch Ges. v. 12. Februar 1974, GVNW, S. 66; vgl. ferner Gola, Die Datenschutzgesetze der Bundesländer - ein Überblick, MDR 1980, 181 ff.; Ruckriegel/v.d. Groeben/Hunsche, Datenschutz und Datenverarbeitung in NW, 1979, Erl. § 1 Anm. 4.

(57) BVerfGE 9, 268, 279; 34, 52, 59.

(58) So etwa Riegel, Spezifisches Datenschutzrecht im Bereich der öffentlichen Sicherheit und Ordnung, ÖVD 1982, S. 16, 18.

(59) Dammann, a.a.O., § 10 Rn 12 b.

(60) So aber Riegel, Probleme der polizeilichen Beobachtung und Observation, JZ 1980 S. 224 f.; ders., Spezfisches Datenschutzrecht, ÖVD 1981, S. 16 f.

(61) Berücksichtigung verdient die Erwägung von Dammann, a.a.O., § 10 Rn 22, daß eine Datenübermittlung im Zweckverbund dort zulässig sein könne, wo eine einheitliche (Verwaltungs-) Aufgabe aus historischen oder besonderen rechtlichen Gründen auf mehrere Behörden oder Stellen verteilt ist, jedoch auf einer einheitlichen Datenbasis erfüllt werden muß, "gleichgerichtete Aufgabe".
Im Ansatz richtig daher auch Riegel, Datenschutz bei ordnungs- und schutzpolizeilichem Handeln, ÖVD 1980, S. 14, der - allerdings für den Einzelfall - bestätigt, daß sich die Übermittlung nicht als eigenständiger Eingriff im rechtlichen Sinne darstellt, wo die gesetzliche Regelung zwar der ersuchenden Behörde des Recht zu einer solchen Maßnahme zugesteht, deren Durchführung aber einer anderen Behörde vorbehält, weil die ersuchende Behörde faktisch hierzu nicht in der Lage ist.

(62) BVerfGE 30, 1, 18.

(63) BVerfGE 33, 367 bis 51, 325.

Informationsverbund Ordnungsbehörden - Polizei

Horst Julich

Ich verkenne nicht, daß das Thema den Verbund mit verschiedenen Zweigen der Ordnungsverwaltung, z.B. dem Meldewesen, umfaßt. Dennoch möchte ich die Thematik meines Referats eingrenzen: nämlich auf die Darstellung der Aufgaben des Kraftfahrt-Bundesamtes und die Nutzung seiner Informationsbestände - besonders über den Systemteil, der unter der Bezeichnung ZEVIS (zentrales Verkehrsinformationssystem) bekanntgeworden ist - für die polizeiliche Arbeit. Es kommt mir weniger darauf an, einen generellen theoretischen Überblick über denkbare Verbundlösungen zu geben; den Schwerpunkt sehe ich darin, einen konkreten, zumindest teilweise realisierten Informationsverbund zu beschreiben. Die Nutzung der Informationsbestände des Kraftfahrt-Bundesamtes für die polizeiliche Arbeit kann zudem gleichzeitig als Modell für einen Informationsverbund innerhalb der Verkehrsverwaltung verstanden werden, weil die zentralen Register Bestandteile eines Informationssystems mit den regionalen Länderbehörden sind.

Die Nutzung der Daten des Kraftfahrt-Bundesamtes für die Polizei macht es indes erforderlich, wenigstens kurz die Aufgaben des Amtes zu skizzieren. Denn bei verschiedenen Anlässen ist mir bewußt geworden, daß vielfach unklar ist, ob der Systemteil ZEVIS der Aufgabenerfüllung des Kraftfahrt-Bundesamtes dient oder der Befriedigung der Informationswünsche der Polizei. Aus diesem Grunde möchte ich klarstellen, daß das Kraftfahrt-Bundesamt fachspezifische Aufgaben der Verkehrsverwaltung zu erfüllen hat. Die Führung des 'zentralen Fahrzeugregisters' und des 'Verkehrszentralregisters' sind nach der historischen Entwicklung, der rechtssystematischen Einbindung und nach der Zielsetzung dieser Register eindeutig dem Verkehrsrecht verhaftet. Der Auskunftsdienst für die Polizei hat zwar einen eigenen Stellenwert gewonnen und stellt besondere Anforderungen an die Datenübermittlung - gleichwohl gründet auch er auf den Funktionen des Amtes als Bundesbehörde für den Straßenverkehr.

Diese Aussage bedarf für das Verkehrszentralregister keiner weiteren Erläuterung. Nach § 30 Abs. 1 StVG werden die registerpflichtigen Daten erfaßt, um für

die Beurteilung der Eignung eines Verkehrsteilnehmers zum Führen eines Fahrzeugs zur Verfügung zu stehen. Darüber hinaus enthielt die - so übel beleumundete - 'Richtlinie zur Behandlung von Mehrfachtätern nach § 15b StVZO' nicht nur das sog. Punktsystem; sie enthielt gleichzeitig die Grundlage für einen 'Informationsverbund' zwischen dem Kraftfahrt-Bundesamt und den regionalen Führerscheinstellen. Denn nichts anderes bedeutete die Verpflichtung des Kraftfahrt-Bundesamtes, die Führerscheinstellen über Verkehrsteilnehmer, die mehrfach eingetragen sind, bei Erreichen eines bestimmten Punktestandes von Amts wegen zu unterrichten. Leider ist die Effizienz dieses Rückkopplungsprozesses später daran gemessen worden, wieviele Fahrerlaubnisse auf diesem Wege entzogen worden sind. Demgegenüber verfolgt die Richtlinie den gegenteiligen Zweck; nämlich durch eine Stufenfolge von Maßnahmen eine Verhaltensänderung zu erreichen und dadurch gerade zu verhindern, daß es zu dem Entzug der Fahrerlaubnis kommt. Erfreulicherweise sind Ansätze erkennbar, die die Bedeutung des Verkehrszentralregisters und der 'Mehrfachtäterrichtlinien' als Instrumente einer konstruktiven Verkehrssicherheitspolitik begreifen: nämlich als Grundlage für die Intensivierung der Nachschulung, eine zielgruppenorientierte Verkehrserziehung und - in Verbindung mit entsprechenden Evaluierungsprogrammen - deren Wirksamkeitskontrolle, gegebenenfalls auch als Motivator bei einer Fahrerlaubnis auf Probe für Anfänger.

Das Informationsbedürfnis der Polizei richtet sich bei dem Verkehrszentralregister in besonderem Maße auf Daten, die die Gültigkeit der Fahrerlaubnis betreffen. Entsprechend dem Inhalt des Registers - es fehlt bekanntlich eine zentrale Erfassung der erteilten Fahrerlaubnisse - müssen sich die Auskünfte auf die 'negativen' Tatbestände beschränken, d.h. auf die Entziehung, die Sperre oder die Versagung einer Fahrerlaubnis (die Daten über die Verhängung eines Fahrverbots stünden zwar auch zur Verfügung, müßten mit Rücksicht auf die kurzen Fristen aber wesentlich schneller aktualisiert werden). Die Polizei benötigt diese Daten zudem zeitnah, um Angaben eines Verkehrsteilnehmers über seine Fahrerlaubnis oder - bei begründetem Verdacht - die Echtheit eines vorgezeigten Führerscheins am Einsatzort (selbst in der Nacht) überprüfen zu können - ich werde darauf eingehen, daß dieses Informationsbedürfnis künftig erfüllt werden kann.

Diese Darstellung möchte ich indes noch einen Augenblick zurückstellen, um die Funktionen des 'zentralen Fahrzeugregisters' ebenfalls kurz zu erläutern, zumal diese Aufgaben weit weniger als die des Verkehrszentralregisters bekannt sind. Das Fahrzeugregister enthält Datenbestände über

- Fahrzeuge mit amtlichen Kennzeichen, geordnet nach Hersteller und Fahrgestellnummer,
- Fahrzeuge mit amtlichen Kennzeichen, geordnet nach Schlüsselnummer der Zulassungsstelle und Kennzeichen,
- Fahrzeuge, die endgültig stillgelegt worden sind, und zwar bis zu fünf Jahren nach der Stillegung,
- Fahrzeuge mit Versicherungskennzeichen,
- technische Fahrzeugbeschreibungen und
- gesuchte Fahrzeuge, Kennzeichen und Fahrzeugbriefe.

Die primäre, verkehrsrechtliche Aufgabe basiert auf der zentralen Erfassung der Fahrzeuge mit amtlichem Kennzeichen, und zwar in der Gliederung nach Hersteller und Fahrgestellnummer, weil diese Daten die bleibenden Merkmale eines Fahrzeugs sind. Die Gliederung nach dem Kennzeichen war ursprünglich eine sekundäre, duplizierte Darstellung des Fahrzeugbestandes und seiner Veränderungen, die statistischen Zwecken diente. Die Fahrgestelldatei - entstanden aus einer manuellen Ablage der Mitteilungen der Zulassungsstellen - bildete (und bildet) die Grundlage der vorrangigen Aufgabe, nämlich der 'Eigentumssicherung'. Es mag mit allem Vorbehalt erlaubt sein, diese Funktion des zentralen Fahrzeugregisters mit der eines Grundbuchs zu vergleichen, freilich mit der Einschränkung, daß nicht der zivilrechtliche Eigentümer, sondern der Halter als Zulassungsträger eingetragen ist. Die zentrale Registrierung des Fahrzeugbestandes entfaltet diese eigentumssichere Funktion in Verbindung mit dem Fahrzeugbrief, weil nur derjenige gegenüber der Zulassungsstelle als berechtigt gilt, der den Brief in Händen hält. Seine Legitimationsfunktion erhält der Brief dadurch, daß eine Vielzahl von flankierenden Maßnahmen sicherstellt, daß zu jedem Fahrzeug jeweils

nur ein Brief existiert. Die Rechtsprechung hat - ergänzend - den Grundsatz entwickelt, daß ein Gutglaubenserwerb an einem Gebrauchtfahrzeug nur dann möglich ist, wenn der Veräußerer den Brief vorweisen kann. Diese zivilrechtliche Reflexwirkung konnte freilich nur begründet werden, weil die zentrale Registrierung der Fahrzeuge nach Fahrgestell- und Briefnummer in hohem Maße gewährleistet, daß der Fahrzeugbrief vor Falsifikaten geschützt bleibt. Der Aufgabenkomplex 'Eigentumssicherung' wird - dies soll besonders hervorgehoben werden - unterstützt durch einen Informationsverbund, der schon seit Anfang der 70'-Jahre besteht: Ich meine die laufende Übermittlung und Aktualisierung der Daten des Sachfahndungsnachweises über gestohlene Fahrzeuge und Kennzeichen, der zwischen dem Bundeskriminalamt und dem Kraftfahrt-Bundesamt stattfindet, und zwar mit dem Ziel, diese Daten ggf. um Hersteller bzw. Typangaben zu komplettieren und mit den laufenden Bestandsveränderungen abzugleichen.

Dieses Informationssystem ist von Anfang an - neben der Eigentumssicherung und der Erfüllung statistischer Belange - auch für den Such- und Auskunftsdienst genutzt worden. Auch diese Aufgabe ist facettenreich - hier sollen freilich die Auskünfte für die polizeiliche Arbeit im Vordergrund stehen. Neu ist diese Aufgabe jedoch nicht. Die Beantwortung polizeilicher Auskunftsersuchen hat es - unabhängig von dem Stand der technologischen Entwicklung - schon immer gegeben; sie gründet auf der Aufgabenstellung der Polizei und wird durch materielle und prozessuale Vorschriften legitimiert und verfassungskonform begrenzt. Damit möchte ich ausdrücklich der Horrorvision, die der Begriff 'Informationsverbund' manchmal auslöst, vorbeugen, zumal die Realisierung des Projektes ZEVIS nach dem derzeitigen Stand für 1984 geplant ist, einem Jahr, das bekanntlich literarisch belastet ist. Es wäre jedoch nach meiner Ansicht unvertretbar, die technologischen Möglichkeiten für einen wirksamen Informationsaustausch ungenutzt zu lassen. Denn die rasante Motorisierung und die damit verbundene Mobilität hat die polizeiliche Arbeit bei der Verkehrsüberwachung und der Verbrechensbekämpfung vor Aufgaben gestellt, die das Informationsbedürfnis und das Anfrage/Antwortenverhalten verändert haben. Diese Infor-

mationsbedürfnisse hatte die Polizei schon frühzeitig formuliert. Die Anforderungen ließen sich jedoch effizient nur durch das Arbeitsmittel 'Datenverarbeitung' lösen, und zwar durch eine realtime-Anwendung. Diese Frage führte im Jahre 1976 auf einer Tagung der Kommission Planung in Malente zur Bildung einer gemeinsamen Arbeitsgruppe, um - ich zitiere aus dem Protokoll - 'unter Umständen in Form eines Pilotprojekts Erfahrungen zu sammeln, indem man die Halterdaten für den Direktzugriff vorbereitet, ferner einen Verbund herstellt zur VZR-Datei und den Fahrerlaubnisdaten'. Die Arbeitsgruppe aus Vertretern der Länder Schleswig-Holstein, Niedersachsen, Berlin und des BKA hat im Herbst 1977 das Arbeitspapier 151 vorgelegt, das die wesentlichen Zielvorgaben für die Realisierung eines Informationsverbundes zwischen der Polizei und dem Kraftfahrt-Bundesamt formulierte.

Das Kraftfahrt-Bundesamt hatte zu diesem Zeitpunkt bereits eine Konzeption entwickelt, die die sequentielle Bearbeitung durch eine Datenbank ergänzen sollte, um das Leistungsangebot zu verbessern und die Maschinenauslastung zu intensivieren. Die eigentliche Innovation liegt deshalb nur in dem Teil des Gesamtkonzeptes, der unter der Bezeichnung ZEVIS bekanntgeworden ist und die technischen Bedingungen für einen Dialogverkehr bietet. Die Realisierung ist zunächst als Pilotanwendung genehmigt worden, weil zu diesem Zeitpunkt (1977/78) noch keine gesicherten Aussagen über die Realisierbarkeit einer Datenbank mit so großen Datenmengen, das Dialogverhalten bei einer Vielzahl von Anwendern und die Kosten der Gesamtrealisierung gemacht werden konnten. Die Pilotanwendung konnte in den Folgejahren mit dem Bundeskriminalamt und dem Landeskrimnalamt Baden-Württemberg realisiert werden und befindet sich seit Anfang 1981 in Betrieb. Den beteiligten Polizeidienststellen möchte ich für ihre Unterstützung an dieser Stelle ausdrücklich meinen Dank aussprechen.

Der Systemteil ZEVIS ist - wie bereits erwähnt - letztlich nur eine Neustrukturierung vorhandener Daten in einer Datenbank mit dem Ziel, u.a. eine zeitnahe Übermittlung zu ermöglichen. Diese Datenbank enthält

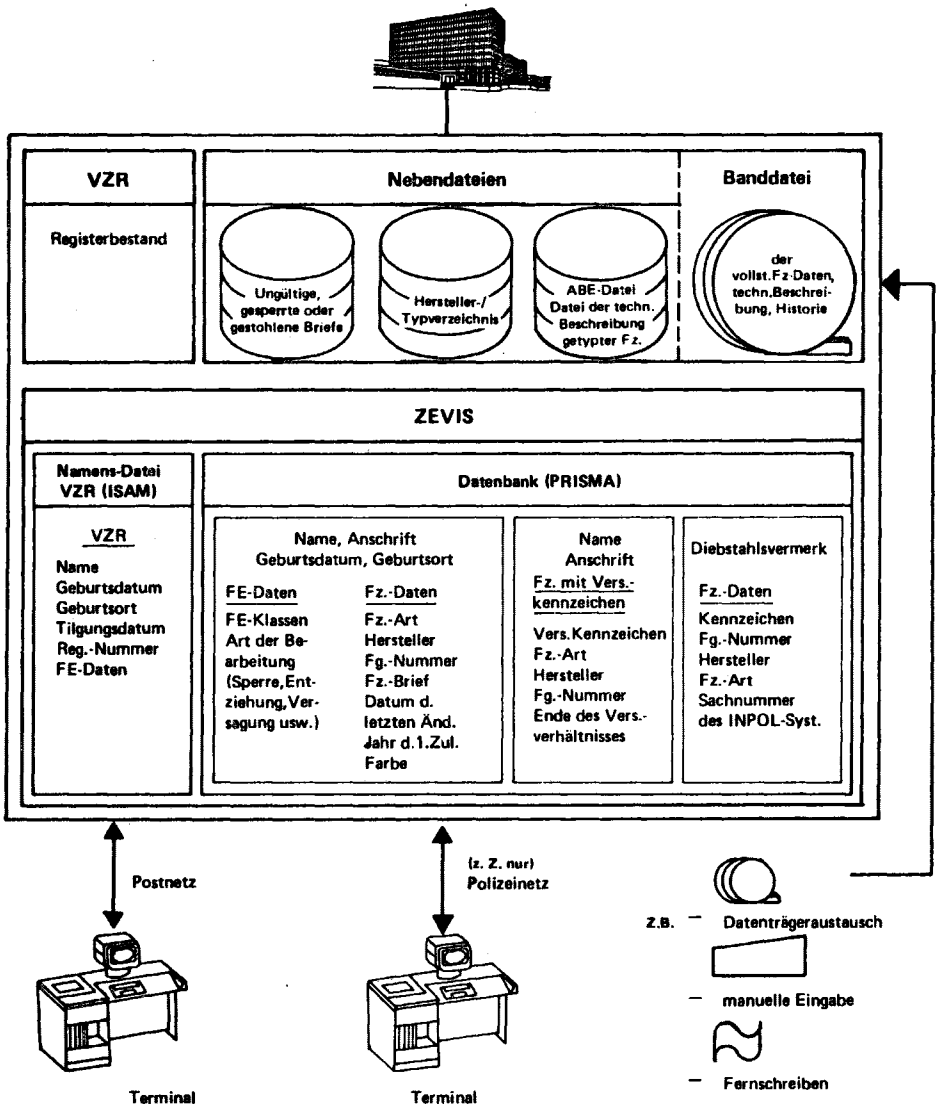
- Daten über Fahrzeuge mit amtlichen Kennzeichen, die für den Auskunftsdienst - und für die interne Sachbearbeitung - relevant sind, einschließlich der Halternamen und der Anschrift,

- die Daten- und Halterangaben der Fahrzeuge mit Versicherungskennzeichen,

- die Daten über gestohlene Fahrzeuge mit der Sachnummer des INPOL-Systems und

- Namen und bestimmte Daten über die Fahrerlaubnis derjenigen Personen, die im Verkehrszentralregister erfaßt sind.

Das Verkehrszentralregister wird im übrigen (s. Abbildung) weiterhin selbständig geführt. Nach der derzeitigen Organisation werden die Personendaten und die Vorgangsnummer (Registeradresse) in einer ISAM-Datei geführt, die bereits heute den externen Dialogverkehr ermöglicht.



Die intendierte Vollautomatisierung, also die Speicherung der Sachdaten, die heute noch in einer manuellen Kartei geführt werden, ist nicht realisiert. Dennoch gehört die ISAM-verwaltete Namensdatei des Verkehrszentralregisters zum Systemteil ZEVIS, wenn auch nur eindimensional, nämlich nach der phonetischen Adresse angefragt werden kann. ZEVIS bezeichnet damit die Datenarchitektur, die den Dialogverkehr technisch zuläßt, unabhängig davon, wie er betrieblich realisiert und freigegeben ist. Es bestünde also bereits heute die Möglichkeit, auch die Namensdatei für die polizeiliche Fernabfrage freizugeben; ein solches Informationsbedürfnis ist jedoch nicht formuliert worden. Die Dialoganfrage wird deshalb vorerst nur von zwei Führerscheinstellen, nämlich Berlin und München, über Postleitungen genutzt.

Die unter PRISMA verwaltete Datenbank ist nach dem derzeitigen Ausbaustand für die Pilotanwendung mit den Fahrzeugdaten der Länder Baden-Württemberg und Schleswig-Holstein und des Kreises München Land, mit etwa zwei Drittel des Gesamtbestandes der Fahrzeuge mit Versicherungskennzeichen, dem vollständigen Bestand der gestohlenen Fahrzeuge und Kennzeichen und dem vollständigen Bestand der Personen geladen, denen die Fahrerlaubnis versagt, gesperrt oder entzogen worden ist (nur dieser Bankbereich umfaßt immerhin ca. 650.000 Sätze). Die Pilotanwendung arbeitet damit etwa mit einem Viertel des für den Endausbau vorgesehenen Datenvolumens, so daß die Erfahrungen und Erkenntnisse, die während der Erprobung gewonnen wurden, auf einer verläßlichen Grundlage beruhen. Der technische Verbund war ursprünglich für einen echten Rechner-Rechner-Verbund geplant. Durch die weitere Entwicklung wurde diese Konzeption überholt; das Kraftfahrt-Bundesamt stellt heute nur eine Terminal-Schnittstelle zur Verfügung, eine Art 'Bankausgabeschalter', der über einen Netzknoten beim Landeskriminalamt Schleswig-Holstein mit dem INPOL-Netz verbunden ist.

Hauptpilotanwender innerhalb des Polizeibereiches sind das Landeskriminalamt Baden-Württemberg und die dort angeschlossenen Datenstationen - zur Zeit 82 Terminals. Weitere berechtigte Terminals stehen beim Bundeskriminalamt, beim Landeskriminalamt Schleswig-Holstein und - als Testzulage - beim Bayerischen Landeskriminalamt.

Entsprechend der Definition der Anfragebedürfnisse der Polizei ist der Zugriff auf die Datenbank über folgende Suchaspekte möglich:

- Geburtsdatum, Geburtsname (phonetische Adresse)
- amtliches Kennzeichen,
- Fahrgestellnummer, Hersteller
- Versicherungskennzeichen.

Der Halterermittlung dient die Anfrageart *H. Bei dieser Anfrage mit dem amtlichen Kennzeichen, der Fahrgestellnummer oder dem Versicherungskennzeichen werden nur die Halterdaten: Name, Vorname, Geburtsname, Geburtsdatum, Geburtsort und Anschrift ausgegeben.

Werden darüber hinaus Daten aus der Fahrzeugbeschreibung benötigt, so kann mit den gleichen Anfragekriterien die Anfrageart *K eingesetzt werden. In diesem Fall erweitert sich die Auskunft um die Fahrzeugart, den Hersteller, den Typ, das amtliche Kennzeichen, die Fahrgestellnummer und die Farbe. Anhand dieser Daten kann im Zweifelsfall eine Identifizierung des Fahrzeugs vorgenommen werden.

Weiter ist die Anfrage mit dem unvollständigen Kennzeichen über die Anfrage *A möglich. Es ist eine Unbekannte im Bereich der Erkennungsbuchstaben oder der Erkennungsnummer möglich. Als Auskunft erscheint eine Liste der in Frage kommenden Fahrzeuge. Dabei werden zu jedem Fahrzeug das amtliche Kennzeichen, der Hersteller, der Typ, die Fahrzeugart, das Jahr der ersten Zulassung und die Farbe genannt. Nach Prüfung dieser Angaben kann der Kreis der Fahrzeuge, zu denen mit Hilfe der Anfragearten *H oder *K der Halter ermittelt werden muß, weiter eingegrenzt werden. Auch bei zwei Unbekannten läßt sich die Anfrage - zerlegt in neue Einzelfragen - wegen des günstigen Antwortzeitverhaltens noch sehr schnell bearbeiten. An einer Erweiterung dieser Anfrageart um zusätzliche Recherchemöglichkeiten wird noch gearbeitet.

Eine weitere Anfrageart ist *F. Es wird in diesem Fall mit den Personendaten 'Geburtsname' und 'Geburtsdatum' in dem Datenbankbereich angefragt, der aus den Unterlagen des VZR gespeist wird und eine Untermenge der ISAM-Datei ist. Die Auskunft enthält - wie schon erwähnt - Angaben über die Gültigkeit der Fahrerlaubnis, wobei Einzelheiten dieser Anfrageart nicht vertieft werden sollen.

Ich möchte nun - wenigstens in Umrissen - skizzieren, welche Erfahrungen der Pilotanwender, die Polizei des Landes Baden-Württemberg, mit dem System ZEVIS gemacht hat. Diese Erfahrungen sind für das Kraftfahrt-Bundesamt deswegen von besonderem Gewicht, weil die Informationsbedürfnisse der Polizei gewissermaßen die Maximalanforderungen darstellen, so daß davon ausgegangen werden kann, daß bei einer Erweiterung der Anfrageberechtigung auf Führerschein- und Zulassungsstellen sowie Bußgeldbehörden keine prinzipiellen Defizite eintreten werden. Das Amt hat deshalb mit Zustimmung des Landeskriminalamtes Baden-Württemberg im Mai 1982 eine Umfrage über die Erfahrungen und die Leistungsfähigkeit des Systems ZEVIS gemacht, deren wichtigste Ergebnisse wie folgt beschrieben werden können:

- etwa 70% aller Anfragen werden im Zusammenhang mit der Verfolgung von Verkehrsstraftaten, z.B. Unfallflucht, und der Verfolgung von Ordnungswidrigkeiten im Straßenverkehr gestellt. Schon dieser Anteil macht deutlich, daß der Informationsverbund Polizei und Kraftfahrt-Bundesamt eine sachliche Berechtigung in der gemeinsamen Aufgabe hat, für die Sicherheit und Ordnung im Straßenverkehr tätig zu werden. Die weiteren Anfragen entfielen auf Ermittlungen bei der Verfolgung allgemeiner Delikte;

- etwa 75% aller Anfragen wurden bisher über die Zulassungsstellen erledigt und nur ca. 20% der Anfragen schriftlich, fernschriftlich oder telefonisch an das Kraftfahrt-Bundesamt gestellt. Trotz des verhältnismäßig hohen Aufwandes, den eine Anfrage bei den Zulassungsstellen bedingt, wurde dieses Verfahren offensichtlich einer Anfrage beim Kraftfahrt-Bundesamt - vor der Einführung der Dialoganfrage - vorgezogen. Die Langwierigkeit regionaler Anfrageverfahren hat nur in ca. 4,3 % die Polizei davon abgehalten, eine Anfrage überhaupt zu stellen. Damit ist die Vermutung

widerlegt, die besonders aus Datenschutzkreisen geäußert wird, daß erst die Direktabfragemöglichkeit ein Anfragebedürfnis weckt - es ist vielmehr eindeutig erkennbar, daß das vorhandene Informationsbedürfnis sich ausschließlich an der technisch optimalen Verfahrensart orientiert;

- die Mehrheit der befragten Stellen hatte eine spürbare oder große Erhöhung der Aufklärungsquote erkannt - das gilt besonders für die Aufklärung bei Unfallflucht und Trunkenheit am Steuer - und schließlich

- haben nahezu alle Dienststellen in der Einführung der Dialoganfragemöglichkeit eine spürbare oder große Entlastung gesehen, weil die bisherigen Anfrageverfahren bei den regionalen Zulassungsstellen teilweise mit eigenen Fahrzeugen, besonders außerhalb der normalen Dienstzeiten, einen erheblichen Mehraufwand verursachten. In diesen Fällen wurde darauf hingewiesen, daß das Personal wie auch die Fahrzeuge nach Einführung einer schnelleren Anfragemöglichkeit für andere wichtige Polizeiaufgaben zur Verfügung stünden.

Bei der Frage nach Erweiterungswünschen wurde ein klares Votum für die Aufnahme weiterer Fahrzeugdaten aus anderen Bundesländern gegeben. Darüber hinaus wurde die Erweiterung der Anfrageart *A für einen Recherche-Arbeitsgang, also mit mehreren Unbekannten, und die Einführung der konzipierten Anfrageart *P für Anfragen mit Personendaten nach den gehaltenen Fahrzeugen genannt. Eine weitere Forderung war die Verbesserung der Aktualität.

Das Kraftfahrt-Bundesamt geht davon aus, daß diese überwiegend positive Resonanz auf die Einführung der Dialoganfrage zwischenzeitlich noch gewachsen ist. Denn zum Zeitpunkt der Evaluierung gab es zwar bereits - wie schon seit Jahren - einen 24-Stunden-Betrieb im Rechenzentrum des Kraftfahrt-Bundesamtes, aber noch keinen Wochenendbetrieb. Ein wesentliches Ergebnis war, daß das Amt ab Mitte d. J. den Rechenbetrieb auch für das Wochenende permanent vorrätig hält, und zwar bedienungsfrei, weil sich herausgestellt hat, daß die Software hinreichend stabil ist. Die Akzeptanz dieser technologisch bedingten Weiterentwicklung des - ich betone es noch einmal ausdrücklich - an sich sehr alten Informationsverbundes der Polizei mit dem Kraftfahrt-Bundesamt erhellt auch die Darstellung des Anfragevolumens seit einem Jahr (s. Tabelle).

Monat/ Jahr	Z E V I S - Anfragen				
	Insgesamt	nach Fahrzeugen mit amtl.Kennz.	nach Fahrzeugen mit Vers.Kennz.	nach FE Daten	nach VZR-Bestands-Daten
09/81	48.381	44.290		716	3.375
10/81	62.458	59.975		987	3.496
11/81	54.711	49.009	84	899	4.719
12/81	49.116	43.944	463	821	4.305
01/82	53.380	46.191	2.617	784	3.788
02/82	68.406	60.508	3.055	1.215	3.628
03/82	88.784	79.655	4.665	1.262	3.200
04/82	77.522	68.987	4.836	1.108	2.591
05/82	76.306	67.838	4.522	1.155	2.791
06/82	82.704	71.116	6.565	1.422	3.601
07/82	81.301	70.771	7.143	1.568	1.814
08/82	90.473	79.220	6.898	2.126	2.229
09/82	103.135	86.688	7.695	2.798	6.954

Die Erprobung für die polizeilichen Auskünfte darf indes nicht darüber hinwegtäuschen, daß ZEVIS für den Dialogverkehr auch mit anderen Anwendern, besonders aus dem Verkehrsbereich, vorgesehen ist. Das gilt für die Führerscheinstellen, die z.B. vor der Ausstellung von Ersatzführerscheinen unmittelbar beim Verkehrszentralregister anfragen können. Der Dialogverkehr ist wirtschaftlich ebenfalls sinnvoll für Zulassungsstellen, um im Einzelfall Unstimmigkeiten durch eine Auskunft aus dem zentralen Fahrzeugregister unterbrechungsfrei zu bearbeiten. Weitere Einsatzbereiche wären die Staatsanwaltschaften und Bußgeldbehörden, die bei dringenden Anlässen ein Informationsbedürfnis ebenso für die Daten des Verkehrszentralregisters wie auch für bestimmte Halterdaten haben können.

Gleichzeitig möchte ich davor warnen, den Dialogverkehr als die einzige Form künftiger Informationsübermittlung zu bewerten. Der Dialogverkehr ist nach meiner Einschätzung eine Form der Arbeitsablaufgestaltung, deren Einsatz - wie bei allen organisatorischen Maßnahmen - den Grundsätzen der Wirtschaftlichkeit und

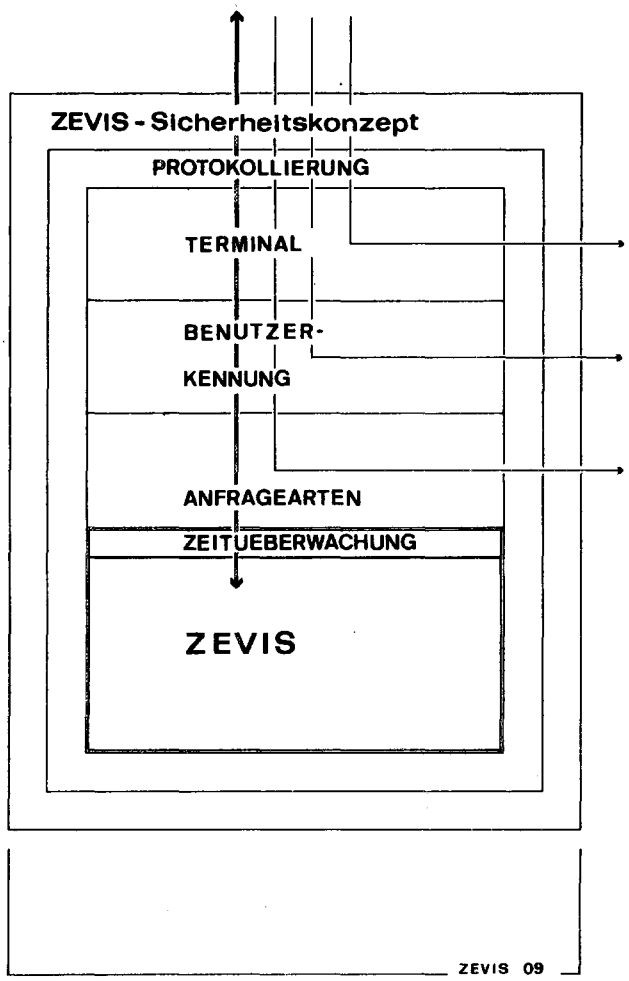
Verhältnismäßigkeit unterworfen ist. Das Konzept der Datenverarbeitung des Kraftfahrt-Bundesamtes geht dementsprechend auch davon aus, daß die derzeitigen Anfrageformen erhalten bleiben - also nicht generell durch den Dialogverkehr ersetzt werden. Das gilt insbesondere für die zahlreichen Kennzeichenanfragen der Bußgeldbehörden, die keiner besonderen Dringlichkeit unterliegen, und für Anfragen der Führerscheinstellen, der Polizei und der Staatsanwaltschaften an das Verkehrszentralregister, bei denen ebenfalls regelmäßig keine besondere Eilbedürftigkeit gegeben sein wird. Das Kraftfahrt-Bundesamt wird daher auch künftig Anfragen bearbeiten, die mit Formularen, fernschriftlich oder über Magnetbänder, gestellt werden. Die 'Hinweise auf Fahndungs- und Ermittlungshilfen durch das Kraftfahrt-Bundesamt' veröffentlicht im BKBl Nr. 4054 vom Januar 1971 und der 'Bundeseinheitliche Anfrage- und Auskunftsdatensatz' - veröffentlicht im VkBl unter dem 10. August 1978 - behalten auch unter Berücksichtigung der technologischen Weiterentwicklung Gültigkeit. Es soll deshalb auch ein Artikel der 'Hessischen Polizeirundschau' vom Oktober d.J. erwähnt werden, der unter der Überschrift 'Verkehrssünderkartei oder mehr?' erfreulicherweise einmal darauf hinweist, daß das Kraftfahrt-Bundesamt nicht nur aus diesem Register besteht und gleichzeitig auf die derzeitigen Anfragemöglichkeiten aufmerksam macht.

Ein Informationsverbund der Polizei mit einer Behörde, die - wie eingehend dargestellt - verkehrsspezifische Aufgaben zu erfüllen hat, wirft naturgemäß auch Rechtsfragen auf. Ausgangspunkt muß sein, daß die Abgabe von Informationen an andere Dienststellen überhaupt zur Aufgabenerfüllung der speichernden Behörde gehört. Dies ist für das Verkehrszentralregister und die Datei der Fahrzeuge mit Versicherungskennzeichen als Teilmenge des zentralen Fahrzeugregisters unstreitig. Dagegen fehlt eine eindeutige Grundlage für Auskünfte aus dem zentralen Fahrzeugregister hinsichtlich der Daten über Fahrzeuge mit amtlichen Kennzeichen.
Dies erscheint eigenartig, weil es doch in der Natur eines zentralen Registers liegt, Auskünfte zu geben. Tatsächlich ist diese Aufgabe auch seit Einrichtung des Fahrzeugregisters erfüllt und als systemimmanent betrachtet worden. Der Beauftragte für den Datenschutz hat indes zu Recht darauf hingewiesen, daß eine normative Ausgestaltung fehlt und seine Bedenken - zumindest für die Auskünfte an Dienststellen - in der Erwartung zurückgestellt, daß eine entsprechende Regelung unverzüglich nachgeholt wird. Entsprechende

Vorlagen sind auch vorbereitet, wobei kein Zweifel an der Aufgabe als solcher besteht - eine gewisse Unklarheit ergibt sich allein für die rechtssystematische Einbindung, d.h. ob durch Novellierung des Gesetzes über das Kraftfahrt-Bundesamt, oder durch ein eigenes Gesetz über die Registrierung von Fahrzeugen, die auch die Zulassungsstellen einbeziehen würde. Die entscheidende Dimension erfährt die Problematik eines Nachrichtenverbundes freilich unter datenschutzrechtlichen Gesichtspunkten, und zwar konkret wegen der Zulässigkeitsvoraussetzungen bei der Übermittlung von Daten im Dialogverkehr, weil das 'Bereithalten zum Abruf' den Verhältnismäßigkeitsgrundsatz tangiert und der abgebenden Stelle die Prüfung der Berechtigung und der Verwendung der Daten für die Aufgabenerfüllung der empfangenden Stelle erschwert, wenn nicht gar unmöglich macht. Den Referaten zu dieser Thematik möchte ich nicht vorgreifen. Ich kann mir indes vorstellen, daß hier eine Abgrenzung nach Risikosphären, wie sie auch für andere Rechtsbereiche entwickelt worden ist, stattfinden kann.Danach trägt die speichernde und abgebende Stelle die Verantwortung dafür, daß die Übermittlung im Dialogverkehr nur an die berechtigten Benutzer erfolgt. Mit dem Empfang der Daten müßte die Verantwortung auf die Dienststelle übergehen, die durch den Antrag auf die Erteilung einer Berechtigung inzidenter auch die Gewähr dafür übernommen hat, daß die über das berechtigte Terminal bezogenen Daten für den gesetzlich übertragenen Aufgabenvollzug verwendet werden. Dies würde bedeuten, daß die Berechtigung 'dienststellen-gebunden' bleibt und die Vergabe der Berechtigung für den einzelnen Sachbearbeiter in der Verantwortung der jeweiligen Dienststelle steht. Ich kann mir auch nicht vorstellen, wie die polizeiliche Arbeit disponiert werden soll, wenn die Berechtigung jeweils personenbezogen gestaltet werden sollte - nicht zuletzt würde dabei eine Datei der Sachbearbeiter bei der abgebenden Dienstbehörde entstehen, ein Ergebnis, das sicherlich nicht dem Datenschutzgedanken entspricht. Auch der Anfragegrund kann nicht Gegenstand der Prüfung und Protokollierung der abgebenden Behörde sein, und zwar umso weniger, als gerade die polizeiliche Arbeit durch Verfahrensvorschriften strengen Regelungen unterworfen ist. Es kann und muß nach meiner Einschätzung - auch unter Berücksichtigung des Verwaltungsaufwandes - davon ausgegangen werden, daß die Verantwortung für die Vergabe der Berechtigung an bestimmte Sachbearbeiter und der Grund einer Anfrage bei der Stelle liegt, die die Daten für ihre

Aufgabenerfüllung anfordert. Die Verantwortung der speichernden und abgebenden Dienststelle sollte sich darauf beschränken, den Dialogverkehr durch die Vergabe der Berechtigung, die Verwaltung der Kennungen und die Protokollierung des Dialogverkehrs zu steuern und zu überwachen.

Nach diesen Gesichtspunkten ist das derzeitige ZEVIS-Sicherheitskonzept aufgebaut (s. Abbildung):



Dieses Konzept läßt eine individuelle Steuerung der Anfrageberechtigung zu. Es ist z.B. daran gedacht, zwischen den einzelnen Polizeidienststellen nach Aufgabengebieten zu unterscheiden. Diese differenzierte Berechtigungskontrolle wird über Kennungen gesteuert. Die Kennung muß für eine Datenstation und für

die entsprechenden Anfragearten berechtigen. Dies ist die erste Schwelle für eine ZEVIS-Anfrage. Des weiteren muß die Datenstation mit ihrer Geräteadresse beim KBA bekannt und generiert sein. Beim Aufbau einer Dialogverbindung bis zu einer ZEVIS-Anfrage sind damit verschiedene Schritte der Identifizierung zu durchlaufen. Alle Aktivitäten, auch wenn eine Anfrage noch gar nicht zustandegekommen ist, werden im ZEVIS-Sicherheitskonzept protokolliert; dazu gehören auch die Fehlversuche mit Anfragen von unberechtigten Terminals, mit ungültigen Benutzerkennungen oder mit Anfragearten, für die keine Zulassung besteht. Schließlich werden selbstverständlich bei der Protokollierung die Anfrage mit den Anfrageinformationen und die gegebenen Auskünfte festgehalten. Ich bin davon überzeugt, daß dieses Sicherheitskonzept den Anforderungen des Datenschutzes genügt und gleichzeitig in einem vernünftigen Verhältnis zum Verwaltungsaufwand steht.

Ein kurzer Blick sei noch auf die Perspektiven für den weiteren Ausbau des Systemteils ZEVIS gestattet, wobei die Nutzung für die polizeiliche Arbeit in der Disposition der einzelnen Länder liegt - das Kraftfahrt-Bundesamt kann lediglich die technologischen Bedingungen für den Nachrichtentransfer im Dialogverkehr anbieten:

- ein wesentliches Ergebnis der ersten Rückkopplung mit den Pilotanwendern hatte ich bereits erwähnt: das Kraftfahrt-Bundesamt hat seit Mitte d. J. den bedienungsfreien Betrieb am Wochenende eingeführt und damit die ununterbrochende Verfügbarkeit der Datenbank geschaffen;

- es ist weiterhin vorgesehen, den Fahrzeugbestand des Landes Bayern bis Ende d. J. in die Datenbank zu übernehmen, so daß auch weitergehende überregionale Anfragen sinnvoll werden und das Dialogverhalten unter stärkerer Belastung getestet werden kann. Ergänzend werden - als Ergebnis einer separaten Arbeitsablaufverbesserung - die Fahrzeuge mit Versicherungskennzeichen ab März 1983 in der Datenbank geführt;

- daneben wird die Software komplettiert, um die Anfrageart *P, d.h. die Anfrage nach Fahrzeugen mit den Suchkriterien 'Name' und 'Geburtsdatum', zur Verfügung stellen zu können, falls weiterhin ein entsprechendes Informationsbedürfnis besteht und keine Einwände des Datenschutzes zu Restriktionen führen. Denn diese Anfragen, zumeist mit hoher Dringlichkeit gestellt, belasten derzeit den Rechenbetrieb des Amtes erheblich;

- der Ausbau der Pilotrealisierung wird damit abgeschlossen sein. Die Gesamtrealisierung ist für 1984/85 vorgesehen, falls die erforderlichen Genehmigungen erteilt werden.

- ein wesentlicher Aspekt ist in diesem Zusammenhang die Aktualität der Fahrzeugdaten. Das Amt untersucht gegenwärtig bereits die Möglichkeiten, durch Veränderungen der internen Sachbearbeitung eine Beschleunigung zu erzielen. Die entscheidende Verbesserung wird von der weitergehenden Automatisierung der Zulassungsstellen - gegenwärtig werden ca. 20% der Fahrzeugdaten auf Datenmeldesätzen übermittelt - erwartet, die eine zeitnahe Verarbeitung der Bestandsveränderungen bewirken wird. Dieses Anliegen hat erst kürzlich der Bundesrechnungshof aufgegriffen;

- schließlich möchte ich noch einmal darauf zurückkommen, daß der Dialogverkehr nach wie vor nur eine Form des Auskunftsdienstes bleibt, und zwar für Vorgänge mit hoher Dringlichkeit. Die derzeitigen Übermittlungsarten bleiben erhalten und werden bei Massenanfragen auch künftig wirtschaftlicher sein. Die Sachbearbeiter des Kraftfahrt-Bundesamtes stehen im übrigen auch weiterhin bei Anfragen zur Verfügung, die einen besonderen Suchauftrag mit ergänzenden technischen Daten erfordern, weil z.B. die Aussagen über den Hersteller und Typ eines Fahrzeugs ungenau sind. Ich möchte damit den Hinweis verbinden, daß die Datenverarbeitung ein Arbeitsmittel bleibt, dessen Effizienz letztlich von der Akzeptanz der Sachbearbeiter getragen wird. Es sollte im Bewußtsein bleiben, daß ein Informationsverbund nicht nur aus Rechnern, Systemen und Terminals besteht - er bedeutet auch Kommunikation und Kooperation zwischen Menschen, die für die gleichen Aufgaben arbeiten.

Die Datenverarbeitung der Polizei und die öffentliche Meinung

Dagobert Lindlau

Ich bin dankbar für diese Einladung. Nicht nur, weil sie mir Gelegenheit gibt, Ihnen ein paar begründete Vermutungen anzubieten, sondern weil sie zeigt, daß es bei der Polizei noch Leute gibt, die Meinungen von außen ertragen können. Klinisch gesprochen läßt das Rückschlüsse auf einen begrenzten Leidensdruck zu und Hoffnung auf eine günstige Prognose.

Einem Außenseiter werden Sie von vornherein einen Mangel an detaillierter Fachkenntnis zugestehen müssen. Ich werde mich meinerseits bemühen, diesen Mangel durch Abstand auszugleichen und vor allem durch die Unabhängigkeit von einem Apparat, dem die meisten von Ihnen angehören. Nur in dieser einen Beziehung ist die Polizei ein ganz ähnliches Gebilde wie die Mafia, man erkennt die Dimension nur von außen und aus einer gewissen Entfernung. Dem Iniziierten bleibt sie verborgen.

Die Frage, was denn die Öffentlichkeit von der polizeilichen Datenverarbeitung hält, ist eine echte Pilatus-Frage. Das heißt nicht nur, daß sie schwer zu beantworten ist. Bekanntlich hat der Law-and-Order-Polizist Pontius Pilatus die Wahrheit und nichts als die Wahrheit wissen wollen. Und beim Versuch, sie zu erfahren, ist er dem folgenreichsten Irrtum der christlichen Geschichte verfallen. Sie selbst wissen am besten, daß Ihre Computer auch keine Wahrheiten anzubieten haben. Bestenfalls ein paar richtige Informationen.

Was sagt die öffentliche Meinung dazu? Sie schweigt, wenn auch geräuschvoll und affektgeladen. Sie flutscht einem durch die Finger, wenn man sie am Schwanz packen will. Sie ist ein Gespenst, von dem alle reden, das aber keiner gesehen hat. Sie ist ein Chamäleon und wechselt die Farben, je nachdem was sie zu fressen bekommt: Von Ihnen, von Politikern und von uns Journalisten.

Wir Journalisten gehen täglich mit diesem manchmal gutartigen, manchmal bösartigen, in jedem Fall aber unberechenbaren Tier um. Wir versuchen es zu ergründen, zu domestizieren und - auch das gebe ich zu - gelegentlich einmal aufzuhetzen.

Daß wir, die Journalisten, öffentliche Meinung nicht nur spiegeln, sondern vor allem machen, das behaupten eigentlich nur Politiker, die der eigenen Paranoia zum Opfer fallen. Glücklicherweise sind sogar von denen die meisten zu klug, um den Unsinn zu glauben, den sie da verzapfen. Zu genau wissen sie, daß an der öffentlichen Meinung Tausende von Faktoren mitwirken, die wir alle miteinander nicht einmal ahnen, geschweige denn exakt beim Namen nennen können. Politiker erteilen uns diesbezügliche Rügen vor allem deshalb, weil sie sich schrecklich darüber ärgern müssen, daß man die Manipulation der öffentlichen Meinung nicht ganz allein und ungestört ihnen überläßt. Wo sie doch ein Mandat haben, auf das sie sich bis zum Überdruß berufen. Wahrscheinlich haben sie wirklich ein Mandat, um zum Beispiel eine bessere Politik zu machen, als sie es tatsächlich in der Regel tun. Sie haben aber definitiv kein Mandat, Fernsehanstalten zu managen, Kliniken zu besetzen oder in polizeiliches Vorgehen hineinzureden. Zum Glück gibt es in dieser Gesellschaft noch ein paar wichtige Angelegenheiten, die nicht durch Partei, politisches Mandat, sondern durch Sachkunde, durch Kompetenz erledigt werden.

Ich habe einen Grund für diesen Seitenhieb. Das Bundeskriminalamt ist eine Spielwiese für Politiker aller Couleur, die eines gemeinsam haben, nämlich noch weniger Sachkenntnis als wir Journalisten. Und die Datenverarbeitung ist nun einmal hier von Horst Herold zu einer respektablen Größe ausgebaut worden. Anreiz für parteipolitische Schaukämpfe. Wie soll man mit einer großen Öffentlichkeit über die polizeiliche Datenverarbeitung sachlich reden, wenn die parteiideologische Polarisierung eines jeden Problems dies unmöglich macht. Solange in diesem Land die Frage danach, ob ein bestimmtes Atomkraftwerk sicher oder unsicher ist, allein dadurch beantwortet wird, ob der Antworter der linken SPD angehört oder der rechten CSU, solange dies nicht eine Frage der technisch-physikalischen Prüfung ist, solange müssen wir uns damit abfinden, daß Sachfragen nicht mehr diskutabel, wahrscheinlich nicht einmal mehr lösbar sind.

Auch die sogenannte öffentliche Meinung über die polizeiliche Datenverarbeitung wird zunächst und vor allem durch das ideologische Vorurteil des einzelnen Betrachters bestimmt. Auf der einen Seite gibt es Leute, die der Polizei alles und jedes zugestehen wollen, gleich welchen Preis die Gesellschaft zu zahlen hätte. Auf der anderen Seite gibt es Leute, die meinen, daß die Polizei überhaupt nichts darf, egal welche Konsequenzen das für die Innere Sicherheit hat. Beide Seiten sind ideologisch geblendet. Ich glaube, wir können uns hier darauf einigen, daß blinde Irrationalisten am Stammtisch unterhaltsam sein mögen, in einer solchen Debatte aber nichts verloren haben.

Wozu - so habe ich mich gefragt - wollen Sie denn eigentlich die öffentliche Meinung über die polizeiliche Datenverarbeitung kennenlernen. Wollen Sie etwa danach handeln? Muß da irgend jemand gewählt werden? Brauchen Sie ein Mandat von der breiten Masse?

Die ernsten Fragen, die Sie hier behandeln werden, können nicht plebiszitär entschieden werden. Sicher: Die öffentliche Meinung ist ein legitimer, ein dringend notwendiger und ein heilsamer Druck auf uns alle, sich zu erklären, die eigene Verantwortung und Kompetenz allgemein verständlich zu machen. Als Fachleute dürfen weder Sie als Polizisten noch wir als Journalisten bloß dem Volk auf das Maul schielen und dann glauben, wir hätten getan, wofür wir bezahlt werden.

Wenn ich es richtig durchschaue, dann versteckt sich hinter der Frage, die Sie mir stellen, in Wahrheit eine ganz andere. Die Frage nämlich: Wieviel Vertrauen genießt denn die Polizei in der Öffentlichkeit? Das ist sehr schlau und es entspricht der polizeilichen Tradition, nach etwas ganz anderem zu fragen, als man eigentlich wissen will. Dabei geht es natürlich nicht um den netten Schupo an der Ecke, den Bullen, der Häuser räumen muß, den freundlichen Beamten, den wir zu Hilfe rufen. Es geht um Ermittlungsvorgänge, die der Laie nicht kennt und die man ihm aus Gründen der eigenen Trägheit oder aus kriminaltaktischen Gründen auch nicht im einzelnen erklären will.

Alle unbekannten Vorgänge, die den Bürger sehr persönlich betreffen, lösen bei ihm großes Unbehagen aus. Das gilt nicht nur für die polizeiliche Datierung. Das gilt zum Beispiel auch in der Chirurgie. Da geschieht mit dem Patienten auch etwas, das ihm durch Narkose verborgen bleibt. Untersuchungen bestätigen, daß die irrationale Angst vor dem operativen Eignriff vor allem darauf zurückzuführen ist.

Alles, was uns angeht und was wir nicht genau durchschauen, ist bedrohlich. Erlauben Sie mir ein Beispiel aus einem ganz anderen Bereich Ihrer Ermittlungsarbeit. Selbst für aufgeklärte Bürger ist die Möglichkeit der Telefonüberwachung ein ständiger Alptraum. Da hocken gesichtslose Beamte herum, die Orwell erfunden haben muß, und lauschen mit perverser Gier, um ihren akustischen Voyeurismus an intimen Dialogen zu befriedigen. Wer einmal - wie ich - diesen eher langweiligen Prozeß miterlebt hat, wer weiß, daß da ein Haufen angeödeter Beamter eine geradezu artistische Technik des Weghörens entwickelt hat, die nur dann unterbrochen wird, wenn endlich die eine spezielle Information im Kopfhörer ist, auf die man seit Tagen oder Wochen wartet, - wer weiß, mit welcher Dickfelligkeit solche Beamte Intimkonversation ignorieren und sich sogar bei kriminologisch relevanten Details, die nicht zum Abhörauftrag gehören, taub stellen, weil die Registrierung nur zusätzliche Arbeit machen würde, - wer das alles weiß, für den hat eine solche Veranstaltung nichts sonderlich Bedrohliches mehr.

Der psychologische Mechanismus bei der polizeilichen Datenverarbeitung ist derselbe. Die sammeln Wissen über mich. Und ich kenne die nicht einmal, die da so viel über mich wissen. Ich habe nicht die geringste Ahnung, was die mit ihrem Wissen machen. Man fühlt sich nackt und ausgeliefert. Das Maskenverhalten, das zumindest eine Voraussetzung jedes höflichen, nachsichtigen, mit einem Wort kultivierten Umgangs miteinander ist, wird vernichtet. Wie soll man fröhlich sein, wenn irgendwo ein Computer steht, der Dinge über einen weiß, die man selber am liebsten vergessen möchte. Welche Anmaßung: denn alles zu wissen, steht doch eigentlich nur einem zu und der ist gnädig, der verzeiht - und vor allem - der verrechnet sich nicht unentwegt. Und er läßt sich weder falsch programmieren, noch mißbrauchen.

Vergessen Sie nicht: Überall da, wo wir Normalbürger mit dem Computer zu tun haben, müssen wir feststellen, daß sein wesentliches Kennzeichen die Panne ist. Wir merken es an der Telefonrechnung und an den Fehlbuchungen der Lufthansa. Vor ein paar Tagen war große Aufregung bei der Süddeutschen Zeitung. Die Ausgabe von Morgen steckte im Computer und der zeigte keinerlei Lust, sie für den Druck herauszugeben. Wenn es nach

meiner letzten Computerdiagnose ginge, dann wäre ich trotz meines zarten Alters von 22 Jahren - für so alt hält mich der elektronische Trottel nämlich - entweder seit Jahren tot, halbverhungert und zu allem Überfluß auch noch impotent. Ausgerechnet beim Bundeskriminalamt soll dann ein solches Ding funktionieren.

Das alles erklärt noch nicht die ganze Angst vor einer Datei, die ebenso unmenschlich wie pannenanfällig ist. Wir erschrecken auch, weil der polizeilichen Datenbank eine der humansten Eigenschaften fehlt, nämlich die Fähigkeit, ganz einfach etwas zu vergessen. Hier wächst kein Gras über Dinge. Von Nietzsche stammt - nicht ganz wörtlich - das folgende Zitat: "Deine Erinnerung sagt dir, dies hast Du getan. Dein Stolz sagt Dir, dies kannst Du nicht getan haben. Dein Stolz wird über die Erinnerung siegen." Der polizeilichen Datenverarbeitung fehlt die theologische Tröstung der Absolution.

Ich beschreibe hier nur ein Gefühl vieler Bürger und prüfe nicht nach, ob sie technisch recht haben. Das ist nämlich unerheblich. Öffentliche Meinung wird nun einmal mehr von Gefühlen bestimmt als von Tatsachen. Daß dies bisher nur von der Waschmittelreklame erkannt wurde und nicht von der Informationspolitik der Polizei, macht die Sache nicht besser.

Aber selbst wenn die Polizei in Bezug auf ihre Informationspolitik über den eigenen Schatten springen könnte - und es ist ein langer Schatten, der bis ins neunzehnte Jahrhundert reicht - dann könnten dadurch allein verfestigte Vorurteile noch nicht vernichtet werden.

Wir Fernsehjournalisten wissen, daß die selektive Wahrnehmung der meisten Zuschauer dazu führt, daß sie aus jeder Sendung nur das heraushören oder -sehen, was ihrem bereits vorhandenen Vorurteil entspricht. Wenn die Sendung ihrer vorgefaßten Meinung entspricht, fühlen sie sich bestätigt, wenn sie ihrer Meinung widerspricht, fühlen sie sich in ihrem Vorurteil bestätigt, daß Fernsehleute Ignoranten und Manipulateure sind. Bestätigt fühlen sie sich in jedem Fall. Die Trennung von einem Vorurteil ist ein schmerzlicher Vorgang, den man vermeidet, solange es geht.

Was die Reaktion der Öffentlichkeit angeht, hatte ich eine paradigmatische Erfahrung im Zusammenhang mit der Rasterfahndung. Meine Nase sagte mir, daß sich im Zusammenhang mit dieser elektronischen Ermittlungstechnik ein Gewitter in den Medien zusammenbrauen würde. Deshalb sagte ich frühzeitig in einem ARD-Kommentar etwa folgendes:

Die Polizei habe seit eh und je Merkmale von Tat und Tätern gesammelt und sich dann gefragt, auf wen die Merkmale passen könnten. Früher unter anderem durch Herumfragen beim Arbeitgeber oder bei den Nachbarn. Heute mit Hilfe einer Datei. Also nichts Neues. Kein Grund zur Aufregung. - Mit Recht hielten die Bürger den Schutz ihrer privaten Sphäre für ein hohes Rechtsgut in einer freien Gesellschaft. Die Rasterfahndung verletze dieses Gut nicht. Die Polizei habe mit einem hochorganisierten Verbrechen fertig zu werden, das systematisch die rechtsstaatlichen Skrupel dieser Gesellschaft ausnütze. Verzicht auf Polizeiliche Datenverarbeitung räume der politischen und kriminellen Unterwelt einen Einfluß in diesem Staat ein, der den Rechtsstaat zu einer leeren Prätention mache.

Der Kommentar lief darauf hinaus, daß es mir persönlich wesentlich lieber wäre, in ein elektronisches Raster zu geraten, als Männer mit Ledermänteln und konspirativ verzogenen Mundwinkeln bei meinem Nachbarn herumfragen zu sehen. Letzteres wäre auch nach dem Beweis meiner Unschuld nie mehr zu reparieren. Die elektronische Rasterfahndung entließe mich aber sang- und klanglos wieder in die Anonymität.

Und nun die symptomatische Reaktion:
Ein Kollege, der sonst nicht leichtfertig mit dem Wort ist, fragte am nächsten Tag in der Redaktionssitzung, wieviel mir wohl das BKA für diesen Kommentar bezahlt hätte. Das verriet nicht nur eine bedauerliche Unkenntnis des Vorgangs und meiner Person, vor allem aber eine traurige Ignoranz, was den pekuniären Habitus des BKA angeht.

Die Reaktionen der Zuschauer waren exakt zweigeteilt. Und das kommt sehr selten vor. Die einen beschimpften mich als Nazi. Die anderen gratulierten mir und hießen mich im extrem rechten Lager willkommen. Auf die Idee, daß ich durch meine wie auch immer begrenzte Einsicht in die Problematik zu einem Urteil gekommen sein könnte, war bei keinem Zuschauer spürbar. Nicht bei einem einzigen.

Dieselben psychologischen Mechanismen, die in der öffentlichen Meinung zur polizeilichen Datei sichtbar werden, gibt es natürlich auch in anderen Bereichen. Bei der Bekämfpung des Organisierten Verbrechens kommt es zu einem atemberaubenden Rollentausch. Ausgerechnet Leute, die sonst einer dezidierten Kapitalismus-Kritik zuneigen, wehren sich mit Händen und Füßen gegen eine Verschärfung des polizeilichen Instrumentariums, mit dem allein das Organisierte Verbrechen effektiv bekämpft werden könnte. Sie erkennen das Organisierte Verbrechen nicht als Sumpfblüte einer brutalen Wettbewerbsgesellschaft, weil ihre überwertige ideologische Antipathie der Polizei gilt. Dabei ahnen sie nicht einmal, daß sie sich auf diese Weise zum Handlanger einer gerade von ihnen immer wieder diffamierten Klassenjustiz machen, die den kleinen Gauner fängt und den großen mangels Werkzeug laufen lassen muß.

An der Fehleinschätzung polizeilicher Datenverarbeitung mögen Vorurteile und Unkenntnis beteiligt sein. An der weitverbreiteten Enttäuschung ist die polizeiliche Informationspolitik ganz allein schuld. Es ist ja wirklich nicht klar, ob die polizeilichen Dateien nicht ebensoviele Fragen aufwerfen wie sie Aufgaben erledigen. Wir erinnern uns noch sehr gut, mit welchem Überschwang "Kommissar Computer" in der Presse begrüßt wurde. Das war Ihr Überschwang. Nicht der unsere. Die Enttäuschung mußte bitter werden. Das Verbrechen ist zu unser aller Staunen nicht ausgerottet. Es gibt sogar mehr davon, seit es polizeiliche Dateien gibt. Wir sind quasi für nichts und wieder nichts zu Nummern geworden. Aber trösten Sie sich: Auf allen Gebieten gibt es Schwankungen zwischen jauchzender Hoffnung und herber Enttäuschung.

In der Medizin waren Quecksilber und Antimon ein Jahrhundert lang Wunderheilmittel, die alles konnten. Wahrscheinlich sind durch die Verordnung dieser Metalle mehr Leute umgebracht worden als durch die Syphilis. Heute sind die beiden Elemente ein nicht sonderlich wichtiges Remedium unter Millionen anderen. Die Akupunktur erlebt regelmäßig alle 150 Jahre eine Blüte und wird dann wieder vergessen.

Man muß auch zur Polizeilichen Datenverarbeitung ein normales Verhältnis finden. Sie kann eine ganze Menge und eine ganze Menge kann sie nicht. Und wieder eine Menge sollte sie gar nicht können.

Gelassenheit ist geboten. Sie alle wissen doch viel besser als ich, was in den USA geschah, als sich zum ersten Mal ein Mann anbot, wissenschaftlich nachzuweisen, daß eine bestimmte Kugel aus einem bestimmten Lauf gekommen sein muß. Die Justiz heulte auf. Das kontradiktorische System der freien Rechtspflege war in Gefahr. Die Unabhängigkeit eines Richters sollte ersetzt werden durch das Gutachten von irgendeinem Niemand. Der Manipulation vor Gericht wäre durch solche Methoden fortan Tür und Tor geöffnet.

Beim ersten Nachweis von Blutgruppenübereinstimmung war der Protest wenn möglich noch lauter. Was, wenn nicht dies, war ein Eindringen des Staates ins Allerpersönlichste, eine Praxis, die allen Prinzipien einer liberalen Gesellschaft ins Gesicht schlug. Bekannte Argumente.

Wenn Sie von mir erwartet haben, wie man an der öffentlichen Meinung über die polizeiliche Datenverarbeitung etwas ändern kann, ohne die eigene Einstellung gegenüber der öffentlichen Meinung zu ändern, dann muß ich Sie enttäuschen. Der wesentliche Bestandteil eines solchen Rezepts wäre nämlich die institutionalisierte Lüge. Davon haben wir aber schon bis an die Grenze des Erträglichen genug, bei den Parteien, bei den Interessengruppen und last not least auch bei der Polizei.

Die Arbeit der Polizei verlangt sparsamen Umgang mit Informationen, um dem kriminellen Gegner keine Vorteile zu bieten und um die im weitesten Sinne Betroffenen in ihrer privaten Sphäre zu schützen. Vielleicht sogar, um keine Nachahmung zu provozieren. Alles honorige und stichhaltige Gründe. Nach dreißig Jahren Berufserfahrung bin ich aber davon überzeugt, daß mehr als die Hälfte aller Informationen von der Polizei nur deshalb zurückgehalten werden, weil die Öffentlichkeit daran gehindert werden muß, ihre Arbeit kritisch zu beurteilen. Ständige Vorteilnahme durch Geheimhaltung können sich außer der Polizei in dieser Gesellschaft nur noch Ärzte und Anwälte verschaffen.

Solange man als Journalist auf Pressekonferenzen der Polizei eigentlich nur noch geht, um zu erfahren, wie es ganz sicher nicht gewesen ist, - solange die Polizei ihre Fehler, ihre Schlamperei und sogar niedrige Beweggründe einzelner hinter einer fadenscheinigen Geheim-

haltung verbirgt, solange einige Polizisten ihr defektes Selbstwertgefühl nur dadurch reparieren können, daß sie sich als Geheimnisträger aufspielen, - so lange darf man den meisten Journalisten mit der Bitte um Aufklärungshilfe nicht kommen.

Vergessen Sie bitte nicht, daß es einen Berufsstand gibt, der noch mehr angelogen wird als die Polizei, - und das sind wir Journalisten. Wenn schon einige von Ihnen die öffentliche Meinung als Nutte betrachten und uns Journalisten als ihre Zuhälter, dann sollten Sie Ihre taktische Einsicht wenigstens dazu zwingen, mit uns eine praktikable Kooperationsbasis zu finden. Mit Kriminellen schaffen Sie das ja auch. So hört man jedenfalls.

Woran liegt denn die Berührungsangst, die selbst Leute wie ich - nicht im Bundeskriminalamt, aber sehr oft sonst - mit der Polizei haben. Das Chor der Polizisten hat ganz unbewußt den Chorgeist seiner kriminellen Gegenspieler übernommen. Man ist ein Freund der Polizei als Journalist nur dann, wenn man jede noch so verheerende Panne als Erfolg feiert und auch die dümmsten Erklärungen ohne Nachfrage schluckt. Hält man journalistische Distanz, läßt man sich nicht durch Informationsentzug erpressen, dann ist man ein Feind der Polizei und wird verfolgt bis ins siebte Glied. Polizeipräsidenten und Päpsten muß man glauben, alles andere ist Häresie. Legen Sie doch bitte endlich diese peinliche Wehleidigkeit gegenüber Kritik ab.

Wir Journalisten andererseits müssen begreifen, daß nicht jeder Mißerfolg der Polizei ein Grund ist, den Notstand auszurufen. Als Patty Hearst in den Vereinigten Staaten 591 Tage lang nicht gefaßt werden konnte, hat das nichts über die Kompetenz oder Inkompetenz des FBI ausgesagt. Es hat aber eine ganze Menge über die Freiheit in diesem Land verdeutlicht. Zumindest ein Kennzeichen einer freien Gesellschaft ist nun einmal, daß der Bürger die meiste Zeit unbeobachtet bleibt. Machen Sie endlich klar, daß auch die elektronische Datenverarbeitung der Polizei daran nichts ändert und nichts ändern will.

Polizei und Datenschutz

Herbert Tolksdorf

"Polizei und Datenschutz" ist ein Thema, das zwischen den Extremen "Datenschutz ist Tatenschutz" - so eine Berufsvertretung der Polizei - und "Datenschutz ist Grundrechtsverwirklichung" - so Datenschutzkontrollinstanzen - immer wieder engagiert, kontrovers, ja unsachlich bis zu gegenseitigen Verunglimpfungen diskutiert wird. Dabei liegen das Schwergewicht und die Gunst der veröffentlichten Meinung eindeutig auf Datenschutzseite. Ein wesentlicher Grund, zumindest Anlaß dafür sind die von den Datenschutzbeauftragten des Bundes und der Länder den Parlamenten jährlich zu erstattenden Berichte und die sich darum rankende öffentliche Diskussion nach Wertung in den Medien. Vielleicht sind deren Motive nicht uneigennützig, weil sie, solange die Sicherheitsorgange im Mittelpunkt des Interesses stehen, selbst nicht einer kritischen Betrachtung unterworfen werden! Die Organe der öffentlichen Sicherheit befinden sich dabei immer in der Defensivrolle. Das erschwert ihre Situation, zumal sie nur selten und dann sehr verhalten Unterstützung erfahren. Es ist nicht populär, sich für Belange der öffentlichen Sicherheit zu engagieren.

Ich will deshalb hier die Gelegenheit wahrnehmen, für die Polizei den Versuch einer Standortbestimmung zu wagen; einen solchen halte ich schon deshalb geboten, um den in der Öffentlichkeit entstandenen Eindruck von unzulässiger, ja gar rechtswidriger Tätigkeit der Polizei zu korrigieren, oder wenigstens zu relativieren. Dabei beziehe ich mich insbesondere auf die Feststellung des Bundesbeauftragten für den Datenschutz in seinem 4. Tätigkeitsbericht mit der Aussage, er habe schwerwiegende Verstöße gegen das Datenschutzrecht festgestellt. Das ist übrigens so nicht richtig, wenn man unter einem Verstoß ein bewußtes, gewolltes Zuwiderhandeln versteht. In den beanstandeten Fällen entsprachen teils alte, übernommene Bestände noch nicht den neuen Regelungen und teils waren Fälle von Erkenntnisübermittlungen streitig.

Für die Polizei ist dies eine neue Situation. Sie war bisher hinsichtlich der Beurteilung der Rechtmäßigkeit ihres strafverfolgungs- bzw. verwaltungsmäßigen Handelns auf die Justiz fixiert und findet sich nun mit anderen offiziellen und auch inoffiziellen Stellen

konfrontiert, die sich dazu berufen fühlen, zweifelsfreie Würdigungen abgeben zu müssen, die m.E. teils über ihre Kompetenz und auch über Fragen des Datenschutzes hinausgehen. Diese dann mit dem Anspruch absoluter rechtlicher oder wissenschaftlicher Autorität verbreiteten und von einem dafür besonders aufnahmebereiten Teil der Öffentlichkeit aufgenommenen Argumente werden umgesetzt mit der Folge allgemeiner Verunsicherung, nicht nur der Polizei. Ich möchte klarstellen, daß ich keine Konfrontation zwischen Polizei und Datenschutz heraufbeschwören oder verschärfen will. Wer eine polemische Abrechnung erwartet, den werde ich enttäuschen. Es kommt mir im Gegenteil sehr darauf an, deutlich zu machen, daß ich im Interesse der Sache einem von Vernunft getragenen, der jeweiligen Aufgabe und Verantwortung verpflichteten sinnvollen Nebeneinander das Wort reden möchte. Dazu gehört nach meiner Auffassung vor allem, daß die andersartige Aufgabe und Interessenlage des Gegenübers respektiert wird. Allerdings darf dabei nicht immer mit noch nicht faßbaren, ja noch streitigen Rechtsentwicklungen operiert werden. Wir haben m. E. in dieser Richtung genug Vorleistungen erbracht. Unabhängig davon halte ich ein angemessenes Spannungsverhältnis zwischen Polizei und Datenschutz für ganz normal. Anormal ist m. E. nur ein Zuviel, wie übrigens auch ein Zuwenig. In beiden Fällen stimmt etwas nicht.

Zur Frage der Notwendigkeit und Erforderlichkeit des Einsatzes der Datenverarbeitung bei der Polizei ist schon viel nachgedacht und gesagt worden. Alle Überlegungen zu dieser Frage - von welcher Seite auch immer sie ansetzen - müssen die Menge der im Rahmen polizeilicher Aufgabenerfüllung anfallenden Informationen berücksichtigen. Eine sinnvolle und effektive Sammlung bzw. Auswertung dieser notwendigen Informationen mit konventionellen Mitteln ist bei jährlich mehr als 4 Millionen Straftaten mit ca. 1,5 Millionen Straftätern nicht zu bewältigen. In besonderem Maße betrifft dies die mit gesetzlich zugewiesenen Sammlungs- und Auswertungskompetenzen ausgestatteten polizeilichen Zentralstellen - die Landeskriminalämter und das Bundeskriminalamt. Die Frage des Verzichts auf EDV als bei oberflächlicher Betrachtung rigoroseste Form des Datenschutzes stellt sich somit nicht. Der Datenschutz als Ausfluß des Zeitgeistes - und dies durchaus positiv betrachtet - wäre auch ohne DV gekommen, vielleicht anders oder etwas später. Bei der Polizei mußte sich aber das Datenschutzbewußtsein in so konkreter, detaillierter Form erst ausprägen. Bis zu diesem Zeitpunkt war die Polizei nicht verpflichtet, jede Sammlung zu begründen, zu beschreiben, sie offenzulegen

und sogar personenbezogene Auskünfte zu geben. Eine so weitgehende Regelung kann man anordnen, das augenblickliche Verständnis dafür aber kaum, das muß wachsen. Vielleicht hat das Problem auch aus anderer Sicht seine Ursache mit darin, daß der Datenschutz das später geborene Kind ist. Trotz der stürmischen Realisierung polizeilicher Projekte wären sicher Regelungen bedacht und berücksichtigt worden, die eine bessere Basis für weitergehende Datenschutzgedanken dargestellt hätten; denken wir nur an Wiedervorlagefristen oder an maschinelle Löschungsfunktionen. Die Tatsache, daß vielfach aus der drückenden Situation heraus - ich denke an das Projekt PIOS für die Terrorismusbekämpfung - Informationsbestände aus Karteien oder auch bereits aus Dateien global ohne große aufwendige Aussonderungsmaßnahmen über- und dann fortgeführt worden sind, hat dann zu Beanstandungen Anlaß gegeben, ohne daß es eben Verstöße gibt.

Aber welche Alternative gab es damals? Zu Bereinigungsaktionen, d.h. nicht nur im System löschen, sondern vorgeschaltet Akten ziehen, durchsehen und aktualisieren, blieb keine Zeit. Beides gleichzeitig ging einfach nicht, sollten nicht die dringenden Aufgaben grob vernachlässigt werden. Schließlich war der Staat in Gefahr. Umsomehr kommt es darauf an, die großen Anstrengungen der Polizei hervorzuheben, denen sie sich in den letzten Jahren unterzogen hat, um den für sie geltenden allgemeinen oder bereichsspezifischen Datenschutzregelungen bei ihrer Informationsverarbeitung auch retrograd Rechnung zu tragen. Diese Aspekte der zum Thema "Polizei und Datenschutz" notwendigen Gesamtschau kommen in der öffentlichen Diskussion leider oft viel zu kurz. Ebenso trifft das zu für die Tatsache, daß die Polizei gewisse Formen des Datenschutzes schon immer praktiziert, indem sie z.B. die ihr zur Verfügung stehenden Informationen grundsätzlich nur innerpolizeilich nutzt.

Die Polizei hortet auch keine Informationen, sie sammelt sie zur Erfüllung der ihr gesetzlich übertragenen Aufgaben, der Gewährleistung der öffentlichen Sicherheit und Ordnung durch die Verfolgung von Straftaten und Abwehr von Gefahren unter Beachtung der unbestrittenen Individualrechte auch von Störern im weitesten Sinne, allerdings ohne daß sie Privilegien genießen. Verlautbarungen, daß in dem Kriminalaktennachweis mittels eines Datenverarbeitungs- und Fern-

übermittlungssystems die Namen aller mit der Polizei in Berührung gekommenen Bürger, also der Verdächtigen, Anzeigenden, Zeugen oder Opfer oder gar die gesamte Bevölkerung erfaßt worden sind - oder werden sollten - sind unzutreffend.

Das Aufgabenfeld der Polizei ist dabei wie kaum ein anderer öffentlicher Bereich durch Gesetze und Rechtsvorschriften reglementiert, die noch durch innerdienstliche Vorschriften ergänzt werden. In den KpS- und den korrespondierenden Dateienrichtlinien sowie den danach zu erstellenden Errichtungs- bzw. Feststellungsanordnungen für Dateien sind exakt die Personenkreise bezeichnet, deren Personalien in der jeweiligen Datei gespeichert werden dürfen. Bei Kenntnis und Anerkennung dieser Tatsache besteht ein legitimer Anspruch der Polizei darauf, ihr Handeln grundsätzlich als rechtmäßig anzusehen und es nicht ständig mit Mißtrauensvermutungen oder gar mit Mißbrauchsbehauptungen in Frage zu stellen.

Erlauben Sie mir, Fragen des polizeilichen Datenschutzes zunächst unter dem Aspekt zu erörtern, daß der Datenverarbeitung in gewissem Sinne Datenschutz bereits immanent ist. Das zeigt sich zunächst an einem Vergleich der Aktualität von on-line-Informationssystemen, wie wir sie in INPOL vor uns haben, mit der des konventionellen Nachrichtenaustauschs. Konkret bedeutet dies z.B. für die Personenfahndung, daß vor Einsatz der Datenverarbeitung Fahndungsersuchen im Deutschen Fahndungsbuch bekanntlich bis zu 4 Wochen und in den Personenfahndungskarteien mehrere Tage aufgrund der redaktionellen Arbeiten zur Aktualisierung veraltet waren. In der Personenfahndungsdatei dagegen führt die Rücknahme eines Fahndungsersuchens augenblicklich zur Inaktualisierung, und eine unzulässige Beeinträchtigung der schutzwürdigen Belange des Betroffenen ist insoweit nicht mehr möglich. Aktualität bedeutet also praktizierter Datenschutz.

Am Beispiel des Personenfahndungssystems lassen sich jedoch auch noch weitere Maßnahmen praktischen polizeilichen Datenschutzes verdeutlichen. Ich meine damit die Zugriffsschutz- und Auskunftsbeschränkungsregelungen, wie sie sich auch in anderen Anwendungen von INPOL finden. Ich verweise damit auf PIOS, ein System, das schon mehrfach öffentlicher Kritik ausgesetzt war.

Die Zugriffsschutzregelungen waren von Anfang an Bestandteil von PIOS, also längst polizeiliche Praxis, bevor es ein BDSG gab. Dort sind sogar jeweils spezielle Dateien eingerichtet für die Bekämpfung des Terrorismus, der Staatsgefährdung, des Landesverrats und der Rauschgiftkriminalität. Zugriffsschutz bedeutet, daß - streng an den Grundsätzen der Erforderlichkeit und der Verhältnismäßigkeit orientiert - jedem - zumindest im Direktzugriff - nur die Daten zugänglich sind, die er zu seiner Aufgabenerfüllung benötigt. In Ausformung der entsprechenden Bestimmungen in den Datenschutzgesetzen von Bund und Ländern enthalten die bereits genannten Vorschriften bzw. Richtlinien hierzu konkrete Regelungen. So ist das Bundeskriminalamt z.B. verpflichtet, für jede einzelne von ihm geführte Datei den Kreis der darauf zugriffsberechtigten Dienststellen exakt festzulegen. Die Einhaltung dieser Vorgaben wird durch programmtechnische Routinen gewährleistet, die sich der Manipulation durch eine anfragende Stelle entziehen. So wird der datenschutzrechtlich bedeutsame Grundsatz "Jedem nur soviel Daten wie nötig" mit Leben erfüllt.

Besonders deutlich und augenfällig wird dies an dem gerade im Aufbau befindlichen, Forderungen des Datenschutzes berücksichtigenden Kriminalaktennachweis (KAN), der sich als ein bundesweit abfragbares Auskunftssystem nur den mit der Bearbeitung kriminalpolizeilicher Ermittlungsvorgänge befaßten Dienststellen erschließt und auch diesen nur Aufschluß über das Vorhandensein von Kriminalakten einer Person und nicht über deren Inhalt gibt. Grenzdienststellen, Zoll und Bahnpolizei - allesamt zugriffsberechtigt für das Fahndungssystem - sind von der Nutzung ausgeschlossen, weil ihre Aufgabenstellung eine derartige Zugriffsmöglichkeit nicht bedingt. Zweifel muß man aber anmelden, ob die Regionalisierung, ja Separierung polizeilicher Datenbestände neben fraglichen kriminalpolizeilichen Aspekten dem Datenschutz im behaupteten Maße Rechnung trägt. Ein z.B. irgendwo erstmals aufgetretener Straftäter - ein unbeschriebenes Blatt - kann mehr oder weniger in den 10 anderen Bundesländern straffällig geworden sein, ohne daß die ermittelnden Polizeidienststellen von den jeweils an anderer Stelle vorhandenen Kriminalakten erfahren müssen. Die Regionali-

sierung vermindert dabei nahezu die Feststellung der im KAN-Konzept als Erfassungskriterium vorgesehenen "erneuten Straffälligkeit des Beschuldigten oder Tatverdächtigen außerhalb seines Wohn- oder Aufenthaltsbereichs". Die in vielen Fällen dadurch geradezu herausgeforderte ungezielte konventionelle FS-Anfrage nach Erkenntnissen würde vermieden, wenn über einen Nachweis gleich die auskunftsfähigen Dienststellen bezeichnet würden. Eine unnötig weite Streuung von Anfragen - verbunden mit einer zumindest kurzen Darstellung des zugrundeliegenden Sachverhaltes - dürfte für den Betroffenen belastender sein. Aber noch ein weiterer Punkt läßt Zweifel an der datenschutzrechtlichen Schlüssigkeit des KAN einerseits, wie auch an seiner kriminalistischen Effektivität andererseits aufkommen. Es ist das Problem einer einheitlichen Aktenaussonderung. Die isolierte, inselartige Aussonderung nur aufgrund eigener Aktenlage ist im Ergebnis sowohl für den Betroffenen als auch für die Arbeit der Polizei wenig befriedigend. Es ist zu hoffen, daß in die für die endgültige Verabschiedung des KAN-Konzepts durch die IMK beschlossene Prüfung der Effektivität und Wirksamkeit datenschutzrechtliche und polizeiliche Interessen kritisch einbezogen werden.

Für den Erkennungsdienst fordert der Datenschutz eine an den KAN-Kriterien orientierte Regelung, d.h. in der Praxis die Auflösung der zentralen daktyloskopischen Sammlung beim BKA und deren Beschränkung auf KAN-relevante Personen sowie Errichtung entsprechender Ländersammlungen. Keine Stelle könnte dann verbindlich Auskunft geben, ob über eine Person bereits ED-Material vorliegt mit der Folge, daß von dem Betroffenen - wenn nicht in der bereits länderbezogenen Sammlung einliegend - erneut Fingerabdrücke und Bilder gefertigt werden müßten. Ein Spurenvergleich, mit dem Ziel Täter zu ermitteln, würde nahezu verhindert.

Der bei einer Identifizierungsmaßnahme erforderliche Aufwand wäre erheblich (Telebild oder Versand möglicherweise an 11 Sammlungen, 11mal klassifizieren und recherchieren). Dies geht zeitlich in vielen Fällen sicher zu Lasten der Betroffenen, wie auch Maßnahmen im Rahmen wiederholter Personenfeststellungsverfahren einschließlich Lichtbildvorlage und Befragung von Auskunftspersonen. So wird Datenschutz auf den Kopf gestellt. Dazu gehört m. E. auch die Forderung, daß -

natürlich unter den gesetzlichen Voraussetzungen - Fingerabdrücke genommen werden können, jedoch der Grund auf dem Fingerabdruckbogen nicht vermerkt werden soll. Die Logik vermag ich nicht zu erkennen.

In diesem Zusammenhang sollte auch nochmals die insbesondere vom Datenschutz aufgeworfene Frage angesprochen werden, ob gemäß §§ 1 und 2 BKA-Gesetz davon auszugehen ist, daß andere als KAN-Daten dem BKA nicht zu übermitteln sind, mit Ausnahme der gesetzlich ausdrücklich vorgesehenen Haftdaten des § 4 BKA-Gesetz. Dieser Auffassung ist aus der Absicht des Gesetzes heraus zu widersprechen. Die Zielrichtung des KAN ist eine andere als die des KPMD. Mit dem KAN ist bezweckt, den polizeilichen Sachbearbeiter auf das Vorhandensein vom Kriminalakten aufmerksam zu machen. Der kriminalpolizeiliche Meldedienst hingegen regelt einen ganz anderen Sachverhalt, nämlich alle Nachrichten und Unterlagen für die Verbrechensbekämpfung zu sammeln und auszuwerten. Während der KAN die Auskunft über bestehende Erkenntnisse ermöglicht, sollen durch die Auswertung im Rahmen des KPMD auskunftsfähige Erkenntnisse erst gewonnen werden. Auskunft und Auswertung sind also zwei völlig verschiedene Bereiche, die deshalb auch differenzierter datenschutzrechtlicher Würdigung bedürfen.

Kurz sollte auf die Datenerhebung eingegangen werden. Diese Vorstufe der Speicherung unterliegt z.Z. noch nicht den Datenschutzgesetzen, sie soll auf Bestreben der Datenschutzbeauftragen jedoch in den Datenschutz einbezogen werden. Gegen ein solches Vorhaben müssen aus polizeilicher Sicht Bedenken angemeldet werden. Die Polizei lebt von Informationen der Bürger; vielen muß in diesem Zusammenhang sogar Vertraulichkeit zugesichert werden, um Gefährdungen, Nachteile oder Enttarnungen zu verhindern. Der Novellierungsvorschlag würde einen schwerwiegenden Eingriff in die polizeiliche Informationsgewinnung bedeuten. Die Folgen sind jedem Fachmann einsichtig. Wenn dennoch die Datenerhebung allgemein datenschutzrechtlich relevant werden soll, bedarf es einer absoluten Ausnahmeregelung für die Sicherheitsbehörden. Im übrigen sind Anlässe und Formen der polizeilichen Datenerhebung durch gesetzliche Vorschriften schon so weitgehend reglementiert, daß damit dem Schutzbedürfnis der Betroffenen in vollem Umfang Genüge getan wird.

Ständig Gegenstand datenschutzrechtlicher Überlegungen und Ausgangspunkt von Forderungen nach Einschränkungen hinsichtlich der Quantität und Qualität ist die Übermittlung von Daten. Polizeiliche Informationen dienen der Verbrechensbekämpfung; zu diesem Zweck müssen sie aus verschiedenen Anlässen innerhalb der Polizei - in Ausnahmefällen auch an außerpolizeiliche Stellen - übermittelt werden. "Übermitteln" bedeutet gemäß Legaldefinition das Bekanntgeben gespeicherter oder durch Datenverarbeitung unmittelbar gewonnener Daten an Dritte durch Weitergabe oder Einsichtnahme bzw. Abruf. "Dritter" ist dabei jede andere als die speichernde Stelle. Diesen Begriffsbestimmungen liegt nach heute allgemein anerkannter Auffassung der organisatorische Behördenbegriff zugrunde. Somit sind also z.B. das BKA und die Landeskriminalämter Dritte zueinander. Datenübermittlungen zwischen diesen Stellen i.S. von § 2 BDSG unterliegen daher dem Gesetz und damit auch der Kontrollbefugnis durch den Bundesbeauftragten für den Datenschutz. Ein anderer Denkansatz, der von der gleichartigen Aufgabenstellung der Polizeien von Bund und Ländern ausging und daraus die Folgerung glaubte ableiten zu können, die Polizei sei als Einheit zu sehen, die nicht Dritter zu sich selbst sein könne, hat sich nicht durchgesetzt. Das Ergebnis ist kurios und unbefriedigend. Während der Kriminalbeamte z.B. in Nordrhein-Westfalen über nahezu jeden dritten der Bevölkerung der Bundesrepublik Auskunft erhält, weil die speichernde Stelle diesen Bereich umfaßt, erhält der saarländische Kollege nur über jeden sechzigsten Informationen. Für ihn sind alle anderen Dritte.
Nun gehen die Vorstellungen des BfD - wie mehrfach verlautbart - offenbar weiter in Richtung auf ein deliktbezogenes Splitten. Das mag, juristisch gesehen, Sinn haben, ausgehend von "einschlägig vorbestraft"! Kriminalistisch erscheint dies absurd, es sei denn, alle Täter verpflichten sich, deliktstreu zu sein.

Für die Polizei sind die Übermittlungsregelungen des § 10 BDSG in den Dateien- und KpS-Richtlinien konkretisiert worden. Dabei spielt die on-line-Übermittlung - auch in der Datenschutzdiskussion - eine herausragende Rolle, da konkrete Einzelfallprüfungen dabei nicht vorgenommen werden. Es wird von der generellen Abfrageberechtigung einer Dienststelle ausgegangen und auf die Zulässigkeit und Erforderlichkeit der Einzelanfrage geschlossen. Um unzulässige Anfragen zu erschweren bzw. zu verhindern, ist sicherzustellen,

daß Datenendgeräte nur von den jeweils berechtigten Bedienern benutzt werden können; sie müssen sich beim Rechner legitimieren, worauf dieser ihnen die auf sie zugeschnittene Auskunft zur Verfügung stellt.

Im Bereich der on-line-Übermittlung im Bundeskriminalamt werden Anfragen und Auskünfte nicht protokolliert. In der Anlage zu § 6 BDSG ist in diesem Zusammenhang lediglich vorgeschrieben, daß "überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten durch selbsttätige Einrichtungen übermittelt werden können". Diesem Anspruch kann jederzeit durch Einsicht in die Unterlagen und durch Kontrolle genügt werden. Das Bundeskriminalamt - nicht alle LKÄ - hat von einer Protokollierung insgesamt Abstand genommen, weil dadurch eine Vielzahl für die Aufgabenerfüllung nicht erforderlicher Daten gespeichert würde und darüber hinaus der Aufwand außer Verhältnis stünde. Auch der Bundesbeauftragte für den Datenschutz ist von seiner zunächst erhobenen Forderung nach Protokollierung abgerückt. Gleichwohl gibt es dabei unter dem Aspekt Datenschutz eine genau gegenteilige Auffassung. Man mag daran sehen, daß in gleicher Zielsetzung manche Maßnahmen auch unter Datenschützern ganz unterschiedlich gesehen werden. Der Verzicht auf Protokollierung ist m. E. aber eine aktive Datenschutzmaßnahme, weil so die Speicherung der Personalien von Personen, die kaum von polizeilicher Relevanz sind, - man denke nur an die Vielzahl der negativen Fahndungsabfragen - gar nicht erst stattfindet. Damit will ich nicht sagen, daß eine protokollierte Personalie gleichsam als elektronische Anhaltemeldung nicht auch einmal ihren kriminalistischen Nutzen haben kann. Es ließen sich Beispiele anführen, wo durch Auswertung von Protokollbändern Informationen direkt erlangt oder gewonnen werden konnten.

Bei konventioneller Übermittlung des Ergebnisses einer Anfrage prüft die auskunfterteilende Stelle, ob die Daten zur rechtmäßigen Erfüllung der Aufgabe benötigt werden. Neben dem Anlaß der Anfrage muß bei bestimmten Stellen der zugrundeliegende Sachverhalt angegeben werden. Umfang und Empfänger einer Auskunft werden in jedem Fall aktenkundig gemacht. Der Vorgang ist so jederzeit nachvollziehbar und nachprüfbar. Bei telefonisch übermittelten Auskunftsersuchen praktiziert die Polizei wegen mehrfach stattgefundener Versuche von Betroffenen oder anderen unbefugten Dritten, die zu einer Person vorhandenen Erkenntnisse zu erlangen, besondere Sicherheitsvorkehrungen. In den Fällen, in denen sich die Gesprächspartner nicht kennen, erfolgt Rückruf unter der Fernsprechnummer der anrufenden Dienststelle und nicht unter der vom

Anrufenden mitgeteilten Rückrufnummer. Vorgänge, wie sie vor mehreren Jahren im Zusammenhang mit dem Fall PLASA in der Öffentlichkeit lebhaftes Interesse gefunden haben, sind praktisch nicht wiederholbar.

Aber die Polizei ist ja nicht nur eine Erkenntnisse übermittelnde, sondern auch eine auf Informationszufluß von außen angewiesene Institution. Und auf diesem Feld hat es durch eine übertriebene Auslegung und Handhabung des Datenschutzes bei der polizeilichen Arbeit die meisten Schwierigkeiten gegeben. Bisher störungsfreie Informationsstränge zwischen Polizei und anderen Behörden - z.B. Arbeitsämtern, Meldebehörden und Ausländerämtern - werden zunehmend undurchlässiger. Selbst Fluggesellschaften und Taxiunternehmen verweigern Auskünfte. Mit dem Zauberwort "Datenschutz" werden berechtigte Auskunftsersuchen der Polizei abgelehnt. Datenschutz als Superrechtsgut. Dieser Eindruck muß sich dem in polizeilicher Knochenarbeit an der Basis ermittelnden Kollegen aufdrängen. Das wirkt demotivierend. Dies ist nicht graue Theorie oder Schwarzmalerei, sondern ließe sich an unzähligen Einzelbeispielen belegen.

Was soll damit gesagt werden? Nicht die gesetzlichen Datenschutzbestimmungen und auch nicht immer die Forderungen der Datenschutzbeauftragten behindern die polizeiliche Arbeit, sondern das in der Öffentlichkeit erzeugte Klima des Mißtrauens gegen die Tätigkeit der Sicherheitsbehörden. Dies stellt das Problem für unsere Aufgabenerfüllung dar. Dabei wird in allen Fällen nichts weiter verlangt als legale, gegen keinerlei gesetzliche Vorschriften verstoßende Informationsübermittlung im Rahmen der Aufgabenerfüllung. Die Verweigerung der Informationen verhindert oftmals die Aufklärung bereits begangener oder die Verhütung vielleicht bevorstehender Straftaten. In manchen Fällen lassen sich die Informationen mit viel Aufwand durch zeitraubende Maßnahmen anders ermitteln. Durch Bindung der Kräfte werden aber weniger Straftaten geklärt und darüber hinaus mehr begangen. Den Mehraufwand auffangende Personalverstärkungen gibt es nicht, er geht zu Lasten der Sicherheit der gesetzestreuen Bürger.

Nicht anders ist die Problematik bei Anforderung von Dateibeständen für Abgleiche, z.B. in der Personenfahndung, obwohl es sich nur um die Daten handelt, zu denen die Polizei z.B. nach den Meldegesetzen Zugang hat, und von denen sie ohnehin nur die zur Kenntnis nimmt, die gesuchte Personen betreffen. Wie nachhaltig negativ die Reaktion einer unzureichend und falsch informierten Öffentlichkeit sich auf die polizeiliche Tätigkeit auswirken kann, stellte sich insbesondere im Laufe der Diskussion um die sogenannte Rasterfahndung sehr deutlich heraus. Alle im Zusammenhang mit der Durchführung einer Rasterfahndung bedeutsamen Vorgänge, die Lagebeurteilung, Festlegung der Verdachtskriterien für die Auswahl des Vergleichsdatenbestandes, das technische Verfahren des Datenabgleichs und die kriminalistische Behandlung der Trefferfälle werden dokumentiert und stehen für Nachprüfungen zur Verfügung. Damit wird nach unserer Auffassung datenschutzrechtlichen Anforderungen optimal Rechnung getragen. Wohlgemerkt nach unserer Auffassung, denn nach anderer Meinung ist das "nur ein erfreulicher Schritt in die richtige Richtung".

Ohne nochmals darauf näher einzugehen, hat die Tatsache, daß im Rahmen der systematisierten Fahndung z.B. auch Daten von Energieversorgungsunternehmen herangezogen wurden, z.T. heftige Reaktionen hervorgerufen. Dazu wäre es mit Sicherheit nicht gekommen, wenn seriös recherchiert und dann berichtet worden wäre. In diesem Zusammenhang muß die Frage erlaubt sein, ob es tatsächlich datenschutzrelevant ist, daß jemand Strom bezieht und diesen bar bezahlt, insbesondere unter dem Aspekt, daß die Polizei dies nicht bei allen Strombeziehern, sondern nur bei denjenigen interessiert, bei denen auch andere im Sinne der Maßnahme relevante Kriterien erfüllt sind. Außerdem lagen sogar vom GBA beantragte und vom Ermittlungsrichter des BGH erlassene Beschlagnahmebeschlüsse vor. Soll die Polizei diese vor Vollstreckung tatsächlich erst durch eine weitere Instanz prüfen lassen? Die Forderung des Datenschutzbeauftragten , Fahndungen dieser Art nicht durchzuführen, solange keine Spezialnorm dafür geschaffen ist, kann seitens der Polizei ebenfalls keine Beachtung finden. Auch der datenschutzrechtliche Aspekt der Weiterbehandlung sogenannter Zufallsfunde darf, polizeilich gesehen, kein Problem sein. Wenn z.B. eine Person erkannt wird, gegen die Haftbefehl besteht, dann muß die Polizei zugreifen. Oder soll sie etwa erklären: Sehen Sie zu, daß

Sie weiterkommen; wir ergreifen hier und heute nur Maßnahmen gegen solche Personen, gegen die sich die Fahndung direkt richtet. Soll etwa das Legalitätsprinzip für die Polizei aufgebrochen werden?

Im Zusammenhang mit Datenübermittlung soll der Vollständigkeit wegen und um die Meinung der Polizei hierzu ganz unmißverständlich zu verdeutlichen, noch auf den Datenaustausch - auch on-line - zwischen Polizei und anderen Behörden, hier insbesondere mit dem Ausländerzentralregister, dem Kraftfahrt-Bundesamt und dem Bundeszentralregister eingegangen werden.

Die Notwendigkeit des Zugriffs auf die genannten Bereiche dürfte unter dem Aspekt der Erforderlichkeit für die polizeiliche Aufgabenerfüllung kaum in Frage zu stellen sein. Der Datenschutz widerspricht den polizeilichen Forderungen mit dem formalen Argument, ein on-line-Anschluß bedeute das Zurverfügungstellen der gesamten Datei. Dies sei zur Aufgabenerfüllung der Polizei nicht erforderlich. Es würden immer nur die Daten der Personen benötigt, die gerade polizeilich relevant seien. Das ist richtig. Die Polizei fragt aber selbstverständlich nur nach Personen, mit denen sie sich im Rahmen ihrer Aufgabenerledigung befaßt. Das Argument des Datenschutzes, die Polizei erhalte durch Einsicht in die verschiedensten Dateien ein umfassendes Persönlichkeitsbild eines Beschuldigten, das alle Lebensbereiche einschließe, ist Theorie, es ist unzutreffend.

Nicht als das befürchtet große Problem hat sich bisher die Handhabung der gesetzlichen Regelung erwiesen, Auskunft an den Betroffenen zu erteilen und von der Befreiung zur Auskunftserteilung gem. § 13 Abs. 2 BDSG keinen grundsätzlichen Gebrauch zu machen. Die erwartete Flut von Anfragen besorgter Bürger ist ausgeblieben, wenn man von propagandistisch gesteuerten Aktionen mit vorgefertigten Texten und in Einzelfällen mit gewisser Hartnäckigkeit absieht. Das Interesse am "polizeilichen Kontoauszug", wie einmal formuliert wurde, ist relativ gering. Eigentlich müßten Gesetzgeber und insbesondere Datenschutzbeauftragte sehr enttäuscht sein. Das BKA hat - und ähnlich ist die Situation in den Ländern - seit 1980 wie folgt Anfragen erhalten und erledigt:

Zeitraum	gesamt	Negativ-auskunft	Auskunfts-erteilung	Auskunfts-verweigerung
1980	414	245	113	56
1981	267	182	61	24
1982	122	78	28	16
	803	505	202	96
		(63%)	(25%)	(12%)

Fälle, in denen durch falsche Legitimation der Versuch unternommen wurde, Auskünfte über andere - Dritte - zu erlangen, wurden nicht bekannt. Zur Handhabung gibt es dazu bekanntlich die von der AG Kripo beschlossene einheitliche Regelung der Übermittlung mittels einfacher Zustellungsurkunde.

Wie sich die Situation gestalten wird, wenn andere - Nichtverdächtigte - entsprechend den Dateienrichtlinien nach einem Jahr Speicherung von uns aus benachrichtigt werden müssen, ist noch nicht abzusehen. Wir wissen um die Problematik, die Interessenkollision, wenn in bestimmten Bereichen - wie der Terrorismus - oder Rauschgiftbekämpfung - zunächst auch über solche Personen Informationen gespeichert werden müssen,um sie zu verifizieren oder falsifizieren. In solchen Fällen werden wir sehr genau abwägen müssen, um nicht durch punktuelles Offenlegen weitergehende Schlüsse auf Maßnahmen zu ermöglichen.

Die Betrachtung der Problematik von Datenübermittlungen wäre unvollkommen, wenn sie den internationalen Bereich nicht einschlösse. Auch dieses Feldes haben sich die Datenschutzbeauftragten intensiv angenommen. Der Bundesbeauftragte für den Datenschutz etwa steht auf dem Standpunkt, INTERPOL sei ein rechtlich nicht faßbares Gebilde und damit juristisch nicht existent. Er bemängelt insbesondere den freizügigen Informationsfluß im Rahmen der internationalen Verbrechensbekämpfung, die Mitteilung von Informationen, wenn sie andere als das gerade in Frage stehende Delikt betreffen, die Tatsache, daß die Aufbewahrungszeit der Informationen beim Empfänger vom Absender nicht mehr zu kontrollieren ist, das Fehlen eines Kontrollorgans

und, daß Betroffene keine Auskunft erhalten. Seine von uns unterstützte Initiative traf beim Generalsekretariat bereits auf Überlegungen zum datenschutzgerechten Nachrichtenaustausch innerhalb der IKPO. Es ist vorgesehen, die Modalitäten der Informationsübermittlung, der Aufbewahrung von Unterlagen, der Auskunft an den Betroffenen und der Kontrolle durch eine unabhängige, möglichst externe Instanz in einer Konvention für die Mitgliedstaaten der IKPO verbindlich festzulegen. Entsprechende Grundsätze sind von der 51. Generalversammlung der IKPO beschlossen worden. Die Arbeiten daran sollen bis zur nächsten Generalversammlung erledigt sein. Das Bundeskriminalamt hat die Arbeiten und die Richtlinien maßgeblich mitgestaltet; allerdings sind wir dort einer unter vielen und unsere Meinung ist nicht allgemeingültig.

Obwohl wir also Regelungen begrüßen, besteht dennoch bei uns generell eine andere Sichtweise des Problems als bei den Datenschutzbeauftragten, nämlich, daß der gesamte personenbezogene Nachrichtenaustausch zwischen den Mitgliedern der IKPO derzeit nicht dem Regelungsbereich des BDSG unterliegt.

Eine datenschutzrechtlich relevante Übermittlung könnte vorliegen, wenn in Dateien gespeicherte oder durch Datenverarbeitung unmittelbar gewonnene Daten an Dritte weitergegeben oder zur Einsichtnahme namentlich zum Abruf bereitgehalten wurden, so § 2 Abs. 2 Nr. 2 BDSG. Tatsächlich werden jedoch konventionell, d.h. auf dem Fernmelde- oder Postweg, Informationen ausgetauscht, die in den Akten des Bundeskriminalamtes oder sonstiger Polizeibehörden enthalten sind. Diese können nicht durch automatisierte Verfahren umgeordnet oder ausgewertet oder gewonnen werden und unterliegen damit nicht dem Dateibegriff. Eine Zuständigkeit des BfD könnte aufleben, wenn ein internationales Datenverarbeitungssystem der IKPO Realität werden sollte. Das ist noch ferne Zukunft.

Wenn bisher nur von Datenspeicherung und Übermittlung die Rede war, muß ich, um den Kreis zu schließen, auch noch kurz auf den Komplex der Löschung von Daten und die Bereinigung bzw. Vernichtung von Unterlagen eingehen. Es ist geboten, Daten zu löschen bzw. zu vernichten, die nicht - nicht mehr - erforderlich sind. Daß die Polizei dies im Rahmen der für sie geltenden Richtlinien oder Dienstanweisungen tut, ist selbstverständlich. Zeitweise waren und sind allein im BKA bis

zu 100 Mitarbeiterinnen und Mitarbeiter mit nichts anderem als Aussonderungsprüfungen befaßt. Parallel dazu wird eine solche Prüfung von allen Sachbearbeitern im Rahmen aktueller Vorgangsbearbeitung verlangt. Sieht man daneben noch die gleichartigen Anstrengungen der Länder, darf dem so quantifizierbaren personellen und materiellen Aufwand die Anerkennung nicht versagt werden, insbesondere in Anbetracht des Umfanges der übrigen polizeilichen Aufgaben, die nicht ab-, sondern zugenommen haben. Die Polizei will nicht "den letzten rostigen Nagel" über einen unvertretbaren Zeitraum aufbewahren, sondern tritt für eine kriminalistisch sinnvolle, verantwortungsbewußte Aktenbereinigung ein. Der Beurteilungsrahmen für die in diesem Zusammenhang immer erforderliche Prognose darf allerdings nicht zu eng angesetzt werden, damit später nicht mehr schließbare Erkenntnis- oder Fahndungslücken entstehen.

Erlauben Sie mir zum Schluß noch einige grundsätzliche Gedanken. Datenschutz, wie auch polizeiliche Arbeit, werden nicht auf der "grünen Wiese" betrieben, sondern in unserer Gesellschaft. Das bedeutet, auch Datenschutz muß sich m. E. wie polizeiliche Arbeit in unser gesellschaftliches Leben einfügen. Der Datenschutz sieht offenbar den einzelnen aber nicht so sehr in seiner Gemeinschaftsbezogenheit, sondern betont seine Stellung als schutzbedürftiges Individuum. Das bedeutet aus der Sicht des Datenschutzes offenbar "Datenschutz um jeden Preis"; zumindest erscheint dies oft so. Das ist die eine Seite der Medaille.

Andererseits allerdings haben auch wir sicher unbewußt, ungewollt zu Fehlinterpretationen, Unbehagen und Reaktionen beigetragen, und zwar weniger durch Nutzung der Datenverarbeitung als allein durch unbedachte, mißverständliche, ja Gefahr suggerierende Wortschöpfungen oder Schweigen. Bei "automatische" oder "rationalisierte Verdachtgewinnung" kann sich z.B. der Gedanke aufdrängen, der Mensch werde der Maschine unterworfen, deren Funktionen zudem nicht nachvollziehbar und undurchschaubar sind. Vielleicht glaubt mancher Bürger im Rüttelsieb der Rasterfahndung hängen zu bleiben. So sollten und müssen wir Verständnis für kritische Betrachtung unseres Tuns aufbringen. Wer einen Kampf - wie die Polizei - am unmittelbarsten führt, läuft Gefahr, das rechte Augenmaß zu verlieren. Tatsächlich wird - allerdings nicht nur bei der Polizei - immer der erfolgreicher sein, der über die besseren Informationen verfügt, wo immer er sie her hat. Information ist eben Macht, sie sollte durchaus kontrolliert, die polizeiliche Arbeit dadurch aber nicht stranguliert werden.

Die Gesellschaft wird die polizeilichen und datenschutzrechtlichen Positionen bestimmen müssen, d.h. die Politiker sind aufgerufen, dies in Abwägung der Rechtsgüter "Sicherheit und Ordnung" und "Datenschutz" zu tun.

Datenschutz und Polizei

Spiros Simitis

1. Zwei Vorbemerkungen

1.1 Über Datenschutz und Polizei ist oft und intensiv diskutiert worden. Umso mehr verwundert die wohl immer noch verbreitete Vorliebe für radikale Vereinfachungen. Die Formel "Sicherheit geht vor Datenschutz" ist nur eines von mehreren Beispielen dafür. Der Vorteil liegt auf der Hand: Klare Rangfolgen ersparen mißliebige Konflikte. Der Nachteil läßt sich freilich genausowenig übersehen. Wo Argumente not tun, werden feste Positionen, und zwar in einer Form bezogen, die letztlich eine gemeinsame Reflexion verhindert. Simple Antithesen können eben zumeist unschwer umgekehrt werden, vom Datenschutz läßt sich genauso emphatisch behaupten, er ginge der Sicherheit vor. Die Folge ist leicht auszumachen. In einem Fall sehen sich vor allem die Datenschutzbeauftragten alsbald verdächtigt, das Sicherheitssystem mit ihren Erwartungen zu destabilisieren, im anderen dagegen fühlen sich die Polizeibehörden vom Vorwurf getroffen, gleichsam am Rande der Legalität zu operieren, weil sie gebannt auf den Erfolg ihrer Tätigkeit starrten und deshalb eine der wichtigsten rechtlichen Rahmenbedingungen zu wenig berücksichtigt.

Nicht weniger bedenklich sind freilich Argumentationen, die , genaugenommen, nicht mehr enthalten, als den Hinweis auf die Notwendigkeit, die "Funktionsfähigkeit" des Staates oder überhaupt den "Bestand" staatlicher Ordnung sicherzustellen. Zugegeben, mit Hilfe der "Funktionsfähigkeit" läßt sich trefflich streiten. Wer wird schließlich schon zugeben,für einen "funktionsunfähigen" Staat zu sein oder gar in Abrede stellen, daß es auch und gerade Aufgabe der Rechtsordnung ist, die Voraussetzungen für die Erfüllung staatlicher Funktionen zu schaffen und abzusichern. Nur: Zur Debatte kann und darf nicht eine abstrakte "Funktionsfähigkeit" stehen, sondern immer nur die eines bestimmtes Staates, genauer, des vom Grund-

gesetz näher definierten. Dann aber gilt es vor allem anderen zu fragen, wie sich dessen konstitutive Elemente zum Datenschutz verhalten. Solange diese Frage nicht klar gestellt und ebenso deutlich beantwortet worden ist, sind weitere Aussagen überflüssig, ja gefährlich.

Kurzum, plakative Antithesen und scheinbar inhaltsschwere Formeln verschaffen zwar unter Umständen rhetorische Vorteile, allerdings auf Kosten einer rationalen Diskussion. Mir scheint es deshalb an der Zeit, auf beides endgültig zu verzichten.

1.2 Belastend wirkt sich auch das vom Gesetzgeber gewählte Regelungskonzept des Datenschutzes aus. Anders als etwa in den Vereinigten Staaten hat sich der Gesetzgeber in der Bundesrepublik dafür entschieden, die Datenschutzprobleme in einem einzigen Gesetz anzusprechen und dort generelle, an die Adresse aller speichernden Stellen gerichtete Verhaltensanforderungen zu formulieren. Das BDSG begnügt sich deshalb mit einer Grobeinteilung, die lediglich den "öffentlichen" vom "nicht- öffentlichen" Bereich abhebt. Vergeblich sucht man daher nach Regeln, die den spezifischen Tätigkeitsbedingungen der einzelnen Teile der öffentlichen Verwaltung Rechnung tragen. Die Konsequenz: Der Versuch, präzise Folgerungen für die eigene Aktivität zu ziehen, gerät immer schwieriger. Wer etwa, um beim Beispiel der Polizei zu bleiben, nach den Auswirkungen des Datenschutzes fragt, muß seine Überlegungen auf dem Hintergrund der konkreten Aufgabenstellung der Polizei und der damit zusammenhängenden Erwartungen formulieren. Mit den Generalklauseln des BDSG kann er, so gesehen, wenig anfangen, sie erfüllen ihn im Gegenteil mit Mißtrauen, weil sie Unsicherheit und Interpretationskontroversen fördern.

Wie schwer die Nachteile wiegen, die dieses Regelungskonzept mit sich bringt, zeigt sich nicht zuletzt an der Novellierungsdiskussion. Die Erhebung bleibt, allem äußeren Anschein zuwider, ausgespart. Den Ausschlag dafür haben wohl in erster Linie die von den Sicherheitsbehörde vorgetragenen, durchaus verständlichen

Bedenken gegen eine allgemeine Regelung gegeben. Die Kehrseite ist freilich ein inhaltsleerer Kompromiß. Einmal mehr erweist sich: Das BDSG zwingt mit seiner Regelungstechnik zu abstrakten Auseinandersetzungen und versperrt damit weitgehend selbst den Weg zu einer fundierten inhaltlichen Argumentation und Diskussion. Beides setzt die Bereitschaft voraus, die Abstraktionsebene des BDSG zu verlassen, um sich an konkreten Konflikten und den durch sie gestellten Problemen zu orientieren. Nur dann kann über die Voraussetzungen der Speicherung, die Grenzen der Übermittlung, die Löschungsbedingungen oder mögliche Auskunftsschranken glaubwürdig und überzeugend diskutiert werden.

Immerhin, die Anzeichen einer Korrektur des ursprünglichen Regelungskonzepts verdichten sich. Die Geschichte des Datenschutzes in der Bundesrepublik ist die Geschichte seiner zunehmenden Konkretisierung mit Hilfe bereichsspezifischer Regelungen. Der Sicherheitsbereich ist zweifelsohne eines der wichtigsten Beispiele dafür. Es genügt, an die KpS- oder die Dateienrichtlinien zu erinnern. Auf die Einzelheiten kommt es hier nicht weiter an. Wichtig ist vielmehr nur die Feststellung, daß mit den Richtlinien gleichsam eine Umkehr einsetzt. Die spezifische polizeiliche Situation steckt das Argumentationsfeld ab, die Kenntnis der für sie charakteristischen Konflikte geht in die Diskussion der Datenschutzanforderungen ein und bestimmt ihren Gang.

Der Verzicht auf Pauschalregelungen und simplistische Antithesen und die dezidierte Hinwendung zu bereichsspezifischen Regelungen macht es freilich nicht leichter, die Frage nach den je spezifischen Auswirkungen des Datenschutzes zu beantworten. Im Gegenteil, der Datenschutz erweist sich als ein komplizierter und mühevoller Lernprozeß, in dem es zunächst vor allem darauf ankommt, Problembereiche exakt zu umschreiben, um dann punktuelle, strikt problemorientierte Lösungen auszuarbeiten.

2. Vorweg freilich, so viel zur Erinnerung:
Ähnlich wie in allen Bereichen der öffentlichen Verwaltung hat auch der Informationsbedarf der Polizei signifikant zugenommen. Schon mit Rücksicht auf die sich permanent ändernden Erscheinungsformen der Kriminalität. Je mehr beispielsweise Rauschgiftdelikte an Bedeutung gewinnen, desto notwendiger sind Daten, die Aufschluß über die Entstehung und den Hergang von Straftaten in diesem einen besonderen Bereich geben könnten. Zudem: Fast jeder Versuch, die Fahndungsmethoden neuen Kriminalitätsformen und gewandelten Umweltbedingungen anzupassen, wirkt sich auf den Informationsbedarf der Polizei aus. Konkret: Der für die Strafverfolgung unerläßliche Individualisierungsprozeß ist dort ungleich datenintensiver, wo Arbeits- und Wohnbedingungen von vornherein auf Anonymität angelegt sind, sich also ihrer ganzen Struktur nach der Entstehung eines festen, Außenstehenden jederzeit erkennbaren individuellen Bezugsrahmens widersetzen. Die Polizei kann unter diesen Umständen Straftaten letztlich nur auf dem Umweg über eine Vielzahl von Informationen aufklären, die es erlauben, allmählich mehr und mehr Gewißheit über den Täter zu gewinnen. Nicht zu unterschätzen sind schließlich die Konsequenzen der Bemühungen, das soziale Umfeld einzubeziehen, um Tat und Täter besser zu verstehen. Einmal mehr verändern sich die Informationserwartungen beträchtlich. Ganz gleich etwa wie die Überlegungen zu den kriminogenen Faktoren und den möglicherweise damit verbundenen kriminellen Karrieren im einzelnen ausfallen, das Informationsspektrum verbreitert sich. Zu den individuellen Daten kommt eine ganze Reihe umfeldbezogener Angaben, die den Schlüssel zum Verständnis konkreter Verhaltensweisen ebenso bilden sollen wie die Grundlage für Verhaltensprognosen.

Je mehr freilich die Informationserwartungen der Polizei zunehmen, desto deutlicher akzentuiert sich das Interesse an den Informationsmöglichkeiten, die sich aus den in den übrigen Bereichen der öffentlichen Verwaltung vorhandenen personenbezogenen Daten ergeben. Niemals zuvor vermochte die öffentliche Verwaltung in der Tat ein so genaues

Bild des einzelnen zu vermitteln. Kaum verwunderlich: Wo staatliche Leistungen die Entwicklung des einzelnen begleiten und damit sein Lebenslauf mehr und mehr programmiert wird, maximiert sich zugleich das Interesse an Informationen zu seiner Person. Die personenbezogenen Daten sind selbstverständliche Voraussetzung einer ebenso personenbezogenen staatlichen Aktivität. Anders ausgedrückt: Der Leistungsempfänger ist der in eine Vielzahl sorgfältig registrierter und verarbeiteter Leistungsfaktoren aufgeschlüsselte einzelne.

Vordergründig bringen diese Daten nur dem Teil der öffentlichen Verwaltung einen Informationsgewinn, der sie mit Rücksicht auf die eigenen Aufgaben erhebt und verarbeitet. In Wirklichkeit stellen aber die einmal gespeicherten Angaben eine Informationsreserve dar, die potentiell der gesamten öffentlichen Verwaltung zugute kommen kann. Den Weg dazu öffnet die automatische Datenverarbeitung. Mit ihrer Hilfe kann nicht nur eine letztlich unbegrenzte Zahl von Daten verarbeitet werden. Zum ersten Mal besteht vielmehr die Chance, die Informationsmöglichkeiten, die der vorhandene Bestand an Daten bietet, voll zu nutzen. Die Funktion der einzelnen Behörde mag also nach wie vor die Erhebung der Daten bestimmen, ihre Verwertung ist dagegen tendenziell multifunktional. Nicht von ungefähr war deshalb die Diskussion über das Melderecht von der Vorstellung beherrscht, die Datenbanken der Einwohnermeldeämter in eine Art Datendepot für die öffentliche Verwaltung umzugestalten. Ebensowenig überrascht es, daß der Wunsch, einen Schlüssel bereitzustellen, der den Zugang zu nahezu allen von der öffentlichen Verwaltung verarbeiteten Angaben ermöglichen würde, mit eines der wichtigsten Argumente für die Einführung eines Personenkennzeichens war. Kurzum, der erhöhte Informationsbedarf führt zwangsläufig zu einer anderen Technik und Organisation der Datenverarbeitung und schafft damit zugleich die Voraussetzungen für eine generelle Verwendbarkeit der Daten. Unter diesen Umständen ist es verständlich und konsequent, wenn die Tendenz, diese Verwendbarkeit für die jeweils eigene Arbeit zu aktualisieren, immer deutlichere Formen annimmt.

Wohl am bezeichnendsten dafür sind die Versuche, on-line-Anschlüsse zu etablieren. Der Direktanschluß macht administrative Umwege überflüssig und ermöglicht es, bestimmte, etwa unter Fahndungsaspekten wichtige Daten unmittelbar und jederzeit zu bekommen. Ob es also um die Kfz-Zulassungsstellen oder die Meldebehörden geht, um die beiden bekanntesten Beispiele zu nennen, spielt weiter keine Rolle, das Ziel bleibt gleich: Der Datenbestand einer dritten Stelle soll für polizeiliche Zwecke genutzt werden. Eines darf man dabei freilich nicht übersehen: Solche Erwartungen sind keineswegs polizeispezifisch. Besonders dann, wenn langfristig angelegte, auf die Prävention bestimmter Entwicklungen bedachte Maßnahmen formuliert werden sollen, erscheint es zunächst selbstverständlich, auf sämtliche relevanten Informationen zurückzugreifen, und zwar ohne Rücksicht darauf, wo sie sich gerade befinden. Sozial- und Gesundheitspolitik bieten, weit über die Bundesrepublik hinaus, bezeichnende Beispiele dafür.

3. Mit dem Datenschutz reagiert der Gesetzgeber auf die quantitativen und qualitativen Veränderungen der Informationsverarbeitung. Die Datenschutzgesetze sind, mit anderen Worten, aus der Einsicht in die Gefahren entstanden, die der zunehmende Informationsbedarf und die modifizierten Informationstechniken mit sich bringen. Genaugenommen greift der Gesetzgeber damit Überlegungen auf, die schon in der vierzehn Monate vor dem ersten Datenschutzgesetz, dem hessischen, ergangenen Entscheidung des Bundesverfassungsgerichts zum Mikrozensus anklingen. Seither steht fest: Das Grundgesetz verträgt sich nicht mit Informationserwartungen, die von einem grundsätzlich unbegrenzten Zugang zu personenbezogenen Daten ausgehen. Wo er hingenommen wird, sind Manipulierbarkeit und Kommunikationsunfähigkeit die Folge. Beides zu verhindern, ist Aufgabe des Datenschutzes. Er steuert die Informationsverarbeitung, um die Steuerbarkeit des einzelnen, seine restlose Programmierung also, zu verhindern. Weder die Intention der Datenschutzgesetze noch die Gesetzesvorschriften lassen sich daher mit einer Interpretation vereinbaren, die im

Datenschutz nur ein Mittel sieht, eine "mißbräuchliche" Verarbeitung personenbezogener Daten zu bekämpfen. Zugegeben: Der Gesetzestext trägt das Seine zu einer solchen Auslegung bei.

Bundes- und Landesdatenschutzgesetze leiten in der Tat ihre Regelung mit der Feststellung ein, der Datenschutz solle dem Mißbrauch bei der Datenverarbeitung entgegenwirken. Anders formulierte noch das erste Hessische Datenschutzgesetz. Seine Eingangsnormen brachten deutlich den Wunsch zum Ausdruck, auf die Informationsverteilung mit Hilfe gezielter Verarbeitungsregeln Einfluß zu nehmen. Hinter dem unterschiedlichen Wortlaut verbirgt sich freilich keine inhaltliche Divergenz. Bundes- und Landesdatenschutzgesetze verfolgen vielmehr genau das vom Hessischen Gesetzgeber schon festgelegte Ziel. Ganz in diesem Sinn untersagt das BDSG jede Verarbeitung personenbezogener Daten, solange es an einer einschlägigen Rechtsgrundlage oder an der Einwilligung des Betroffenen fehlt. Aus dem gleichen Grund enthalten alle Datenschutzgesetze detaillierte Vorschriften zu den einzelnen Verarbeitungsphasen, die den Umfang der Datenverarbeitung ebenso einschränken wie die Verbreitung personenbezogener Angaben. Nichts anderes bezwecken schließlich die in den Gesetzen festgeschriebenen organisatorisch-technischen Verarbeitungsvoraussetzungen. Kurzum, die Datenschutzgesetze sind durchweg darauf bedacht, die Informationsverteilung um einer konsequenten Gefahrenabwehr willen zu regeln. In dem Maße aber, in dem es ihnen gelingt, dieses Ziel zu erreichen, verhindern sie zugleich jede mißbräuchliche, weil gegen die festgelegten Verteilungsgrundsätze verstoßende Verarbeitung.

Die Datenschutzgesetze versuchen, bei allen Unterschieden in den Details, ihre Steuerungsfunktion mit Hilfe von sechs Grundsätzen zu erfüllen:

- Die Verarbeitung personenbezogener Daten muß unter allen Umständen subsidiär sein. Solange es also möglich ist, die jeweils wahrzunehmende Aufgabe anders zu erfüllen, muß von einem Rückgriff auf personenbezogene Angaben abgesehen werden.

- Wo sich die Verarbeitung nicht vermeiden läßt, muß sie immer mit einer klar definierten, jederzeit nachvollziehbaren Aufgabe zusammenhängen und auf das konkret erforderliche Maß beschränkt bleiben. Jede Verarbeitung ist, mit anderen Worten, besonders zu rechtfertigen. Die Legitimation kann aber allein durch die Verknüpfung mit einer bestimmten Aufgabe erbracht werden. Damit ist einerseits die Transparenz, andererseits aber auch die Kontrollierbarkeit der Verarbeitung gesichert. Daraus erklären sich beispielsweise die langen Auseinandersetzungen um das Melderechtsrahmengesetz. Solange wie die Aufgabe der Meldebehörden, genaugenommen, lediglich darin bestand, Sammelstelle der von der öffentlichen Verwaltung benötigten Informationen zu sein, war es inakzeptabel. Den Anforderungen des Datenschutzes entsprach es erst, als der Gesetzgeber den Identitätsnachweis in den Vordergrund stellte und von dort aus die Registrierung rechtfertigte (§ 1). Die eindeutig eingeschränkte Aufgabe hat eine ebenso klar begrenzte Verarbeitung zur Folge. Konsequenterweise knüpft das Bayerische Datenschutzgesetz (Art. 16 ff.) die Zulässigkeit der Verarbeitung ausdrücklich an eine gesetzliche Aufgabenzuweisung. Der Gesetzgeber soll damit gezwungen werden, die Tätigkeit der öffentlichen Verwaltung auch und gerade im Hinblick auf die Verarbeitung personenbezogener Daten zu überdenken. Die geforderte gesetzliche Regelung bietet die Chance zur Korrektur allzu vager Aufgabendefinitionen und verspricht damit mehr Schutz vor oft für Außenstehende kaum wahrnehmbaren Aufgabenmodifikationen, die das Maß und die Intensität der Verarbeitung beträchtlich erhöhen.

- Die strikte Aufgabenorientierung beinhaltet zugleich eine Zweckbindung der Verarbeitung. Personenbezogene Daten, die für bestimmte Aufgaben erhoben und verarbeitet werden, sind kein beliebig nutzbares Informationsmaterial. Sie bleiben vielmehr ein grundsätzlich nur beschränkt verwendbares Informationsinstrument. Die Organisationseinheit ist unter diesen Umständen kein tauglicher Maßstab für den Zugang zu den Daten. Auch wenn also eine Verwaltungs-

einheit für eine Vielzahl ebenso unterschiedlicher wie komplexer Aufgabenbereiche zuständig ist, ändert sich nichts an der Verpflichtung, die vom Datenschutz aufgerichteten Informationsschranken auch und gerade innerhalb ihres eigenen Bereiches zu beachten. An die Stelle eines rein formalen Behördenbegriffs tritt damit eine strikt funktionale Betrachtung. Wiederum bietet das Melderechtsrahmengesetz (§ 18 Abs. 6) ein Beispiel dafür. Der Gesetzgeber spaltet die Kommune bewußt in klar voneinander getrennte Aufgabenbereiche und unterbindet damit gezielt alle Versuche, Daten, über die das Einwohnermelderegister verfügt, als Teil einer jedenfalls intern jederzeit zugänglichen kommunalen Datenbank anzusehen.

- Der Datenschutz kann und will die Übermittlung personenbezogener Daten nicht ausschließen, stellt aber Anforderungen, die eine Einschränkung der Übermittlungsrisiken zum Ziel haben. Dazu zählt zunächst und vor allem eine genaue Überprüfung der jeweils verarbeiteten Angaben auf ihre Übermittlungsfähigkeit. Der Gesetzgeber hat es zwar ausdrücklich und zu Recht abgelehnt, den Datenschutz je nach der Art der verarbeiteten Daten zu variieren oder überhaupt erst vorzuschreiben. Freie Daten gibt es deshalb ebensowenig, wie sich die gesetzlichen Bestimmungen auf Vorkehrungen zur Verarbeitung "sensitiver" Daten beschränken. Entscheidend ist nicht eine wie immer durchgeführte abstrakte Klassifikation der personenbezogenen Angaben, sondern allein der Verarbeitungskontext. Wo aber auf den Kontext sorgfältig geachtet wird, macht sich alsbald die Notwendigkeit weitreichender, ja unter Umständen vollständiger Übermittlungssperren bemerkbar. Ganz in diesem Sinn hat das Bundesverfassungsgericht den Zugriff auf die Drogenberatungsstellen vorhandenen Daten verwehrt. Die therapeutische Funktion der Drogenberatungsstellen verbietet in der Tat jede Proliferation der ihnen überlassenen Angaben, zwingt also zu einer Abschottung gegenüber allen anderen Behörden, so wichtig, ja unverzichtbar die Information aus deren Perspektive erscheinen mag. Das Sozialgesetzbuch geht diesen Weg in

seinem zehnten Buch (§§ 67 ff.) konsequent weiter. Die dort formulierten Übermittlungsschranken räumen endgültig mit der Vorstellung auf, die öffentliche Verwaltung könne und dürfe die in ihrem Bereich vorhandenen Daten grundsätzlich für alle ihr obliegenden Aufgaben verarbeiten. Je breiter vielmehr die Palette staatlicher Aufgaben gerät, desto mehr nehmen die Informationssperren zu. Der Verarbeitungskontext signalisiert die Verwendungsgrenzen.

- Die Zulässigkeit der Übermittlung begründet noch keine Verwendungsfreiheit. Im Gegenteil, die jeweils weitergegebenen Angaben dürfen grundsätzlich nur zu dem Zweck verarbeitet werden, zu dem sie übermittelt worden sind. Konsequenter Datenschutz beinhaltet insofern immer und zugleich ein Zweckentfremdungsverbot. Die Informationsbarrieren entfallen also nicht mit zunehmender Entfernung von der ursprünglichen speichernden Stelle. Der Verarbeitungsprozeß bleibt vielmehr an Orientierungspunkte gebunden, die seine Überschaubarkeit und Kontrollierbarkeit sichern. Die Zweckbindung engt den Verarbeitungsspielraum ein und setzt einer technisch durchaus möglichen Variation der Verarbeitungsziele von vornherein Grenzen.

- Aufgabenbindung und Zweckentfremdungsverbot widersetzen sich jedem Versuch, einen wie auch immer gearteten Schlüssel zu entwickeln, der den Zugriff auf sämtliche der öffentlichen Verwaltung zur Verfügung stehende personenbezogene Daten sichert. Deshalb begnügt sich das Personalausweisgesetz nicht damit, die für die Ausweisfunktion notwendigen Aufgaben abschließend aufzuzählen, sondern beugt zugleich einer Verwendung der Seriennummer für die Erschließung von Dateien vor. Der Personalausweis mag sich technisch vorzüglich als Schlüssel zu den staatlichen Datenbanken eignen, jeder Schritt in diese Richtung ist aber zugleich ein Schritt in die Illegalität. Der Gesetzgeber duldet nur einen Ausweis, der die Chancen der Verarbeitungstechnik eben nicht nutzt und damit eine multifunktionale Verwendung bewußt ausschließt. Das Personalausweisgesetz greift mit seinen Bestimmungen den gemeinsamen Beschluß des Rechts- und des Innen-

ausschusses des Bundestages auf. Dort war bereits auf die mit der Einführung eines allgemeinen Personenkennzeichens verbundenen Gefahren hingewiesen worden. Sie wiederholen sich immer dann, wenn das gleiche Ziel, der Zugang zu grundsätzlich allen über den einzelnen gespeicherten Daten, auf anderem Weg erreicht werden kann. Ein wirksamer Datenschutz ist nur so lange möglich, wie eine Parzellierung der Information bewußt in Kauf genommen und rechtlich abgesichert wird.

4. Mit diesen Grundsätzen sind zugleich die Problemzonen angedeutet. In der Auseinandersetzung mit den sich aus jedem dieser Grundsätze ergebenden Anforderungen werden Widerstände und Schwierigkeiten deutlich und gewinnt der Datenschutz eine konkrete, auf die jeweiligen Teile der öffentlichen Verwaltung bezogene Bedeutung. Nur auf dem Hintergrund der einzelnen Grundsätze lassen sich deshalb auch die Fragestellungen beschreiben und verstehen, die Verlauf und Stand der Diskussion über die Auswirkungen des Datenschutzes auf die polizeiliche Tätigkeit markieren.

4.1 Ganz gleich nun, um welchen Verarbeitungsaspekt es im einzelnen geht, ein Stichwort kehrt ständig wieder: Die "Verrechtlichung" der polizeilichen Informationsverarbeitung. Gemeint ist die Notwendigkeit, die Verarbeitung personenbezogener Daten im polizeilichen Bereich mit Hilfe besonderer, an den spezifischen Aspekten der polizeilichen Tätigkeit orientierter Rechtsvorschriften genau zu regeln. Wer freilich in der "Verrechtlichung" eine schlicht selbstverständliche, für alle Teile der öffentlichen Verwaltung gleichermaßen geltende und deshalb keiner weiteren Diskussion bedürftige Konsequenz des Datenschutzes erblickt, sieht sich alsbald heftigem Widerspruch ausgesetzt. Für die einen ist die "Verrechtlichung" in Wirklichkeit nur ein unverhohlener Versuch, eine rechtlich bedenkliche polizeiliche Praxis nachträglich zu legalisieren. Die anderen halten sie nicht nur deshalb für inakzeptabel, weil sie, wie man meint, einen, wenn auch kaschierten Vorwurf der Illegalität an die Adresse der Polizei beinhaltet, sondern auch und vor allem, weil sie in ihr das trojanische Pferd einer schier unerträglichen Bürokratisierung der polizeilichen Arbeit sehen.

Zunächst: Der Datenschutz schafft für die Polizei wie für die gesamte übrige öffentliche Verwaltung eine völlig neue Ausgangssituation. Ganz gleich wie die Verarbeitung personenbezogener Daten bisher erfolgte, sie muß fortan den sich aus dem Datenschutz ergebenden Anforderungen angepaßt werden. Weder das BDSG noch irgend eines der Landesdatenschutzgesetze läßt auch nur den geringsten Zweifel aufkommen: Die Verarbeitung bleibt solange unzulässig, wie es an einwandfreien, den konkreten Verarbeitungsprozeß rechtfertigenden rechtlichen Grundlagen fehlt. Eine Alternative zur "Verrechtlichung" gibt es unter diesen Umständen nicht. Bislang benutzte Verarbeitungsformen müssen daher nach den neuen, am Datenschutz ausgerichteten Verarbeitungsmaßstäben beurteilt werden. Von einer nachträglichen Legalisierung kann, so gesehen, keine Rede sein. Ebensowenig aber von einem Vorwurf. Der Gesetzgeber ahndet nicht bislang Praktiziertes, er stellt lediglich die Weichen für alle zukünftige Verarbeitung personenbezogener Daten. Vorwürfe lassen sich infolgedessen nur dort erheben, wo den veränderten, dem Datenschutz Rechnung tragenden Bedingungen nicht entsprochen wird. Auch der Bürokratisierungseinwand überzeugt nicht. Zur Debatte steht keineswegs eine zweifelhafte oder gar überflüssige Normenproduktion, sondern einzig und allein jenes Mindestmaß an Vorschriften, dessen es unbedingt bedarf, um den Verarbeitungsspielraum, nicht zuletzt im Interesse der Polizeibehörden, klar festzulegen, die für ihre Tätigkeit also notwendige Rechtsgrundlage zu schaffen.

Der kritische Punkt liegt in Wirklichkeit anderswo. Der Forderung nach einer "Verrechtlichung" der polizeilichen Informationsverarbeitung läßt sich, jedenfalls nicht ohne weiteres, entnehmen, wie sie realisiert werden soll, inwieweit mithin untergesetzliche Vorschriften schon ausreichen oder eine erschöpfende gesetzliche Regelung vonnöten ist. Hier herrscht in der Tat nach wie vor Unklarheit. Der bisherige Diskussionsverlauf, aber auch vor allem die mit dem Datenschutz gewonnenen Erfahrungen geben immerhin so viel zu erkennen: Die "Verrechtlichung" muß notwendigerweise zu einem wesentlichen Teil "Vergesetzlichung" sein. Schon des-

halb, weil die Verarbeitung personenbezogener Daten durch die öffentliche Verwaltung, besonders im Rahmen der polizeilichen Tätigkeit, Eingriffe in die Grundrechte der Betroffenen mit sich bringt. Ganz gleich deshalb, um welche Verarbeitungsphase es im einzelnen geht, die Verarbeitung bedarf stets der gesetzlichen Grundlage. Niemand anders als der Gesetzgeber vermag infolgedessen den Polizeibehörden die Verarbeitungsbefugnis zu erteilen.

Dennoch: Eine gesetzliche Regelung kann, und auch dies zeigt die Erfahrung, letztlich nicht mehr als Grunddaten polizeilicher Informationsverarbeitung normieren. Es ist nicht nur müßig, sondern gefährlich, vom Gesetzgeber zu erwarten, etwa auf alle Details jeder einzelnen Datei einzugehen. Gesetzlich festzulegen sind unter allen Umständen das Verarbeitungsziel, der Verarbeitungsumfang und die Verknüpfungsmöglichkeiten. Alle weiteren Aspekte lassen sich dagegen nur mit Hilfe von Verwaltungsvorschriften regeln. Erst das Zusammenspiel gesetzlicher und administrativer Vorkehrungen vermag einerseits den vom Datenschutz geforderten festen Verarbeitungsrahmen zu schaffen und andererseits eine Verarbeitungsregelung zu garantieren, in die polizeiliche Erfahrungen und die damit zusammenhängenden Informationsanforderungen, in Kenntnis der Konsequenzen des Datenschutzes, konstant eingehen. Die Balance zwischen dem notwendigen Eingriff des Gesetzgebers und seiner ebenso erforderlichen Zurückhaltung ist freilich schwer zu halten. Wo sie mißlingt, werden Datenschutz und polizeiliche Arbeit gleichermaßen diskreditiert. Ein Mehr an gesetzlicher Regelung, als der Datenschutz wirklich braucht, erschwert in der Tat die polizeiliche Arbeit in einer nicht mehr zu rechtfertigenden Weise. Umgekehrt gefährdet eine Regelung, die auf gesetzlich abgesicherte Anforderungen zugunsten von Verwaltungsvorschriften verzichtet, nachhaltig den Datenschutz. Mißt man nun daran den gegenwärtigen Zustand, dann läßt er sich als eine ebenso vorsichtige wie langsame Annäherung an die Balance zwischen gesetzlichen und Verwaltungsvorschriften beschreiben. Die Richtlinien für die kriminalpolizeilichen Sammlungen oder für die beim Bundeskriminalamt geführten Dateien sind ebenso untrügliche Signale dafür wie die an

die Adresse der Sicherheitsbehörden im Melderechtsrahmengesetz und im zehnten Buch des Sozialgesetzbuchs formulierten Bestimmungen. Anders ausgedrückt: Der Weg ist eingeschlagen, das Ziel noch nicht erreicht.

4.2 Präziser: Konsequenter Datenschutz verlangt, soweit es um eine gesetzliche Regelung geht, auf jeden Fall ein Doppeltes. Der Gesetzgeber muß über die bloße Aufgabenbeschreibung hinaus die Verarbeitungsbefugnis festlegen. An einer gesetzlichen Aufgabendefinition fehlt es nun ohne Zweifel nicht. Beide, gleichsam klassische Funktionen polizeilicher Tätigkeit werden vom Gesetzgeber ausdrücklich angesprochen, die präventive in den Polizeigesetzen der Länder, die repressive in der Strafprozeßordnung. Sicher, ein Nachteil fällt sofort auf, die gesetzliche Regelung gründet sich auf Generalklauseln. Die Qualität einer Aufgabenbeschreibung mißt sich aber unter Datenschutzgesichtspunkten an der Präzision der Angaben zu der jeweiligen Funktion. Nur dann kann es wirklich gelingen, den Verarbeitungsumfang und das Verarbeitungsziel verläßlich abzuschätzen. Jeder Versuch, dies zu erreichen, droht dort zu scheitern, wo das Gesetz nicht mehr enthält, als etwa den Hinweis auf die Verpflichtung, Gefahren für die öffentliche Sicherheit und Ordnung abzuwehren. So nahe jedoch die Kritik an den Generalklauseln liegt, so wenig hilft sie letztlich weiter. Nicht von ungefähr finden sich Generalklauseln nicht nur in den geltenden gesetzlichen Regelungen, sondern kehren auch in allen Vorschlägen zur Reform des Polizeirechts wieder. Man kann gewiß darüber streiten, ob es noch angebracht ist, Sicherheit und Ordnung zu erwähnen. Doch selbst wenn man sich mit der öffentlichen Sicherheit begnügt, ändert sich an der für den Datenschutz allein relevanten Perspektive nichts. Nach wie vor gibt eine Generalklausel den Ton an. Nur zu verständlich. Die Gefahrenabwehr kann eben immer nur mit Hilfe einer Generalklausel umschrieben werden. Punktuelle Konkretisierungen sind bestenfalls Interpretationswegweiser; sie eignen sich also nicht dazu, die Generalklausel zu ersetzen, wenn der polizeilichen Tätigkeit nicht ein jederzeit überholbares und damit letztlich zufälliges Gefahrenbild zugrundegelegt werden soll.

Um so sorgfältiger gilt es freilich den Anwendungsbereich der Generalklausel zu betrachten. Schon im Hinblick auf die mögliche Ausgrenzung einzelner Aufgaben, die dann, für sich betrachtet, präziser gefaßt werden könnten. Unter diesem Aspekt verdienen gerade die Bemühungen, die Ordnungsverwaltung von allen übrigen polizeilichen Aufgaben zu trennen, besondere Beachtung. Bei der Ordnungsverwaltung lassen sich in der Tat die jeweils in Betracht kommenden Funktionen genau festlegen und so zugleich die Verarbeitung personenbezogener Daten eingrenzen. Einmal mehr gilt es an das Melderecht zu erinnern. Für den Datenschutz war und ist die Absonderung der Meldebehörden, verbunden mit der gesetzlichen Festlegung der ihnen zugewiesenen, spezifischen Aufgaben eine essentielle Voraussetzung einer begrenzten, überschaubaren und kontrollierbaren Verarbeitung. Ähnlich kann, ja muß bei allen anderen Teilen der Ordnungsverwaltung verfahren werden. Wiederum kommt es also darauf an, den Verarbeitungsprozeß mit der einzelnen zur Debatte stehenden Aufgabe zu verbinden, ein strikt aufgabenorientiertes Informationssystem also zu konstruieren, dessen Verwendungsmöglichkeiten feststehen müssen und das, wie bei den Meldebehörden, anderen Behörden nur unter bestimmten gesetzlich festgelegten Voraussetzungen zugänglich sein darf. Der Datenschutz widersetzt sich insofern allen Versuchen einer wohlfahrtsstaatlichen Definition der Polizeiaufgaben. Die Risiken der Informationsverarbeitung lassen sich nur verringern, wenn jede Chance wahrgenommen wird, zwischen den einzelnen Aufgaben zu differenzieren und gezielt auf sie zu reagieren.

Selbst dort aber, wo, wie im eigentlichen Polizeibereich, der Gesetzgeber auf Generalklauseln angewiesen ist, bietet die Aufgabenbeschreibung durchaus Ansatzpunkte, die es erlauben, den Rahmen der Informationsverarbeitung abzustecken. So mag kein Zweifel an der Verpflichtung der Polizei bestehen, Gefahren für die öffentliche Sicherheit abzuwehren, ebensowenig ist aber zu bestreiten, daß polizeiliche Gefahrenabwehr eine konkrete Gefahr voraussetzt. Genau diese Bedingung bekommt dann eine ganz besondere Bedeutung, wenn sich die Polizei im Rahmen ihrer präventiven Aufgabe dem

Staatsschutz zuwendet. Der Gesetzgeber hat hier alles getan, um Fehlinterpretationen zu vermeiden. Die generelle Beobachtung verfassungsfeindlicher Bestrebungen ist ausschließlich Sache des Verfassungsschutzes (§ 3 VerfSchutzG), mithin einer von der Polizei deutlich getrennten Behörde, die bewußt nicht mit polizeilichen Befugnissen ausgestattet wurde. Konsequenterweise müssen deshalb auch Polizei und Verfassungsschutz mit eigenen, klar voneinander abgesonderten Informationssystemen arbeiten.

Diese vom Gesetzgeber deutlich gezogene und im Informationsbereich nachhaltig bestätigte Grenze riskiert dann überschritten zu werden, wenn die Staatsschutzabteilungen der Polizei Daten im Vorfeld von Straftaten verarbeiten. Allzu leicht geht die durch die Aufgabe der Polizei gebotene Verbindung zwischen der Informationsverarbeitung und einer konkreten Gefahr verloren. Soweit etwa die Polizei ohne einen spezifischen Anlaß Kandidaturen für eine bestimmte politische Gruppierung, Parteimitgliedschaften u.ä. registriert, verarbeitet sie Angaben, die, wenn überhaupt, in dem jeweils zulässigen Umfang einzig und allein durch den Verfassungsschutz aufgenommen und verwertet werden dürfen. Der Gesetzgeber duldet keine Verdoppelung der Verarbeitung, er statuiert eine ausschließliche Kompetenz, die unter allen Umständen gewahrt werden muß. Die Staatsschutzabteilungen sind kein zweiter Verfassungsschutz. Die konkrete Gefahr ist deshalb bei aller Verpflichtung zur präventiven Tätigkeit eine verbindliche, strikt zu beachtende Schranke der Informationsverarbeitung. Dementsprechend stellen Übermittlungen der Polizei an den Verfassungsschutz und umgekehrt Übermittlungen des Verfassungsschutzes an die Polizei keine behördeninternen Übermittlungen dar, sondern die Weitergabe personenbezogener Daten an eine andere Behörde, die in jedem Einzelfall an den Zulässigkeitsvoraussetzungen der Datenschutzgesetze und der bereichsspezifischen Regelungen zu messen sind.

4.3 Freilich: Je deutlicher sich zeigt, wie wenig bei der Aufgabenbeschreibung auf Generalklauseln verzichtet werden kann, desto mehr verschiebt sich unter Datenschutzgesichtspunkten der Regelungsschwerpunkt auf die Befugnisnormen. Ihnen kommt dann ein besonderes Gewicht zu, wenn, wie etwa bei den Polizeibehörden, Aufgaben nur in einer sehr allgemein gehaltenen Form angegeben werden können. Die Befugnisnormen kompensieren, so gesehen, die mangelnde Präzision der Aufgabenbeschreibung. In dem Maße, in dem es mit Hilfe der Befugnisnormen gelingt, die Verarbeitungsvoraussetzungen möglichst genau festzulegen, werden auch die mit den bei der Aufgabenbeschreibung benutzten Generalklauseln verbundenen Risiken ausgeglichen. Wohl keine andere Frage ist gegenwärtig allerdings so kontrovers wie die nach den Befugnisnormen. Gewiß, die Akzente werden in einer zuweilen sehr unterschiedlichen Weise gesetzt. Während für die einen der präventive Bereich gleichsam das Musterbeispiel für fehlende Befugnisnormen ist, erscheint den anderen die Situation im repressiven Bereich mindestens ebenso bedenklich, wenn nicht noch regelungsbedürftiger.

Ganz gleich aber wie man sich dazu stellt, eines läßt sich der Diskussion inzwischen mit Sicherheit entnehmen: Weder die Grundnormen der Polizeigesetze noch Bestimmungen wie die §§ 161 und 163 StPO genügen letztlich den Anforderungen einer Befugnisnorm. Man mag ihnen, wie sich vor allem am Beispiel der StPO zeigt, im Einzelfall den einen oder anderen Anhaltspunkt für konkrete Befugnisse bei der Informationsverarbeitung entnehmen können. Gewonnen ist aber damit nicht viel mehr als eine kurzfristige Überbrückung der durch den Mangel an einer klaren, die einzelnen Verarbeitungsaspekte aufgreifenden gesetzlichen Befugnisregelung verursachten Schwierigkeiten.

Die Datenschutzgesetze bieten keinen Ausweg. Sie enthalten zwar durchweg Vorschriften, die ausdrücklich auf die einzelnen Verarbeitungsphasen eingehen und gezielte Anforderungen formulieren. Schaut man aber genau hin, dann stellt man alsbald

fest, daß der Gesetzgeber nicht mehr tut, als bestimmte, generelle Verarbeitungsgrundsätze festzulegen. Konkret: Sowohl das BDSG als auch die Landesdatenschutzgesetze knüpfen beispielsweise die Zulässigkeit der Speicherung personenbezogener Daten an die Erforderlichkeit der jeweils zur Debatte stehenden Angaben für die im einzelnen wahrzunehmende Aufgabe. Mehr als der für die Verarbeitung rechtlich verbindliche Rahmen ist damit nicht angegeben. Was "Erforderlichkeit", mit anderen Worten, genau bedeutet, kann nicht den Datenschutzgesetzen, sondern allein einer sich direkt auf die polizeiliche Tätigkeit beziehenden Befugnisnorm entnommen werden.

Kurzum, der Gesetzgeber hat keine Wahl. Er muß die Konsequenzen aus der Prämisse ziehen, die er selbst gesetzt hat. Die Entscheidung für den Datenschutz ist zwangsläufig zugleich eine Entscheidung für die Informationsverarbeitung regelnde Befugnisnormen. Nur so lassen sich weitere, den Datenschutz gefährdende und die Polizeibehörden verunsichernde Kontroversen vermeiden. Und nur auf diesem Weg kann eine Regelung gefunden werden, die auch und gerade bei der Informationsverarbeitung deutlich zwischen präventiven und repressiven Funktionen mit all den damit für die Verarbeitung verbundenen Konsequenzen unterscheidet, also beim Verarbeitungsverlauf die gleichsam originäre polizeiliche Tätigkeit im Rahmen der Gefahrenabwehr von der Aktivität als Hilfsorgan der Staatsanwaltschaft abgrenzt. Wer dabei Regelungsadressat ist, die Polizei oder die Staatsanwaltschaft, spielt für die Notwendigkeit, die Verarbeitungsbedingungen festzulegen, weiter keine Rolle. Präzise Verarbeitungsregeln bleiben in jedem Fall notwendig.
Sicher, gesetzliche Regelungen, die, wie die Datenschutzgesetze, ebenso neue wie weitreichende Verhaltensanforderungen formulieren, zwingen dazu, eine Übergangszeit in Kauf zu nehmen, um die Anwendungsprobleme genau erkennen und auf sie gezielt reagieren zu können. Doch die Schonzeit ist abgelaufen. Dies um so mehr als Regelungen vorliegen, die sich durchaus als Grundlage für die notwendigen Befugnisnormen anbieten. Die Richtlinien für die kriminalpolizeilichen Sammlungen sind das wohl wichtigste Beispiel dafür. Sie zeigen, wie in Kenntnis sowohl der Anforderungen des Datenschutzes als auch der Besonderheiten polizeilicher Tätigkeit über-

zeugende und praktikable Lösungen gefunden werden können. Mit Hilfe der KpS ist es etwa gelungen, den Konflikt um die Auskunftsverpflichtung gegenüber dem Betroffenen aus der diskussionsvernebelten Abstraktion des BDSG herauszunehmen und weitgehend zu entschärfen. Die polizeiliche Praxis zeigt, wie sehr die vom Datenschutz im Interesse des Betroffenen geforderte Transparenz der Verarbeitung auch im polizeilichen Bereich gesichert werden kann. Nach wie vor gibt es freilich eine Reihe offener Fragen. Auch dafür ein Beispiel. Das Bundeszentralregistergesetz knüpft an die Verpflichtung, Eintragungen über Verurteilungen zu tilgen (§§ 43 ff.), ein Verwertungsverbot (§ 49), eine unter Datenschutzgesichtspunkten überaus wichtige Konsequenz. Gerade wenn, wie von den Datenschutzgesetzen gefordert, Kontext und Zweck den Verlauf und die Bedingungen der Verarbeitung bestimmen, zählt eine zeitliche Befristung der Verwendung personenbezogener Daten zu den ebenso selbstverständlichen wie elementaren Voraussetzungen des Datenschutzes. Spätestens an den Löschungsbestimmungen des BDSG erweist sich: Konsequenter Datenschutz verlangt ein kontrolliertes Vergessen. Nicht die zeitlose Information, sondern die in Kenntnis der Verarbeitungsziele und ihrer konkreten Bedeutung zeitlich begrenzte Verarbeitung ist deshalb der Grundsatz, von dem jede speichernde Stelle inner- und außerhalb des öffentlichen Bereichs ausgehen muß. So gesehen beinhaltet § 49 BZRG eine den Datenschutzanforderungen voll entsprechende Zielvorgabe. Die Erfahrung zeigt freilich: Das Verwertungsverbot wirkt nur partiell. Für die Polizeibehörden jedenfalls gilt: Sie verarbeiten Informationen über Straftaten nach anderen als den im BZRG festgehaltenen Grundsätzen. Man kann nun in der Tat lange darüber streiten, ob die in § 49 BZRG verwendete Formulierung von der "im Rechtsverkehr" untersagten Verwertung, etwa die Weitergabe von Informationen über getilgte Verurteilungen und die damit verbundenen Straftaten innerhalb der Polizei sowie an andere Behörden ausschließt oder nicht. Fest steht in jedem Fall soviel: Jede restriktive Interpretation untergräbt das Ziel des BZRG, die Resozialisierung, und begünstigt die Errichtung von ihm gerade nicht gewollter Parallelregister. Aus dem "kontrollierten Vergessen" kann so leicht eine "manipulierte Vergeßlichkeit" werden.

Strafverhütung und Strafverfolgung mögen im Hinblick auf die polizeiliche Tätigkeit für andere und längere Fristen sprechen, als sie das BZRG vorsieht. Die Konsequenz kann aber dann nur sein, die Gründe offenzulegen und das BZRG entsprechend zu korrigieren. Die KpS versuchen, der Kritik an der bisherigen Verarbeitungspraxis Rechnung zu tragen. Sie sehen Übermittlungsschranken vor, die sich ausdrücklich an § 49 BZRG orientieren. Bedenken sind dennoch angebracht. Schon deshalb, weil unklar bleibt, wie es um die Geltung der anderen im BZRG enthaltenen Schutzvorschriften steht. Zudem konnte gerade dieser Teil der KpS bislang nicht realisiert werden. Der Ausgang des Verfahrens ist eben der Polizei in sehr vielen Fällen unbekannt. Sie ist infolgedessen gar nicht in der Lage, sich anhand der eigenen Unterlagen Gewißheit über die Fristen zu verschaffen. Ferner fehlt es noch immer an einem praktikablen Weg, der es ermöglichen könnte, die BZRG-Fristen bei allen Auskünften zu beachten. Und schließlich: Dem Datenschutz entspricht allein eine unmißverständliche Trennung zwischen polizeiinternem Gebrauch der Information und einer Übermittlung an Dritte. An einer solchen klaren Grenzziehung mangelt es aber.

4.4 Bleibt eine letzte, nicht minder signifikante Problemzone: Die Auswirkungen der durch den Datenschutz bewirkten Abschottung der Verarbeitung personenbezogener Daten. Sie verändert ohne Zweifel die Zugriffsmöglichkeiten der Polizei. Der Gesetzgeber hat allerdings den Konflikt durchaus gesehen. Das zehnte Buch des Sozialgesetzbuches, um nur das wahrscheinlich wichtigste Beispiel zu nennen, schließt eben nicht jeden Zugang von vornherein aus, sondern akzeptiert Ausnahmen. Sie sind sorgfältig abgestuft, und zwar sowohl durch die Restriktion der übermittelbaren Angaben als auch durch unterschiedliche Übermittlungsbedingungen (§§ 68, 72, 73).

Der Kompromiß verdeutlicht zugleich: Für alle Behörden, also auch für die Polizei, gibt es nur den einen im Gesetz festgelegten Zugang zu den Sozialdaten. Spätestens an den §§ 67 ff. SGB-X zeigt sich deshalb, wie wenig sich die traditionellen Vorstellungen über die Amtshilfe in ein

Regelungssystem der Informationsverarbeitung einfügen lassen, das sich an der Zweckbindung orientiert und sich deshalb für eine sorgfältige Abschottung ausspricht. Konsequenterweise ist daher auch in anderen Bereichen gefordert worden, die herkömmlichen Grundsätze der Amtshilfe durch eine die Anforderungen des Datenschutzes berücksichtigende Informationshilfe zu ersetzen.

Wie weit nun die Folgen der gesetzlichen Zugangsregelung reichen, erweist sich dann etwa, wenn Sozialbehörden Informationen an Gewerbeämter übermitteln, für die sich auch die Polizei interessiert. Die Daten haben zwar den Sozialbereich verlassen. Sie sind aber deshalb nicht freigegeben. Die Übermittlung ist vielmehr im Hinblick auf die Informationserwartungen einer bestimmten Behörde erfolgt. Die Zulässigkeit der Weitergabe ist also in Kenntnis dieser Erwartungen geprüft und bejaht worden. Daraus folgt freilich zugleich die Verpflichtung, die Angaben anderen Behörden nicht zu überlassen. Entscheidend ist mit anderen Worten nicht, ob der Informationswunsch durch die je spezifische Aufgabe gedeckt wird, den Ausschlag gibt vielmehr allein der Informationsweg. Das Sozialgesetzbuch versperrt den indirekten Zugang und verlangt eine direkte Anfrage bei den Sozialbehörden. Dort muß die Relevanz der Daten für die konkrete Aufgabe geltendgemacht werden und dort sind auch die gesetzlich vorgeschriebenen Übermittlungsvoraussetzungen zu prüfen.

Die Verwirklichungschancen einer strikt funktional orientierten, auf Abschottung bedachten Verarbeitungsregelung schwinden freilich, sobald sich Direktanschlüsse durchzusetzen beginnen. Die klare, zweckgebundene Zuordnung des Datenbestandes weicht einer eindeutig multifunktionalen Verwendung. Darauf gründen sich die Vorbehalte gegen die von den Polizeibehörden angestrebten und partiell realisierten on-line-Verbindungen zu den Dateien der Kraftfahrzeugzulassungsstellen oder der Meldebehörden. Sicher, der Direktanschluß stößt, jedenfalls teilweise, auch auf Einwände, die sich auf das geltende Recht stützen. Die Straßenverkehrszulassungsordnung (§ 26 Abs. 5) läßt nun einmal nur einen auf den

Einzelfall begrenzten Zugriff zu, eine Einschränkung, die mit dem Direktanschluß jeden Sinn verlieren würde. Weit mehr fällt jedoch letztlich die tiefgreifende strukturelle Veränderung der Informationsverarbeitung ins Gewicht. Sie stellt genau die Grundsätze in Frage, die, wie etwa eine deutliche funktionale Trennung, den Kern eines wirksamen Datenschutzes ausmachen. Direktanschlüsse sind trotzdem nicht ausgeschlossen. Gerade am Beispiel der Kraftfahrzeugzulassungsstellen läßt sich demonstrieren, daß es durchaus überzeugende Gründe dafür geben kann. On-line-Verbindungen müssen allerdings die Ausnahme bleiben und bedürfen stets einer besonderen Rechtfertigung. Ihre Zulassung ist zudem von spezifischen, gesetzlich abzusichernden Vorkehrungen abhängig zu machen, die eine vergleichbare Einschränkung und Kontrolle wie bei der Einzelfallübermittlung sicherstellen. Ganz mit Recht zählt deshalb die on-line-Regelung zu den wohl wichtigsten Aspekten einer Novellierung der Datenschutzgesetze.

5. Kurzum, die Aufgaben sind keineswegs gering und alles andere als einfach. Sie lassen sich aber nicht verschieben und erst recht nicht verdrängen. Der Datenschutz signalisiert eben nicht nur eine von vielen rechtlichen Anforderungen. Die Legalität administrativen Handelns mißt sich vielmehr in einer rechtsstaatlichen Demokratie auch und vor allem an der Informationsverarbeitung. Die Folge sind unstreitig komplexe Regelungen. Die Komplexität gehört jedoch zu den Kosten des Rechtsstaates. Ihre Entrichtung sichert nicht nur die Legalität administrativer Tätigkeit, sie ist zugleich ein nicht zu unterschätzender Legitimationsgewinn für die öffentliche Verwaltung.

Technisch-wissenschaftliche Datenverarbeitung und Forschung im BKA

(Einführungsreferat zur Gruppendiskussion)

Ernst Bunge

Die materielle Spur, der gegenständliche Tatortbefund und seine Auswertung gewinnen in jüngerer Zeit mehr und mehr an Bedeutung. Zunehmende Einsichten in die Fragwürdigkeit von subjektiven Zeugenaussagen und Geständnissen fördern diese Entwicklung ebenso wie die Liberalisierung des Strafprozesses, dessen Ausgestaltung sich an der Vorstellung von unantastbaren Grundrechten des Individuums, auch des fehlsamen und kriminellen, zu orientieren bemüht. Mit dieser wachsenden Prävalenz des Sachbeweises korrespondieren Techniken, wie sie im Kriminaltechnischen Institut des Bundeskriminalamtes angewandt und weiterentwickelt werden. Die Elektronik bietet hier entscheidende Hilfen. Bereits heute bilden Prozeßrechner die notwendige Ergänzung moderner Untersuchungsmethoden, bei denen - in Erweiterung des herkömmlichen Instrumentariums - etwa das Rasterelektronenmikroskop, das Massenspektrometer und das Infrarot-Fourier-Spektrometer eingesetzt werden. Die mit solchen Großgeräten nunmehr der Verbrechensaufklärung dienstbar gemachten neuen Techniken führen bei weitgehender Reduzierung der für die Untersuchungen benötigten Einsatzmengen zu einem Maximum an analytischer Information. Die rationelle Erfassung und Auswertung der dabei in Sekundenschnelle anfallenden Daten können nur mit Hilfe der EDV gewährleistet werden. Elektronische Prozeßrechner ermöglichen die Datenerfassung im Echtzeitbetrieb, die Datenreduktion und den zuverlässigen Vergleich mit bereits vorhandenen Datenbeständen. Sie ersparen im kriminaltechnischen Labor z.B. dem Chemiker die langwierige Auswertung von Meßdaten und bereiten die Ergebnisse seiner Untersuchungen zu übersichtlichen Protokollen auf.
Diese neuen Techniken sind zunächst in der Industrie und in den Hochschulinstituten entwickelt und eingeführt worden, ehe sie für Zwecke der Kriminaltechnik eingesetzt wurden. Hier erweitern sie den Aktionsradius des kriminaltechnischen Gutachters und leisten einen wesentlichen Beitrag zur Steigerung der Effizienz des Ermittlungsverfahrens. Dabei liegt die Bedeutung ebenso in der zweifelsfreien Überführung des Täters wie im sicheren Ausschluß Unschuldiger aus dem Kreis der Verdächtigen.

Um neue Techniken und Verfahrensweisen auf ihre Möglichkeiten für eine Intensivierung der Verbrechensaufklärung zu untersuchen und gegebenenfalls mit dieser Zielrichtung spezifisch weiterzuentwickeln, hat das Bundeskriminalamt im Rahmen seines Kriminalistischen Instituts eine technisch-naturwissenschaftliche Forschungseinheit "Technische Forschung KI 2" aufgebaut. Aufgabe dieser Einheit ist es, im Zusammenwirken mit den kriminalpolizeilichen Fachabteilungen des BKA und mit den Polizeien der Bundesländer den Bedarf an neuen technischen Verfahren zu ermitteln, daraus die Problemstellungen für Forschungs- und Entwicklungsvorhaben zu erarbeiten und entsprechende Schwerpunktprogramme zu realisieren.

Ein elektronisches Entwicklungslabor sowie ein Prozeßrechenzentrum für wissenschaftlich-technische Datenverarbeitung stehen einem Team von 36 Wissenschaftlern und Ingenieuren zur Verfügung, die - unter dem Oberbegriff "Angewandte Mustererkennung" - neue Methoden der rechnergestützten Verarbeitung von Meßdaten, Texten, Bildern und Stimmen für die kriminalpolizeiliche Praxis erarbeiten. Das wissenschaftlich-technische Rechenzentrum, dessen Aufbau im Zusammenhang mit einigen Forschungsprojekten wirkungsvoll vom Bundesminister für Forschung und Technologie unterstützt wurde, stellt mit seinen fünf großen Prozeßrechnersystemen und mit seinen Zusatzgeräten zur Digitalisierung und Wiedergabe von Daten, Bildern, Signalen sowie mit seinen Programmsystemen international die größte Anlage dieser Art im Polizeibereich dar.

Ein anschauliches Beispiel für Aufgabenstellung und Arbeitsweise ist das Forschungsprojekt "Forensische Tonbandauswertung/Stimmenvergleich". Es geht dabei um die rechnergestützte Auswertung von Tonbandaufnahmen, wie sie z.B. in Fällen von erpresserischem Menschenraub, bei Geiselnahmen oder bei Drohanrufen sich ergeben. Solche Tonbänder mit den Stimmen der Täter bzw. Tatverdächtigen enthalten Informationen u.a. zu folgenden Fragen:

- Wer ist der Sprecher?
- Welche Schlüsse lassen sich aus Hintergrundgeräuschen ziehen?
- Handelt es sich um ein Orts- oder ein Ferngespräch?

- Welche Ermittlungsansätze können aus dem Dialekt des Sprechers und seinen Sprachbesonderheiten abgeleitet werden?

- Wenn etwa die Täter selbst ein Tonband mit ihren Forderungen usw. übermittelten: Mit welchem Tonbandgerät wurden die Aufnahmen gefertigt? Und: Wurden die Tonbänder (z.B. mit der Stimme eines Entführten) manipuliert?

Die Beantwortung dieser Fragen wird erschwert durch Besonderheiten der jeweiligen Gesprächssituation, bei Telefongesprächen durch Verzerrungen des Sprachsignals, durch den Einfluß von Stress und Emotionen auf Anrufer und Angerufenen, durch Stimmen-Verstellung usw. Im Rahmen des Forschungsprojektes des Bundeskriminalamtes wurde nun ein Prozeßrechnersystem aufgebaut, mit dessen Hilfe Sprache digitalisiert, segmentiert, analysiert und auf vielfältige Wiese vermessen werden kann. Zugleich kann das System zur akustischen Verbesserung von Sprachaufnahmen eingesetzt werden, deren Verständlichkeit durch überlagerte Störungen beeinträchtigt ist. Es geschieht dies durch den Einsatz komplexer digitaler Filterverfahren.

Mit Hilfe der Methoden, die im Rahmen dieses Forschungsprojektes interdisziplinär von Nachrichtentechnikern, Phonetikern und Informatikern erarbeitet wurden, konnten bereits in vielen Fällen von Schwerkriminalität den mit der Aufklärung beauftragten Kriminalbeamten nützliche Ermittlungshinweise gegeben werden. Gerichte erkannten die Eignung der Verfahrensweise für die Beweisführung an. Die Forschungsarbeiten werden weitergeführt, um die Schwankungsbereiche der Sprechermerkmale systematisch zu untersuchen. Zu diesem Zweck muß mit erheblichem Arbeitsaufwand eine große Anzahl von "Sprach-Proben" gesammelt und ausgewertet werden, um zu einer statistischen Absicherung von Einzelhypothesen zu gelangen. Die Weiterentwicklung des Projektes erfolgt beim BKA in Verbindung mit Forschungseinrichtungen des amerikanischen Federal Bureau of Investigation (FBI) und der britischen Polizei.

Ebenso wie die Sprache enthält auch die Handschrift Informationen über ihren Urheber. Gelingt es, diese Informationen zu entschlüsseln, können sie im Falle eines Verbrechens zu dessen Aufklärung sowie auch zur

Verhinderung der Fortsetzung oder Wiederholung der Straftat beitragen. Bei handschriftlichen Vorlagen, die in Verbindung mit einem Verbrechen eine Rolle spielen, ist u.a. von Bedeutung, wer den Text geschrieben hat, ob mehrere Schriftstücke von der gleichen Person geschrieben wurden usw. Um die Beantwortung solcher Fragen nach objektiv meßbaren Kriterien vornehmen und um zugleich das Massenproblem der vielen tausend Untersuchungsaufträge bewältigen zu können, die dem BKA zugeleitet werden, wurde mit Förderung des Bundesministers für Forschung und Technologie ein entsprechendes Forschungsprojekt durchgeführt. Zur Untersuchung einer Schriftprobe wird diese von einer Fernsehkamera abgetastet, und es werden die Helligkeitswerte digitalisiert und in Form von Zahlenwerten in den Rechner eingegeben. Diese Zahlen - pro Schrift ergeben sich etwa 250 000 Werte - werden nach einem hierfür entwickelten Programm vom Rechner analysiert, der schreiberspezifische Merkmale ermittelt. Für jeden in Frage kommenden Schreiber werden diese Merkmale gespeichert. Bei einer neuen Schriftprobe dienen diese Merkmale dazu, den Rechner die Frage beantworten zu lassen, ob ihm bereits Schriften (und damit Schreiber) "bekannt" sind, die schreibspezifische Merkmale mit größtmöglicher Ähnlichkeit aufweisen. Unter den Laborbedingungen des Forschungsprojektes konnten erstaunlich hohe "Erkennungssicherheiten" erzielt werden.

In der inzwischen eingeleiteten Entwicklungsphase des Projektes werden die bisher erzielten Ergebnisse als Grundlage für ein Handschriftenanalyse- und -recherchiersystem benutzt, das dem kriminalpolizeilichen Handschriftensachverständigen die Vorauswahl in größeren Vergleichsbeständen erleichtern soll. Mit anderen Worten: Nach Eingang einer Schriftprobe, die daraufhin zu untersuchen ist, ob vom Urheber bereits andere Schriften vorliegen, soll der Rechner dem Sachverständigen bereits eine Auswahl solcher Schriften nachweisen, die mit der neuen Probe eine größtmögliche Ähnlichkeit haben. Damit würde der derzeit noch sehr zeitaufwendige Suchvorgang erheblich beschleunigt. Zugleich soll das System die Möglichkeit der objektiven Vermessung von Tat- und Vergleichsschrift eröffnen.

Ebenfalls den Bereich der Handschriftenuntersuchung betrifft ein weiteres Forschungsprojekt, bei dem Grundlagenuntersuchungen zur Schrifterzeugung durchgeführt werden. Zu diesem Zweck werden die im Verlauf des Schreibvorganges auftretenden Erscheinungen wie Schreibdruck, -geschwindigkeit und -beschleunigung

gemessen, die in ihrer Gesamtheit das Schreibverhalten eines Menschen bestimmen. Ein Ausmessen dieses Schreibverhaltens und das Verständnis der einzelnen Vorgänge sind insbesondere dann wichtig, wenn Schriftfälschungen als solche erkannt werden sollen. Zusätzlich zur Gewinnung solcher Grundlagenerkenntnisse über Mechanik und Motorik des Schreibvorgangs wird im Rahmen des Forschungsprojektes versucht, durch Einsatz eines speziell für diese Zwecke entwickelten Laser-Scanning-Mikroskops von der Eindrucktiefe z.B. eines Schreibstiftes in das Papier auf den Schreibdruckverlauf während des gesamten Schreibvorgangs zu schließen, um so ein zusätzliches Verfahren zur Erkennung von Schriftfälschungen zu erhalten. Gleichsam als Nebenprodukt werden bei diesen Untersuchungen Erkenntnisse gewonnen, die zur Entwicklung eines Systems der Zugangskontrolle dienen sollen, bei dem sich ein "Befugter", dem der Zugang zu gestatten ist, durch seine Handschrift ausweist.

Bei der kriminalpolizeilichen Auswertung insbesondere von sogenannten "Bekennerschreiben" nach terroristischen Anschlägen, bei Briefen mit erpresserischem Inhalt usw. ergeben sich Probleme der inhaltlichen und sprachstilistischen Analyse, um z.B. die Authentizität der Schreiben erkennen und sonstige Rückschlüsse auf die Urheber ziehen zu können. Im Rahmen des beim BKA durchgeführten Projektes "Linguistische Textanalyse" wird untersucht, ob für die Lösung dieser Probleme das Verfahren der rechnergestützten Textverarbeitung herangezogen werden kann. Zur Durchführung dieser Aufgabe ist ein Programmsystem entwickelt worden, mit dessen Hilfe Texte in ihre stilistischen und inhaltlichen "Bausteine" zerlegt werden können. Das Prinzip des Vergleichens zweier Texte beruht dann auf dem Grundsatz, daß sie als umso ähnlicher angesehen werden, je mehr Wörter es gibt, deren Stämme in beiden Texten vorkommen, die jedoch im allgemeinen Sprachgebrauch selten sind, und daß der insoweit festgestellte Grad der Ähnlichkeit Rückschlüsse auf die Wahrscheinlichkeit gleicher Autorenschaft zuläßt. Die Merkmale, anhand derer die stilistische Ähnlichkeit ermittelt werden soll, werden - nach derzeitigem Stand des Projektes - teils automatisch ausgewählt, teils vom Gutachter über ein Bildschirmgerät dem Rechner mitgeteilt, wobei eine eigens hierfür entwickelte Benutzersprache angewandt wird. Solche sprachlichen Besonderheiten können aber auch in computerverständlicher Formulierung verwendet werden, um in einer Text-Datenbank bereits vorhandene Texte auffinden zu können.

Das polizeiliche Informationssystem INPOL speichert und verarbeitet u.a. für Zwecke der Personen- und Sachfahndung Texte und Ziffern. Wünschenswert wäre es nun aber auch, über dieses System den abfrageberechtigten Polizeidienststellen den raschen Zugriff zu bildhaften Informationen zu ermöglichen. Lichtbilder gesuchter Straftäter, Fotos mit gestohlenen Gegenständen, Abbildungen von Tatwerkzeugen, Tatortfotos: Diese und andere Abbildungen enthalten Informationen, die für die polizeiliche Tätigkeit von erheblicher Bedeutung sein können. Es ist daher die Aufgabe eines beim BKA mit Unterstützung des Bundesministers für Forschung und Technologie betriebenen Pilotprojektes, die Probleme eines "Bilddatenbank- und Informationssystems" zu bestimmen und Lösungsmöglichkeiten zu entwickeln. Dabei kommen modernste Verfahren der digitalen Bildverarbeitung, der Mustererkennung und der Datenbank-Technologie zur Anwendung.

In diesem Zusammenhang werden zunächst geeignete Bildabtast-Systeme untersucht, die einer Digitalisierung der bildlichen Darstellung dienen, d.h. mit deren Hilfe sich die geometrischen und die tonwertmäßigen Elemente der Abbildungen registrieren lassen. In einem zweiten Arbeitsschritt geht es darum, die digitalisierten Bilder mit Hilfe entsprechender Codierverfahren so zu speichern, daß im Rechner möglichst wenig Speicherplatz in Anspruch genommen wird. Dies ist erforderlich, weil Computerspeicher für die Speicherung digitalisierter Bilder derzeit erhebliche Kosten verursachen. Bei der daher anzustrebenden "Datenkompression" sollen Bilder einerseits durch möglichst wenig Datenwerte dargestellt werden, ohne daß andererseits bei einer Wiedersichtbarmachung ein Informationsverlust entritt, der dem menschlichen Auge ein Wiedererkennen oder einen Vergleich verwehrt. Für Fachleute ist die Feststellung bemerkenswert, daß bisher Reduktionsfaktoren bis maximal 1:10 bei der Digitalisierung von Personenlichtbildern erreicht werden konnten. Die Untersuchungen beziehen neueste Bildspeichermethoden mit ein, die bereits angeboten werden oder sich noch in industrieller Entwicklung befinden (z.B. das Verfahren der optischen Bildplatte, das hochauflösende Mikrofiche-Retrieval-System).

Voraussetzung des Funktionierens einer Bilddatenbank ist die Möglichkeit raschen Auffindens von nicht präzise beschreibbaren Bildern. Auch für die Lösung dieses Problems werden im BKA Verfahren entwickelt, die auf Mustererkennungstechniken beruhen. Als Beispiel hierfür kann die Erarbeitung einer "Suchformel" dienen, die ein Porträtfoto durch eine Reihe geometrischer Daten sowie durch verbal benannte Aussehensmerkmale beschreibt. Und schließlich müssen die in einer Bilddatenbank enthaltenen Bilder wiedergegeben, also wieder sichtbar gemacht werden. Auch hierfür werden im BKA unterschiedliche Techniken überprüft und miteinander verglichen.

Ziel des Pilotprojektes ist es, sämtliche Komponenten eines Bilddatenbank-Systems - von der Digitalisierung über die Codierung, das Speichern und das Wiederauffinden bis hin zur Wiedergabe - in einem Demonstrationsmodell zusammenzufassen, um mit möglichst geringem Risiko die langfristige Entwicklung eines solchen Systems durchführen zu können.

Im übrigen legt der größer gewordene Datenanfall im kriminaltechnischen Bereich, der allerdings nicht nur auf den Einsatz computergestützter Verfahren zurückzuführen ist, eine dokumentarische Aufbereitung nahe. Hiermit werden Möglichkeiten zur statistischen Auswertung geschaffen, welche zur Objektivierung der Indizienbewertung beitragen sollen. Weiterhin wird damit auch eine bessere Verfügbarkeit des Datenmaterials erreicht. In diesem Zusammenhang ist auch die vor einigen Jahren begonnene computergestützte Dokumentation ausgewählter kriminaltechnischer Literatur zu sehen.

Es liegt auf der Hand, daß die zunehmende Bedeutung kriminaltechnischer Untersuchungen und die Anwendung rechnergestützter Vergleichsmethoden nicht nur das kriminalpolizeiliche Ermittlungsverfahren, sondern letztlich auch den Inhalt des Strafprozesses beeinflußt. Durch Erkenntnisgewinnung auf der Grundlage naturwissenschaftlicher Denkabläufe und Faktenbewertung, die nachprüfbar und wiederholbar sind, wird eine Objektivierung des Strafprozesses möglich, wie sie seit Überwindung des Schuld"nachweises" durch Geständniserpressung im peinlichen Hals- und Gerichtsverfahren angestrebt wurde, aber erst in unseren Tagen erreichbar wird.

Die Veränderung der Arbeitswelt des polizeilichen Sachbearbeiters

(Einführungsreferat zur Gruppendiskussion)

Hans-Georg Stuff

1. Einleitung

Kriminalpolizeiliche Tätigkeit - sowohl unter präventiven als auch unter repressiven Aspekten - setzte seit je das Sammeln, Auswerten und Anwenden von Informationen, also von Daten, voraus. Zur Bewältigung ihrer Aufgaben hat sich die Kriminalpolizei - und auch das schon seit jeher - eigene Informationssammlungen aufgebaut:

- Sammlungen, die dem Stande der jeweiligen Büroorganisationspraxis entsprachen: in Form von gebundenen Registern bis hin zur Karteikarte in ihren vielschichtigen Gestaltungsformen.

- Sammlungen, deren Aufbau und dezentrale Führung geprägt waren von der Initiative des jeweils zuständigen Sachbearbeiters. Der Sachbearbeiter gestaltete sich sein Arbeitshilfsmittel den Bedürfnissen der Zeit entsprechend.

In fast allen Bereichen der öffentlichen Verwaltung hat der rasante Wandel der Wirtschafts- und Sozialstrukturen in den 60er Jahren zu einschneidenden Veränderungen in der täglichen Arbeit geführt.

Den Bereich polizeilicher Tätigkeiten berührte vor allem die Entwicklung zur Wohlstandsgesellschaft mit dem veränderten sozialen Verhältnis zum Eigentum einerseits und die sich rasant entwickelnde Mobilität der Bevölkerung andererseits. Die Polizei sah sich vor die Aufgabe gestellt, mit einer ständig steigenden Zahl von Straftaten - insbesondere Eigentumsdelikten - und mit einer permanent steigenden Anzahl reisender und internationaler Straftäter fertig zu werden.

Sie mußte erkennen, daß konventionelle Methoden der Informationssammlung, -aufbereitung und -auswertung den täglichen Bedürfnissen nicht mehr gerecht wurden, und es ist nur folgerichtig, daß sich die Polizei die aufgrund der fortschreitenden Entwicklung der elektronischen Datenverarbeitung gegebenen Möglichkeiten, umfangreiche Informationen zu speichern, zu selektieren und in kürzester Frist bereitzustellen, zunutze machte. Seit etwa 1970 haben Großrechner bisher konventionell geführte Sammlungen abgelöst.

Aufgabe dieses Arbeitskreises soll es nun sein zu untersuchen, welche Veränderungen der Arbeitswelt des polizeilichen Sachbearbeiters durch den Einsatz des Mediums EDV bewirkt wurden, wobei es mir notwendig erscheint, etwa die folgenden vier Aspekte einer näheren Betrachtung zu unterziehen:

* Welche organisatorischen Veränderungen wurden bewirkt?

* Was hat sich im taktischen Vorgehen der Polizei geändert?

* Welche Veränderungen in der Berufsausbildung sind festzustellen, und letztlich

* welche rechtlichen Auswirkungen sind zu beobachten?

2. Die Einzelaspekte

2.1 Veränderungen im organisatorischen Bereich

Datenverarbeitung ist nicht nur die Übernahme einer Kartei auf ein anderes Medium, sondern sie ist einmal die Zusammenfassung vieler gleichartiger aber dezentral verteilter Einzelkarteien, zum anderen aber auch die Integration der inhaltlich verschiedensten Karteiarten zu einem einheitlichen Datensatz, wie er etwa heute als INPOL-Konzept vor uns liegt:

die Zusammenfassung von

- Suchkarteien zu den Kriminalakten,

- Fahndungskarteien,

- Haftkarteien,

- ED-Karteien.

Diese Zentralisation der Information - nicht nur im Verhältnis Bund/Länder, sondern auch auf Länderebene - hat naturgemäß die Einrichtung neuer Organisationseinheiten bewirkt, Zentralstellen, deren Aufgaben wie folgt beschrieben werden können:

- Entwicklung von Informationssystemen,

- Betrieb von Rechenzentren,

- Verarbeitung von Informationen.

Und es entstehen Zentralstellen - Datenstationen - für den Änderungs- und Auskunftsdienst bei den Behörden und Dienststellen der Polizei, die im allgemeinen rund um die Uhr ihren Dienst versehen.

Wir müssen aber auch erkennen, daß mit der Einführung von PIOS und SPUDOK - wie auch der FDR - der Trend zum Terminal in Sachbearbeiterhand geht. Nach Telefon, Fernschreiber und Funkgerät wird das Datensichtgerät Kommunikationsmittel im polizeilichen Alltag und ist in die Arbeitsabläufe zu integrieren.

2.2 Neue polizeiliche Berufsbilder

Der verbreitete Einsatz der automatisierten Datenverarbeitung fordert den Spezialisten:

* DV-Organisatoren,

* Programmierer,

* Operatoren,

* Terminalbediener

  wirken zusammen bei der Entwicklung und im täglichen Betrieb von Informationssystemen.

* Organisatoren, die in fast allen Ländern auf der Basis eines fundierten polizeilichen Wissens zu Datenverarbeitern fortgebildet wurden,

* Programmierer und Operatoren in den polizeilichen Rechenzentren, die die Uniform auszogen, um praktisch einen neuen Beruf zu erlernen und

* Terminalbediener als Mittler quasi zwischen Datenverarbeitungsanlage und dem informationssuchenden Polizeibeamten.

Diese Palette von Berufsfeldern reicht für den Betrieb der derzeitig betriebenen Informationssysteme aus. Der polizeiliche Sachbearbeiter selbst bleibt von den besonderen Anforderungen der Datenverarbeitung weitgehend verschont - er formuliert seine Anträge in konventioneller Weise und erhält die erbetene Auskunft von seiner Datenstation.

Schon die Probeläufe der Straftaten-/Straftäterdatei, viel mehr aber noch der Einsatz von Dokumentationssystemen wie PIOS oder SPUDOK, zwangen zum Überdenken des Berufsbildes des Terminalbedieners. Hier war der Datentypist überfordert.

Für die sachgerechte Erfüllung der Aufgaben mußten erfahrene Kriminalbeamte herangebildet werden mit

* meldedienstlicher Erfahrung, d.h. Analytiker mit dem taktischen, technischen und dienstkundlichen Wissen des Kriminalisten; Auswerter, die die Auswertungsstrategien des Meldedienstes beherrschen, die Fingerspitzengefühl für Tatzusammenhänge und Tat-/Täterbeziehungen mitbringen. Mitarbeiter schließlich, die abstrahieren und logisch kombinieren können, die fremde Logik überwinden und in andere Formen zu kanalisieren vermögen,

* vertieftem Verständnis für programmtechnische Abläufe komplizierter Speicherungs- und Rechercheverfahren,

* sicherem Gefühl für die notwendige Vereinheitlichung des Sprachgebrauchs,

Mitarbeiter letztlich, deren Arbeitsplatz das Datensichtgerät ist, dessen Bedienung beherrscht werden muß. Insgesamt fordern wir hier Qualifikationen, die beileibe nicht von allen Polizeibeamten - auch nicht Kriminalbeamten - erbracht werden.

2.3 Veränderungen im taktischen Vorgehen der Polizei

2.3.1

Unbestritten darf heute festgestellt werden, daß nach Einführung des INPOL-Verbundes eine Fahndungsaktualität erreicht wurde, die kaum noch verbesserungsfähig ist. Wir haben aber auch durch die erleichterte Form des Zugriffs auf Fahndungsdaten die Fahndungsdichte erheblich erhöht. Der straff organisierte Abgleich von personenbezogenen Daten in Strafanzeigen und Berichten pp. mit Fahndungs- und KAN-Daten bietet dem Sachbearbeiter schnelle Entscheidungshilfen.

Wir beobachten ein steigendes Interesse am Einsatz von SPUDOK-Systemen bei großen Ermittlungsverfahren. Die Möglichkeiten des Rasterabgleichs von Datenbeständen schaffen Ermittlungsansätze, die konventionell nicht zu erlangen waren. Das gilt auch für den Erkenntnisgewinn aus dem beim BKA geführten neuen Daktyloskopieverfahren.

2.3.2

Wir müssen aber auch erkennen, daß die Datenverarbeitung nicht nur leistet, sondern auch fordert:

* Nur schnelle und genaue Anlieferung von Daten sichert hohe Aktualität und schützt vor Fehlinformation.

* Der sinnvolle und optimale Einsatz von Recherchesystemen zwingt zu einer Vereinheitlichung des Sprachgebrauchs und zur Verwendung von umständlich zu handhabenden Katalogen.

* Das Formularwesen hat sich erheblich ausgeweitet.

2.3.3

Wie der Stabsgliederung in der PDV 100 zu entnehmen ist, ist die Datenverarbeitung aus der Arbeit großer Stäbe nicht mehr wegzudenken. Es ist aber auch schon deutlich geworden, daß Sonderkommissionen der Kriminalpolizei neben den taktischen und technischen Beamten den Datenverarbeiter in ihr Team holen.

2.4 Veränderungen in der rechtlichen Situation

2.4.1

Informationssammlungen der Polizei standen früher außerhalb jeder Diskussion - sie galten als schlichtes Verwaltungshandeln. Dem sog. Mikrozensus-Beschluß des Bundesverfassungsgerichts blieb es vorbehalten, diesen Sammlungen eine neue Rechtsqualität zu verleihen, nachdem festgestellt wurde, daß die Sammlung und Registrierung von personenbezogenen Informationen den Bürger in der freien Entfaltung seiner Persönlichkeit einenge und das Sammeln von Informationen Eingriffscharakter haben kann. Damit entstanden für die Polizei zwei Problemkreise:

2.4.1.1

Die Rechtmäßigkeit polizeilicher Informationsverarbeitung schlechthin wurde in Zweifel gezogen. Wenn das Sammeln von Informationen die grundsätzlich geschützten Persönlichkeitsrechte antastet und Eingriffscharakter bekommen hat, fehlen der Polizei tatsächlich die speziellen Rechtsgrundlagen. Mit den Generalklauseln des § 163 StPO und der Polizeigesetze lassen sich diese Eingriffe nicht rechtfertigen - eine spezialgesetzliche Regelung ist bestenfalls für den Bereich der erkennungsdienstlichen Maßnahmen gem. § 81 b StPO und vergleichbarer polizeirechtlicher Normen vorhanden, wie auch für die Weiterleitung von Informationen an das BKA gem. § 2 BKAG.

Die fehlende Initiative des Gesetzgebers wurde ersetzt durch die Fülle von Dienstvorschriften zur Regelung von Teilaspekten polizeilicher Datenverarbeitung: Dateirichtlinien, Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen (KpS), Kriminalaktennachweis, PDV 384.1 und 384.2, ED-Richtlinien, PIOS-Richtlinien usw. Das Gebiet der Vorschriften über die polizeiliche Informationsverarbeitung ist nicht mehr recht überschaubar und nur noch von Spezialisten sachgerecht zu handhaben.

2.4.1.2

Die Schwierigkeiten, im Rahmen von Ermittlungen alle notwendigen Informationen zu erlangen, haben sich potenziert. Seit dem 01.01.81 ist mit Inkrafttreten des § 31 Sozialgesetzbuch I und des Kap. 2 SGB X z.B. aus dem Bereich der Sozialleistungsträger praktisch keine Information mehr zu erlangen.

Restriktiv verhalten sich aber auch andere außerpolizeiliche Behörden und Private. Die Polizei wird so gezwungen, selbst für simpelste Informationen wie Anschriften von Zeugen und Beschuldigten aufwendige Anträge zu stellen, um richterliche Beschlüsse zu erwirken. Hier sind nunmehr die Gesetzgeber in Bund und Ländern aufgerufen, die Initiative zu ergreifen.

3. Ausblick

Die Datenverarbeitung scheint weitgehend in die Arbeitsabläufe des polizeilichen Alltags integriert. Eine Vielzahl von Anforderungen für spezielle Einsätze macht deutlich, daß weitere Einsatzmöglichkeiten von den Praktikern gesehen werden.

Für mich wird eine Diskrepanz zwischen taktischer Forderung und technischer Möglichkeit einerseits und rechtlichem Zugeständnis - d.h. Datenschutz- und Haushaltsrecht - deutlich.

Ganz sicher ist die Datenverarbeitung nicht das Allheilmittel bei der Verbrechensbekämpfung - auch konventionelle Hilfsmittel können rationell und optimal sein -, sie ist aber eine wesentliche Hilfe bei der Bewältigung polizeilicher Aufgaben.

Unsere Politiker müssen sich die Frage stellen, wieviel Kriminalität wir ertragen wollen oder welche Bekämpfungsintensität der Polizei politisch - d.h. rechtlich - zugestanden werden soll.

Die technischen Möglichkeiten der Datenverarbeitung sind nicht erschöpft.

ADV-Probleme in der Aus- und Fortbildung

(Einführungsreferat zur Gruppendiskussion)

Thomas Gnad

Es ist zunächst einmal Aufgabe der Ausbildung, zu erklären, wie ein Computer funktioniert. Soll die ADV von den Mitarbeitern angenommen werden, darf sie nicht das "unbekannte Wesen" bleiben, das in Erstaunen versetzende Leistungen vollbringt. Es ist deshalb erforderlich, diese Informationslücke mit der für den jeweiligen Mitarbeiter erforderlichen Wissensvermittlung zu schließen. Darauf aufbauend werden die ADV-Anwendungen in Bund und Land ausbildungsbedarfsorientiert dargestellt.

Das Erfordernis der sukzessiven Neuorientierung der Polizei, das Umstellen der Personen- und Sachfahndung, der Vorgangs- und Kriminalaktenverwaltung, der kriminalpolizeilichen Statistik, der Daktyloskopie und einiger Teilbereiche des kriminalpolizeilichen Meldedienstes von manueller auf ADV-Erfassung muß allen Mitarbeitern verdeutlicht werden.

Es ist hierbei dringend geboten, neben der Wissensvermittlung über das Funktionieren der ADV (Terminals, Drucker usw.) die psychologische Seite bei den Bediensteten ganz besonders zu beachten. Hier ist die Scheu vor der neuen Informationstechnologie zu nehmen. Die Unsicherheit der Sachbearbeiter muß abgebaut werden; sie sind ständig zur Annahme der ADV zu motivieren. Es muß immer wieder aufgezeigt werden, daß die polizeilichen Informationssysteme Arbeitshilfen darstellen, die dem einzelnen nützen, die keinen Prestige- und Kompetenzverlust verursachen, die aber den Arbeitsplatz verschiedener Mitarbeiter zum Vorteil verändern.

Durch diese Aus- und Fortildungsmaßnahmen dürfte Frustration nicht entstehen, denn es wird

- die ADV als modernes Arbeits- und Organisationsmittel dargestellt,
- der technologische Fortschritt, der zwar Arbeitsplätze und bisherige Arbeitsmethoden verändert, der aber viel Routine erledigt, als unabänderlich dargestellt,

- die Bereitschaft zur Annahme der ADV bei dem Sachbearbeiter gefördert,

- das Selbstvertrauen zur ADV-Anwendung gestärkt.

Der "Anwender" soll dahingehend motiviert werden, die ADV als unverzichtbares Arbeitsmittel der Zukunft anzuerkennen und zu sehen, daß sie zu seinem Vorteil nur dann wertvolle Arbeit leisten kann, wenn er zuvor als Sachbearbeiter, Datenstationsbediener, Analytiker usw. ordentlich gearbeitet hat.

Nur durch die Aus- und Fortbildung ist es möglich, die ADV immer mehr an den Arbeitsplatz einer immer größeren Anzahl von Mitarbeitern zu bringen und zu erreichen, daß diese sich mit ihrer Aufgabe, mit ihrem Beruf auch unter den veränderten Bedingungen identifizieren. Die ADV-Anwendung muß in die tägliche Arbeit integriert werden, sie muß Routineanwendung sein. Standardanfragen müßte jeder Polizeibeamte beherrschen.

Es muß allgemein bekannt sein, welche Anfragemöglichkeiten und Anfrageerfordernisse beim Ersteinschreiten oder im Laufe von Fahndungen und Ermittlungen, aber auch zur optimalen Wahrnehmung von Führungsaufgaben und auf dem Gebiet der Forschung und Lehre, vorhanden sind. Es ist jedoch trotz ständiger Hinweise durch die Aus- und Fortbildung und durch Dienst- und Fachaufsicht immer wieder festzustellen, daß einmal Anfragen nicht umfassend genug erfolgen und daß zum anderen die Bereitschaft zur Datenaktualisierung nicht optimal ist.

Bei Lehrveranstaltungen wird das Erfordernis anerkannt, jedoch in praxi unzureichend umgesetzt. Die Datenaktualisierung wird als Belastung angesehen und meist mit Arbeitsüberlastung begründet.

Bei der Schutzpolizei fehlt häufig die Kenntnis über die kriminalpolizeiliche Sachbearbeitung und über den Kriminalpolizeilichen Melde- und Fahndungsdienst. Aber auch bei der Kriminalpolizei wird der Meldedienst allzuoft nur als Belastung angesehen.

Ein besonderer Problemkreis im Bereich der ADV-Anwendung ist der Datenschutz. Die in Polizeikreisen und im Bereich der veröffentlichten Meinung erfolgten Diskussionen führten mehr zu einer Verunsicherung als zu einer Klarstellung über die Frage, in welchen Fällen wem welche Auskünfte gegeben werden dürfen und wann dies nicht geschehen darf. Es ist auch hier Aufgabe der Aus- und Fortbildung, ihren Beitrag zum aktuellen Stand des Datenschutzrechts zu leisten.

Es ist hier klarzustellen, daß das zur Gewährleistung der öffentlichen Sicherheit und Ordnung erforderliche Informationsbedürfnis der Polizei mit dem individuellen Persönlichkeitsrecht der Staatsbürger, die möglichst unbeeinträchtigt leben möchten, konkurriert und deshalb hie und da eingeschränkt werden muß.

Ein weiteres Problem ist die Frage, ob für Ausbildungszwecke von Datenstationen der Polizeischulen aus Anfragen an das polizeiliche Informationssystem gehalten werden dürfen oder ob sog. Übungsprogramme erstellt werden müssen.

Hinsichtlich der Schulung auf dem Gebiet der ADV-Anwendung fehlt bei den Polizeischulen oft der ständige Bezug im Fachunterricht; bei den Lehrkräften ist nicht genügend "ADV-Bewußtsein" vorhanden.

Die Aus- und Fortbildung der Polizei richtet sich länderspezifisch nach der jeweils praktizierten Datenerfassung:
Entweder erfolgt die Datenerfassung durch den polizeilichen Sachbearbeiter, der als erster alle für die Datenverarbeitung erforderlichen Informationen erhält = Sachbearbeiterprinzip, oder eine angemessene Anzahl von Beamten analysiert und erstellt alle anfallenden Daten = Analytikerprinzip. Beide Verfahren haben Vor- und Nachteile, besonders hinsichtlich der Aktualität, der Fehlerquote und der Wirtschaftlichkeit.

Die Aus- und Fortbildung der Anwender stellt bei dem Sachbearbeiterprinzip aufgrund der großen Zahl der Auszubildenden ein Problem dar. Hier werden z.B. Grundkurse zur Erstinformation mit Leistungskontrollen durchgeführt, in denen Theorie und Praxis mit Anwendungsbeispielen und Gerätebedienungskenntnisse vermittelt werden. Die Verwaltungsfachhochschulen erteilen in den verschiedenen Studienabschnitten Unterricht über ADV-Themen und Datenschutz, außerdem wird z.T. während der Praktika mit der ADV gearbeitet.

Neben dieser Grundausbildung sind Instruktoren (in Hessen Koordinatoren), die als Multiplikatoren im Fortbildungsbereich eingesetzt werden und die alle ADV-Neuerungen und ADV-Probleme an die Anwender herantragen, notwendige Wegbereiter für die Anwendungserweiterungen und Problemlösungen. Sie sind es auch, die Fragen aus der Praxis an die ADV-Fachabteilung herantragen und so ihren Beitrag zur weitgehend reibungslosen ADV-Anwendung leisten.

Bei speziellen ADV-Verfahren (Daktyloskopie, PIOS, Recherchierprogramme) werden wenige Bedienstete sehr intensiv ausgebildet.

Für die fortlaufende Information sind ferner Anwenderhandbücher, schriftliche Mitteilungen mit Anwendungsbeispielen, periodische Rundschreiben, Broschüren und Merkblätter in Postkartengröße wertvolle, die Ausbildung unterstützende Medien.

Mit das größte Problem polizeilicher Arbeit und Ausbildung ist die Massenkriminalität und hier im besonderen die Kriminalität "rund um das Fahrzeug". Diese mit enormen Informationsmengen verbundene Kriminalität ist mit dem Kriminalpolizeilichen Meldedienst nicht optimal zu bekämpfen. Zum einen fehlt bei diesen Delikten in der Regel eine wichtige Voraussetzung für einen effizienten Meldedienst, der für jeden Tatortbeamten erkennbare modus operandi. Dieses täter- und tatbezogene perseverante Handeln ist kaum mehr festzustellen und wenn, nicht täter-, sondern nur noch objektspezifisch. Zum anderen mangelt es an einer bundesweiten nichtnumerischen Sachfahndung, die evtl. über die Sicherstellung von Diebesgut einen Beitrag zur Straftatenaufklärung leisten könnte. Eine adv-unterstützte nichtnumerische Sachfahndung besteht nur in Bayern, Hessen, Niedersachsen und Schleswig-Holstein.

Im Bereich der nichtnumerischen Sachfahndung sollte der desolate Zustand des Kriminalpolizeilichen Meldedienstes durch Installation einer bundeseinheitlichen Sachfahndung nach eindeutig beschreib- und unterscheidbaren Gegenständen mittels ADV erfolgen. Es muß hierbei insbesondere durch Schulungsmaßnahmen dafür gesorgt werden, daß der Rechner kein Müllplatz für nicht wieder auffindbare Gegenstände wird. Vor Eingabe von Fahndungsdaten ist die Frage nach dem Nutzen zu stellen; es ist zu prüfen, ob man selbst mit dem Ausdruck einer entsprechenden Datenmenge etwas anfangen kann. Eine Überfrachtung der Datei mit nicht unterscheidbaren Daten muß unterbleiben. Gerade hier hat die Aus- und Fortbildung einen wichtigen Informationsbeitrag zu leisten.

Ausbildungs- und Informationsprobleme - aus der Sicht der Anwendung

(Einführungsreferat zur Gruppendiskussion)

Hans-Georg Kaesehagen

Die auf das Thema hinführende Fragestellung wird deutlich, wenn man sich einen bestimmten Unterschied unter den Anwendungen auf dem Gebiet der Datenverarbeitung vor Augen führt. Es gibt Anwendungen wie z.B. Statistiken, Einwohnerdatenbanken, Anwendungen zur Bearbeitung von Verkehrsordnungswidrigkeiten, die dem Benutzer statt des konventionellen Hilfsmittels, meist der Kartei, ein elektronisches Hilfsmittel in die Hand geben und im übrigen den seither stattfindenden Arbeitsablauf kaum berühren. Es sind dies Anwendungen, die von den Benutzern im Prinzip keine Änderung gewohnter Tätigkeiten verlangen; außerdem sind die Vorteile der Automation ohne weiteres klar. Die pädagogische Hinführung auf die Anwendung kann sich - vereinfacht gesagt - auf die Information über die Technik und die Benutzung beschränken. Besondere Ausbildungs- und Informationsprobleme sind insoweit nach meinem Dafürhalten nicht zu erörtern.

Anders verhält es sich mit Anwendungen, die der Polizei Einsatzinformationen vermitteln, wie Fahndungshilfen aus INPOL oder Informationen zur Unterstützung der Führungstätigkeit in Einsatzzentralen. Hier gilt, daß der Beamte im Funkstreifenwagen und der Beamte am Leittisch der Führungs- und Lagezentrale (FLZ) nicht gezwungen sind, sich der elektronischen Hilfen in einem weitgehend festliegenden Umfang zu bedienen. Es ist vielmehr ihrer Initiative, ihrer Phantasie und ihrem Engagement überlassen, ob und inwieweit sie sich in den zahlreichen Einsatzfällen des Alltags dieser Hilfen bedienen, bzw. ihre Wahrnehmungen dem System mitteilen oder in einen Dialog mit diesen treten.

Der von mir formulierte Unterschied soll verdeutlichen, daß Anwendungen, die erst infolge Zuspruchs der Benutzer, nach der Akzeptanz der Beamten Nutzen bringen, pädagogisch und hinsichtlich der Menschenführung aufwendig sind. Über ein solches in der Information und Ausbildung der Benutzer auf allen Ebenen der Hierarchie aufwendiges Projekt will ich als Beispielsfall kurz berichten.

Es handelt sich um eine Computerunterstützung mit der Abkürzung ELIAS in unserer Führungs- und Lagezentrale. Die Anwendung umfaßt erstens das bekannte Funkmeldesystem, zweitens einen Anwendungsbereich Ereigniserfassung und -bearbeitung einschließlich eines sogenannten Reportgenerators, das ist die Zusammenführung von Informationen aus den erfaßten Ereignissen, drittens den Durchgriff auf Fremdanwendungen wie INPOL und das Einwohnerdatensystem des Landes (externes Infosystem), viertens einen lokalen Informationspool (internes Infosystem), dessen Gestaltung uns weitgehend freigestellt ist, schließlich Statistik, Auswertung und Dokumentation. Das Ganze ist dem bekannten CEBI aus Nordrhein-Westfalen nicht unähnlich, aber wegen des Durchgriffs auf andere Anwendungen wie EWOIS und INPOL weniger aufwendig, im internen Infosystem für den Benutzer freier.

Als Hardware ist vorhanden eine Zentraleinheit IBM 8140 mit der üblichen Konfiguration für 3 Bedienplätze in der Führungs- und Lagezentrale, nämlich je zwei Farbbildschirmen, einem Doppel-Zusatzleitplatz für größere Lagen, sowie einem Administratorenleitplatz, der ebenfalls ein Aktiv- und Passivgerät hat. Außerhalb der Führungs- und Lagezentrale verfügen wir über je einen Einzelleitplatz für den Unfalldienst, den Verkehrsüberwachungsdienst und die Kriminalwache, jeweils mit eingeschränkter Funktion.

Die Software wird von dem Landesrechenzentrum Rheinland-Pfalz geliefert. Die Administration, insbesondere die Dateneingabe und Datenpflege, wird durch eigene Kräfte des Polizeipräsidiums Mainz bewirkt, die vom Landesrechenzentrum ausgebildet worden sind.

Der Stand der Realisierung ist folgender: Die Maschinenseite einschließlich Datenstationen sowie Bedienplätze sind in unserer FLZ seit Mai 1982 vorhanden und seit August 1982 im effektiven Betrieb; allerdings befindet sich die Anwendung in den einzelnen Bereichen noch in schrittweisem Aufbau. Es laufen aber alle fünf Anwendungsbereiche.

Die Problemstellung für unsere Führungskräfte lautet: Wie bringen wir unsere Beamten dahin, die zahlreichen, ihrer Disposition unterliegenden Möglichkeiten der Anwendung zu nutzen, so daß die nicht unerheblichen Kosten der Realisierung rentierlich werden im Sinne verbesserter polizeilicher Erfolgschancen. Dies gilt um so mehr, als Mainz - eine Großstadt mit knapp 200.000 Einwohnern - generell gesehen nicht im oberen Bereich der effektiven Nützlichkeit einer solchen Anwendung liegen kann. Wenn das also nicht nur ein

Prestige- und Vorzeigeobjekt sein soll, dann ist es erforderlich, unter Beteiligung aller Führungskräfte, des Bedienpersonals in der Führungs- und Lagezentrale, insbesondere aber auch der Beamten vor Ort, das Ganze mit viel Leben zu erfüllen.

Dem Beamten muß also klargemacht werden, welche Möglichkeiten die Anwendung eröffnet und welchen konkreten Nutzen bei hohem Benutzer-Komfort ihm diese Möglichkeiten im alltäglichen Geschäft z.B. für die Aufgabe der Verbrechensbekämpfung bieten, allerdings auch, was von ihm verlangt wird. Dies bedeutet, daß wir auf allen Ebenen von S und K informierte und motivierte Beamte haben müssen, die von der Anwendung überhaupt Gebrauch machen und insbesondere Ereignisse und Erkenntnisse ihrer Wahrnehmung in das System geben oder der Führungs- und Leitzentrale melden sowie auch dort gebotene Informationsmöglichkeiten abrufen.

Zu erwähnen ist, daß die Ausgangssituation für die Bewältigung der Informations- und Ausbildungsprobleme bei der neuen Anwendung für uns nicht ungünstig ist. Seit Mitte der 70er Jahre verfügen wir nämlich über Datenverarbeitungsanwendungen in unserer FLZ; und zwar kann das rheinland-pfälzische Einwohnermeldesystem EWOIS aus der Einsatzzentrale seither abgefragt werden, ebenso INPOL in dem fragmentarischen Umfang der parallelen Führung durch das Landesrechenzentrum. Es ist davon auszugehen, daß durch den jahrelangen Gebrauch im Alltagsbetrieb insbesondere den Funkstreifenbesatzungen die Nützlichkeit der elektronischen Datenverarbeitung allgemein geläufig ist. Der Beamte hat erlebt, daß Informationen der erwähnten Systeme über Funk prompt und bequem verfügbar sind. Andererseits habe ich folgende Sorge: Das Projekt ELIAS, das wir als Pilotprojekt für das Land erproben, birgt die Gefahr in sich, daß die Führungskräfte moderne Technik als Wert an sich betrachten und den Umgang mit der Anwendung nicht primär unter dem Verhältnis Kosten/Nutzen sehen.

Der Anwendungsbereich Funkmeldesystem kann z.B. eine Entlastung des Funkverkehrskreises um etwa 40 % des Routinebetriebes bringen; man muß aber wissen, daß bei der Polizei in der Größenordnung von Mainz die Zeit der Überlastung des Funkverkehrskreises, also des Nutzens des FMS als Entlastung, vielleicht 2 - 3 von 168 Stunden in der Woche beträgt. Der Nutzen des Systems bei abhörgefährdeten Einsätzen ist dagegen stets vorhanden, wenn solche Einsätze stattfinden.

Die Aufgabe der Führung unter diesen Bedingungen muß sein, zusätzliche Anreize für Intitiative, Originalität und Ideenreichtum zur Ausschöpfung der gebotenen Möglichkeiten zu geben.

Im einzelnen sehe ich folgende Informations- und Ausbildungsprobleme, die für eine Realisierung unserer Anwendung grundlegend sind:

- Heranführen der Führungskräfte von S und K an eine streng am Nutzen für die Erfüllung polizeilicher Aufgaben orientierte Betrachtungsweise als Maßstab der Anwendung; das bedeutet: eine möglichst intensive Nutzung anzustreben.

- Auswahl und Ausbildung von dazu geeigneten Polizeibeamten zu Systemadministratoren, d.h. Besetzung der Stabstelle SB 24 der bundesweiten Führungsstabgliederung. Aufgabe dieser Kräfte ist es, in Zusammenarbeit mit dem Projektbearbeiter des Landesrechenzentrums die Anwendung in der Behörde zu betreuen, das heißt insbesondere die Dateneingabe selbst vorzunehmen, die Daten zu pflegen und bei den Kinderkrankheiten der ersten Realisierungsphase ständig als Bindeglied zum Landesrechenzentrum zu fungieren.

- Schrittweise intensive Einweisung der Beamten am Leittisch in ihren völlig neugestalteten Leitplatz, Notwendigkeit einer Nullserie (eines Probelaufes) vor Inbetriebnahme. Ständiger Kontakt des Systemadministrators mit diesen Beamten.

- Training der Vorgesetzten der Einsatzsachbearbeiter, also des Leiters der Führungs- und Lagezentrale im Zusammenhang mit dem erforderlichen Testlauf.

- Training der Polizeiführer vom Dienst, der Dienstgruppenleiter, Wachhabenden durch Vermittlung des Inhalts des Benutzerhandbuches und Einweisung in die neue Technik der FLZ möglichst noch während des Testlaufes.

- Das Training der Beamten vor Ort bedient sich ebenfalls des Benutzerhandbuches sowie eines Videofilms über das Funkmeldesystem, hergestellt vom Landespolizeipräsidium in Stuttgart. Es bedient sich weiter der Möglichkeit, die Beamten des Außendienstes - auch die Beamten der Kriminalpolizei - informatorisch in der Führungs- und Lagezentrale einzuweisen. Bei der Information und Schulung der Beamten kann glücklicherweise auf die, wenn auch lückenhafte Praxis mit Datenverarbeitung in der Führungs- und Lagezentrale aus den letzten Jahren zurückgegriffen werden. Wir können dabei stufenweise vorgehen, da wir die Anwendung auch stufenweise innerhalb der einzelnen von mir beschriebenen Anwendungsbereiche realisieren. Dies erscheint uns wichtig, weil die Akzeptanz nur in einem Dialog, in einem Prozeß der theoretischen Erörterungen und des praktischen Ausprobierens, der sich über eine gewisse Zeit erstreckt, bewirkt werden kann. Dabei muß insbesondere verdeutlicht werden, daß das Projekt keine gegen die Beamten gerichtete Kontrollfunktion hat, daß es vielmehr ein Führungsinstrument ist, das die Effektivität der Polizei steigern soll. Vielleicht berührt die Anwendung den Stolz insbesondere unserer Funkstreifenbeamten, allein auf sich gestellt mit den Problemen des täglichen Dienstes fertig werden zu können. Gewiß kann man ihnen aber auch klarmachen, daß das Führungs- und Auskunftssystem ihnen rechtzeitig wirksame Hilfen in diesen ständig wechselnden Situationen immer wieder geben kann. Wenn dies gelingt, ist nach meinem Dafürhalten die Anwendung mit dem nötigen Leben erfüllt.

Als Folgerung am Schluß möchte ich herausstellen, daß die Grundhaltung des Außendienstbeamten zur Datenverarbeitung wichtig ist. Deswegen darf eine Anwendung nicht primär als Prestige- oder Vorzeigeobjekt hingestellt werden. Bei allen Beteiligten sollte vielmehr als Grundmaßstab die konkrete Nützlichkeit in den Vordergrund gestellt werden. Die angesichts der immer noch wachsenden Kriminalität notwendige Steigerung der Effizienz der Polizei ist ein ständiges Führungsproblem, das der Computer nicht automatisch lösen kann, aber deutlich werden läßt. Führung indessen beginnt bei notfalls ständig wiederholter Information und Ausbildung.

P o d i u m s g e s p r ä c h

Innere Sicherheit und Datenverarbeitung

Teilnehmer: Paul Laufs, Kuno Bux, Herbert Neu, Hans Peter Bull, Axel Wernitz, Heinrich Weyer, Heinrich Boge

Gesprächsleitung: Edwin Kube

E. Kube

Die Polizei hat Vorstellungen über wünschbare Handlungsspielräume. Sie verfügt über Konzepte und stellt Überlegungen an, wie technisch Machbares im Interesse der Verbrechensbekämpfung weiterentwickelt wird, wie es in Dienststellen optimal eingesetzt und genutzt wird. Dies gilt nicht zuletzt für die elektronische Datenverarbeitung.

Technisch Machbares im Polizeibereich ist begrenzt und eingebunden in politische Grundsatzentscheidungen, die ihrerseits an den verfassungsrechtlichen Vorgaben des Grundgesetzes ausgerichtet sind. Da Freiheit und Ordnung (im Sinne des inneren Rechtsfriedens) verfassungsrechtlich gleichrangige Werte sind, ist die Entscheidung für das Überwiegen des einen oder des anderen Aspekts eine immanent politische Entscheidung.

Es ist deshalb nicht nur sinnvoll - sondern notwenige Voraussetzung für eine sachgerechte und kompetent geführte Diskusssion, daß Politiker unser Gespräch wesentlich mitgestalten. Ich begrüße als Vertreter der Politik die Herren Bundestagsabgeordneten Dr. Laufs und Dr. Wernitz. Herr Dr. Wernitz ist bekanntlich Vorsitzender, Herr Dr. Laufs Mitglied des Innenausschusses des Deutschen Bundestages. Ebenso herzlich willkommen heißen darf ich Herrn Neu, ehemaligen stellvertretenden F.D.P. - Fraktionsvorsitzenden im Landtag Nordrhein-Westfalen. Ihm gebührt Dank auch deshalb, weil er sehr kurzfristig anstelle des verhinderten MdB Dr. Burkhard Hirsch zu uns gekommen ist.

Ein ausgewogener und in der Begrenzung eindeutiger Datenschutz kann zusätzliche innere Sicherheit schaffen, zumindest im Sinne eines umfassenderen Sicherheitsgefühls der Bevölkerung. Datenschutz ist Grundrechtsverwirklichung,

Verbrechensbekämpfung ist dies aber nicht weniger. Zwischen Polizei und Datenschutz wird es - und muß es vielleicht - Bewertungskonflikte geben, wenn es um Ausmaß und Struktur der polizeilichen Datenverarbeitung geht. Auch die Polizei sieht ihre Funktion im Bereich des Datenschutzes. Allerdings werden insoweit ihre Auffassungen nicht selten vom institutionalisierten Datenschutz als höchst unzureichend angesehen.

Als sachkundige Vertreter des Datenschutzes begrüße ich Herrn Prof. Bull, Bundesbeauftragter für den Datenschutz, sowie Herrn Dr. Weyer, Landesbeauftragter für den Datenschutz Nordrhein-Westfalen. Die polizeilichen Belange bei der Podiumsdiskussion nehmen Herr Bux, Präsident des Landeskriminalamtes Baden-Württemberg sowie der Hausherr des Amtes, Präsident Dr. Boge wahr.

Ich bitte zunächst die Teilnehmer am Podiumsgespräch zum Thema "Innere Sicherheit und Datenverarbeitung" jeweils ein kurzes Statement als Basis für die weitere Diskussion abzugeben. Im Anschluß an die Diskussion auf dem Podium ist das Plenum eingeladen, sich an der Aussprache zu beteiligen, um die unterschiedlichsten Sichtweisen und Bewertungen in das Gespräch einfließen zu lassen.

H. Boge

Erklärtes Ziel dieser Arbeitstagung war es, den derzeitigen Entwicklungsstand der Datenverarbeitung in der Polizei in aller Offenheit darzustellen und aus unterschiedlichen Positionen zu bewerten und darüber hinaus ansatzweise die Möglichkeiten und Grenzen der Weiterentwicklung aufzuzeigen.

In den bisherigen Referaten und Diskussionen ist das erfolgt, und wie zu erwarten war, wurden in der durchweg sachbezogenen Diskussion auch konträre Standpunkte deutlich.

Über Art und Umfang polizeilicher Datenverarbeitung bestehen, was aufgrund der unterschiedlichen Interessenlage der einzelnen Redner selbstverständlich ist, verschiedene Ansichten. Was aber ganz deutlich wurde, ist, daß niemand, der sich zu Wort gemeldet hat, davon ausgeht, daß der polizeiliche Beitrag zur Gewährleistung der Inneren Sicherheit ohne Hilfe der Datenverarbeitung erbracht werden kann.

Aufbauend auf diesem Grundkonsens muß um eine Lösung gerungen werden, die es der Polizei in rechtsstaatlich einwandfreier Weise ermöglicht, effiziente Verbrechensbekämpfung zu betreiben. Grundvoraussetzung dafür ist, daß ihr die erforderlichen Daten schnell und umfassend zur Verfügung stehen.

Für erforderlich halte ich dabei die Daten sowohl aus der repressiven Arbeit der Polizei als auch aus dem präventiven Bereich.
Ich halte es für unverträglich für die polizeiliche Aufgabenerfüllung, wenn die Justizseite generell fordert, deliktisch einheitliche Sachverhalte in präventive und repressive Daten zu teilen, um sie sodann unterschiedlichen Kompetenzen und Zugriffen zu unterwerfen. Prävention und Repression sind unmittelbar miteinander verbundene, untrennbare Bereiche polizeilicher Tätigkeit.

Die heutige Spezialisierung der öffentlichen Verwaltung hat dazu geführt, daß zur polizeilichen Aufgabenerfüllung zwingend erforderliche Daten auch bei einer Vielzahl von Behörden der Ordnungsverwaltung, z.B. beim Kraftfahrt-Bundesamt, beim Ausländerzentralregister, bei den Einwohnermeldeämtern, aber auch beim Bundeszentralregister im Justizbereich selbst, geführt werden. Es wäre dem Bürger gegenüber unverantwortlich, mit der Datenfernübertragung heute zur Verfügung stehende Mittel der schnellen und sicheren Informationsübermittlung nicht zu nutzen. Wenn im Rahmen der Verkehrspolizei oder der Grenzpolizei die Zugriffsberechtigung auf bestimmte Datenbestände etwa des Kraftfahrt-Bundesamtes oder des Ausländerzentralregisters, anerkannt und notwendig ist, kann das Verfahren, das dem Interesse - auch des etwa von Überprüfungen Betroffenen - am besten dient, nämlich, der "on-line"-Zugriff, nicht ausgeschlossen werden.

Zum Umfang der benötigten Daten ist festzustellen, daß die Polizei selbst am wenigsten an "blindwütigem" Sammeln interessiert ist, Quantität wird nicht automatisch Qualität. Datenschutz findet am intensivsten im Bereich der Polizei durch diese selbst statt. Auch die externe Kontrolle ist im Rechtsstaat selbstverständlich, sie darf aber nicht derart sein, daß eine rechtmäßige Aufgabenerfüllung unmöglich gemacht wird. Die Vermutung der Rechtmäßigkeit darf nicht durch eine Vermutung der Unrechtmäßigkeit ersetzt werden.

Die angesichts zunehmender Kriminalität ständig schwieriger werdende Aufgabe, zur Gewährleistung der Inneren Sicherheit beizutragen, verlangt, daß die Anwendung der Datenverarbeitung weiter in Breite und Tiefe ausgebaut wird. Ziel ist die Verbesserung der Unterstützung beim Tätigwerden möglichst weit vor Ort, in der mittelbaren Einsatz- und Ermittlungsunterstützung, in der Kriminaltechnik und Forschung. Die ständige Überprüfung, Optimierung und der Ausbau vorhandener Systeme werden die Unterstützung der Sachbearbeiter, etwa durch noch bessere Möglichkeiten der Verknüpfung bei der Recherche, aber auch der Führung der Polizei durch bessere Analyse der Erscheinungsformen der Kriminalität und der Methoden ihrer Bekämpfung, ermöglichen.

Nicht zuletzt gehört dazu der Ausbau der Informationsbeziehungen über die nationalen Grenzen hinweg. Der Zusammenarbeit mit Interpol dürfen nicht unter Gesichtspunkten eines engen nationalen Datenschutzes Fesseln angelegt werden, die nur der Ausbreitung des internationalen Verbrechens zugute kommen würden.

Auch aus der Sicht der Polizei geht es jedoch nicht allein um die weitere Optimierung ihrer Funktionsfähigkeit. Wichtig, ja vorrangig, ist die vom Grundgesetz legitimierte Optimierung, die ihre Grenzen vor allem auch im Respekt vor der Freiheit des Bürgers findet. Dies ist vor allem eine Frage an die Politik. Nicht alles, was machbar ist und die polizeiliche Arbeit erleichtern würde, wird von mir und uns Polizeibeamten als erstrebenswert angesehen.

P. Laufs

Im politischen Bereich trifft man viele Menschen, die sich vom enormen Fortschritt der Informations- und Kommunikationstechniken bedroht und sich der modernen Datenverarbeitung ausgeliefert fühlen. Man begegnet auch zunehmend einer Grundstimmung, die vom Verlangen nach neuen Freiräumen und Autonomie gegenüber der immer perfekter werdenden Einbindung in das Geflecht staatlich reglementierter sozialer Abhängigkeiten geprägt ist. Die Selbstbestimmung über Informationsbeziehungen soll sich dabei keineswegs auf die aktive Gestaltung der Kommunikationsumwelt beschränken, sondern vor allem auch die Abwehrrechte umfassen, die verhindern können, zum Objekt der Datenverarbeitung durch Dritte zu werden. Insbesondere könne - so wird gesagt - jeder staatliche Akt der Erhebung und Verarbeitung persönlicher Daten ein Eingriff in die Grundrechte des einzelnen darstellen und dürfe nur unter engen Voraussetzungen zulässig sein. Besonders leidenschaftlich wird über die polizeiliche Datenverarbeitung bei der Gefahrenabwehr und der Strafverfolgung im Bereich der Inneren Sicherheit diskutiert. Es sind politische Bestrebungen erkennbar, jede Vorfeldtätigkeit auszutrocknen sowie die Handlungsräume bei der Verfahrenseinleitung und das Ermessen bei der Auswahl von Beweismitteln äußerst restriktiv zu gestalten. Wer aber die Realitäten nüchtern prüft, kommt um die Feststellung nicht herum, daß in unserem Land die Vision vom gläsernen, im Zugriff des Computers total manipulierten Menschen auch nicht im entferntesten Wirklichkeit zu werden droht. Es gibt überhaupt keine Hinweise darauf, daß die Gefahr des "großen Bruders" des Orwellschen Jahres 1984 im Verzug wäre. Wirklicher Mißbrauch bei der Verarbeitung personenbezogener Daten und daraus entstehender Schaden sind bisher nicht bekannt geworden. Dies muß so auch in Zukunft bleiben. Über die Notwendigkeit sorgfältiger Planung von Informationssystemen, der Datenhygiene und des vorbeugenden Datenschutzes zur sicheren,

die Persönlichkeitsrechte des Bürgers wahrenden Beherrschung der neuen Techniken gibt es deshalb im Grundsatz keinen politischen Streit. Es kann auf der anderen Seite jedoch kein Zweifel darüber bestehen, daß durch ängstlichen Verzicht auf die Nutzung moderner Datenverarbeitung sowie durch eine einseitig offensive Anwendung des Datenschutzrechts die Funktionsfähigkeit der Sicherheitsbehörden beeinträchtigt und damit die Freiheit der Bürger, die Sicherheit des Staates und der Rechtsfrieden gefährdet werden können. Der Konflikt entzündet sich am richtigen Verständnis von Zuständigkeiten, von rechtmäßiger Erfüllung erforderlicher Aufgaben, von Amtshilfe und anderen unbestimmten Rechtsbegriffen. Die Abwägung zwischen dem Allgemeinwohl des Staates und seiner Bürger und den persönlichen Interessen des einzelnen ist eine schwierige Aufgabe. Die Behörden haben diese Abwägung auf Grund von Verfassung und Gesetz vorzunehmen. Es wäre unerträglich, wenn durch einen ständigen öffentlichen Streit über den Datenschutz im Sicherheitsbereich der falsche Eindruck entstünde, als würden die Behörden diesen Ausgleich tendenziell stets zuungunsten der Individualinteressen entscheiden. Datenschutz hilft Freiheit sichern und dient dem Persönlichkeitsschutz. Der Sicherheitsbereich darf selbstverständlich kein Bereich frei von Datenschutz sein - im Gegenteil. Aber der Datenschutz darf niemals zum Vehikel werden, um die Erfüllung verfassungsmäßiger und gesetzlicher Aufgaben bei der Verbrechensbekämpfung und -vorbeugung von Polizei, Verfassungsschutz und Nachrichtendiensten zu behindern. Er kann auch nicht allein und vorrangig über die weitere Nutzung elektronischer Informations- und Kommunikationstechniken im polizeilichen Bereich entscheiden. Die Leistungsfähigkeit und Einsatzvielfalt der polizeilichen Datenverarbeitung haben noch lange nicht ihre Grenzen erreicht. Denken wir etwa an intelligente Auskunftssysteme mit integrierter Verarbeitung von Daten, Texten, Bildern und Sprache, an rechnergestützte Stimm- und Handschriftenerkennung oder an vermaschte Netze. Es ist selbstverständlich, daß diese neuen Techniken, soweit sie ausgereift und sinnvoll anwendbar sind, auch genutzt werden. Alle Überlegungen, welche zusätzlichen Anwendungen noch auf den Computer genommen werden könnten, muß man aber - schon wegen der Kosten - stets mit der Frage verbinden: Was sollte man dem zwar langsamen aber mit seinen Kombinationsmöglichkeiten völlig unerreichbaren menschlichen Gehirn überlassen?

A. Wernitz

Ich begrüße es, daß eine solche Tagung konkret und gezielt den Versuch unternimmt auszuloten, wie es um Datenschutz und Innere Sicherheit bestellt ist. Ich habe, mit vielen Freunden gemeinsam, seit Jahren gefordert, daß nicht nur punktuell und gelegentlich sondern permanent ein Dialog

zwischen den Vertretern der Inneren Sicherheit und dem Datenschutz zustandekommt. Dies ist eine Aufgabe, die sich im Grunde genommen Tag für Tag stellt; diese Einsicht sollten wir von einer solchen Tagung für die künftige Arbeit jeder in seinem Bereich mitnehmen.

Der Kollege Laufs hat eben zu Recht das Problem der Gefahr des gläsernen Menschen in die Diskussion eingeführt und sie verneint. Wirksamer Datenschutz ist auch im Bereich der Inneren Sicherheit unverzichtbar. Auch wenn man das aktuelle konkrete Risiko des sogenannten gläsernen Menschen verneint, ist es dennoch notwendig, sich politisch dazu zu bekennen, daß es nicht dazu kommen darf, daß irgendwo alle über den einzelnen Bürger gespeicherten Daten zu einem umfassenden Persönlichkeitsbild zusammengeschaltet werden können und so gleichsam eben doch eines Tages der sogenannte gläserne Mensch produziert wird. Hier gilt es, sehr genau zu unterscheiden zwischen der gegenwärtigen Lage, von der viele Insider mit guten Gründen sicher sagen können, daß keine aktuelle Gefahr besteht und der Notwendigkeit, die Sorgen und Ängste der Menschen in unserem Staat, und nicht nur in der Bundesrepublik, in diesem Punkt ernstzunehmen. Man muß offen darüber reden und, soweit dies irgend geht, die Dinge offenlegen, damit hier Ängste, Vermutungen, Verdächte, Sorgen etc. abgebaut werden können. Dies darf eben nicht nur verbal geschehen, sondern muß sich auch überzeugend durch Handeln im Alltag im konkreten Einzelfall darstellen.

An der Diskussion zum Thema "Innere Sicherheit und Datenschutz" stört mich seit Jahren, und zwar bis in diese Tagung hinein, der törichte pauschale Streit oder die Kontroverse über die Frage des Stellenwertes der einen Vokabel, nämlich der Sicherheit auf der einen Seite und des Datenschutzes auf der anderen Seite. Nichts ist unfruchtbarer und nichts ist vielleicht typischer deutsch, als dieser Prinzipien- und Papierstreit: Die Innere Sicherheit darf nicht vor dem Datenschutz stehen bzw. umgekehrt. Ich halte nichts von solchen Thesen wie der: Sicherheit gehe vor Datenschutz. Das ist genauso falsch, wie wenn andere sagen, Datenschutz müsse in jedem Fall über der Inneren Sicherheit stehen. Von diesem Schlagabtausch müssen wir wegkommen, denn er dient weder dem einen noch dem anderen Bereich. Wir sollten vielmehr klar und eindeutig erkennen, daß es in beiden Fällen darum geht, Bürgerrechte, Persönlichkeits- und Freiheitsrechte, also Grundrechte zu sichern. Es ist im Einzelfall ein Zielkonflikt, und hier muß immer wieder austariert werden. Man muß Kompromisse schließen. Es gilt, konkrete Lösungen im Einzelfall zu finden, und deshalb muß man von diesen pauschalen Thesen abkommen.

Es ist und bleibt notwendig, daß sich die Sicherheitsbehörden bei der Erfüllung ihrer Aufgaben moderner technischer Hilfsmittel und damit auch der elektronischen Datenverarbeitung bedienen können. Ich bin in diesem Punkt immer sehr offensiv für Ihren ehemaligen Präsidenten Herrn Herold eingetreten und ich habe nie Verständnis dafür gehabt, wenn manchmal mit Ironie gesagt wurde, er sei in die EDV "verliebt" und dies sei eine Spielerei. Ich bin überzeugt, daß wir heute nicht in der Lage wären, eine effektive Kriminalitätsbekämpfung und damit die Innere Sicherheit in unserem Land hinlänglich zu garantieren, wenn die EDV nicht auch im Bereich der Inneren Sicherheit eingeführt worden wäre. Ich meine, dies muß bei einer solchen Gelegenheit auch gesagt werden. Das Bundesdatenschutzgesetz läßt dies - allerdings unter bestimmten Voraussetzungen - auch ausdrücklich zu. Das Ja zur EDV beinhaltet aber zugleich das Ja zu den notwendigen Datenschutzmaßnahmen. Hierzu haben wir ja das Bundesdatenschutzgesetz geschaffen - mit all seinen Unvollkommenheiten. Ich will sie hier nicht einzeln aufzählen - es fängt bei den unbestimmten Rechtsbegriffen an. Aber es war für uns immer klar, daß der Weg Schritt für Schritt zu bereichsspezifischen Lösungen führen muß - und diesen Weg sind wir auch gegangen.

Ich habe mit Interesse zur Kenntnis genommen, was Herr Spranger zu Beginn dieser Tagung gesagt hat. Was in den Zeilen steht, ist, leger formuliert, okay. Aber ich muß auch die Praxis der letzten Jahre mit einbeziehen und dabei auch zwischen die Zeilen gehen. Bei den Tätigkeitsberichten des Datenschutzbeauftragten im Innenausschuß haben wir, was die Grundsätze angeht, schon oft sehr weitgehend Einigkeit und Einmütigkeit erzielt. Der Teufel steckt dann aber im Detail und da beginnt dann die Nagelprobe. Ich habe in den letzten Jahren erlebt, daß es bei manchen, die ihre Grundsätze abstrakt bejahen - auch was das Ja zum Datenschutz angeht - im Einzelfall dann oft anders aussieht. Als wir uns seinerzeit im BDSG zur externen Kontrolle auch im öffentlichen Bereich bekannt haben, wurde auch die These vertreten, der öffentliche Bereich sei an die Gesetzmäßigkeit gebunden und die Kontrolle erübrige sich daher. Dies scheint mir so nicht haltbar. Meine Bitte an alle geht dahin, daß wir bei aller Kritik am Verhalten der anderen Seite jeder in seinem Bereich - dies ist ein Appell aus der Legislative heraus - lernen müssen, auf diesem Gebiet bei den Zielkonflikten, die wir ohne Zweifel haben, fair und manchmal vielleicht auch zurückhaltend, aber dennoch offen und hart in der Sachaussage miteinander umgehen müssen. Hier sind wir alle miteinander noch in der Phase des Lernens. Dies bedingt einerseits eine offene klare Sprache, aber auch da und dort Vorsicht in der Ausdrucksweise; denn sonst könnte unter Umständen in der Tat Schaden entstehen. Er entsteht aber nicht schon dadurch, daß man bestehende Defizite offenlegt. Ich will keine Mauschelei haben. Wenn der Datenschutzbeauftragte

den Eindruck hat, daß nach seiner Beurteilung der Sachverhalte im allgemeinen und im konkreten Einzelfall Defizite bestehen, daß mißbräuchlich mit Daten umgegangen wurde - nicht nur im Sicherheitsbereich, aber auch dort - dann will ich eine klare Aussage haben, was er zu bemängeln hat. Und wenn nach seiner Beurteilung die Rechtsgrundlagen nicht hinreichend tragfähig sind, dann will ich als Mitglied der Legislative wissen, wo aus seiner Sicht solche Defizite bestehen und mehr Rechtssicherheit, d.h. Absicherung vom Grund her, geboten erscheint. Hier ist auch die bisherige Opposition im Bundestag nicht immer konsequent gewesen. Bei einer Debatte anläßlich der Diskussion des letzten Tätigkeitsberichts im Ausschuß wurde gesagt, man solle diese Fragen nicht vor der Öffentlichkeit austragen, sondern intern halten. Einige Wochen später hatten wir dann die kleine Anfrage der Union auf dem Markt, wo diese Punkte alle als Drucksache aufgelistet wurden. Das kann man sicher so machen, und vielleicht müssen wir das auch bei anderen Gelegenheiten einmal ausdiskutieren. Ich bin hier durchaus für Transparenz - man kann nur nicht beides gleichzeitig fordern. Ich bin auch überzeugt, daß eine offene Debatte über Pro und Contra, über Defizite, aber auch über die Mängel, die bereits abgestellt wurden, letzten Endes beiden Seiten hilft. Sie kommt der Inneren Sicherheit und dem Datenschutz zugute, und der Bürger ist überzeugt, daß allgemein und im Einzelfall dieser schwierige Prozeß des Austarierens und Abwägens von Innerer Sicherheit und Datenschutz tatsächlich stattfindet.

Ich möchte deshalb an die Vertreter der Inneren Sicherheit, an Herrn Boge und an den Bundesbeauftragten für Datenschutz die Bitte und den Appell richten, es nicht bei gelegentlichen Begegnungen wie der heutigen zu belassen, sondern in gewissen regelmäßigen Abständen auch immer wieder einmal in Klausur in Vier-Augen-Gespräche zu gehen. Dies wäre für beide Seiten und für uns alle eminent hilfreich. Ich sage dies als Mitglied der Legislative, als Anregung und als Appell.

H. Neu

Ich bin aus zwei Gründen ein wenig gehandicapt. Zum ersten habe ich Landespolitik gemacht und mich mit dem Bundesdatenschutzgesetz nur als Beispiel für unser eigenes Gesetz befaßt und nicht in seinem Alltag in entsprechenden Ausschüssen mitgewirkt. Zum zweiten bin ich nicht mehr Parlamentarier und habe mich somit seit 3 Jahren nicht mehr mit dem Datenschutz befaßt. Auch an der Diskussion über den ersten Datenschutzbericht unseres Datenschutzbeauftragten habe ich nicht mehr als Parlamentarier teilgenommen. Daher möchte ich mich in meinen Ausführungen an das halten, was ich hier bisher gehört habe und auch an das, was ich früher bei der Diskussion über das Datenschutzgesetz im Plenum gesagt habe.

Die Ausgewogenheit zwischen Ordnung und Freiheit im Grundgesetz hat bei den Gesetzgebern häufig Gewissenskonflikte ausgelöst; sie mußte auch beim Datenschutzgesetz zum Gewissenskonflikt führen. Hierbei wurde sehr schnell deutlich, daß Technik kein Wert in sich ist, sondern daß man sich ernsthaft fragen muß, was neue Techniken dem Menschen an Beglückung oder auch an Bedrückung bringen können. Bei der Diskussion über das Datenschutzgesetz von Nordrhein-Westfalen haben sich zwei Dinge herausgestellt. Einmal wird durch die Technik der Computer die Gewalt der Datensammlung zwar bedrückend, aber im Grunde genommen wird die menschliche Unzulänglichkeit bei der Verwaltung dieser Daten verringert. Denn wer 5 Millionen Daten mit bestimmten Angaben über Einzelpersonen in einem Computer verwaltet, ist von der betroffenen Einzelperson viel weiter entfernt als der, der eine Handakte oder eine Handdatei führt, z.B. in einer kleinen Gemeinde oder einem anderen überschaubaren Bereich. Dies kann viel schlimmer sein, als wenn diese Daten in einem Großcomputer verschwinden. Die Gefahr von Unkorrektheiten im Umgang mit intimen Daten wird für den einzelnen wesentlich geringer. In der Diskussion ist meist untergegangen, daß so zwei sehr unterschiedliche Momente des Unbehagens und der Bedrücktheit entstehen können bei der Frage nach der alten Handdatei und dem Computer. Daher haben wir in der Diskussion um die Lösung dieser Fragen in Nordrhein-Westfalen auch den Zugriff des Datenschutzbeauftragten für die Handdateien sichergestellt, was nicht in allen Ländern der Fall ist.

Ein besonderes Problem scheint mir die Sammlung von Präventivdaten für die präventive Kriminalitätsbekämpfung aufzuwerfen. Es handelt sich zumeist um Vermutungsdaten oder Schlußfolgerungsdaten, und der Rückgriff auf solche Daten wird dann erfolgen, wenn man den Umkreis bestimmter Täter beobachten will oder beobachten muß. Hier ist natürlich der Computer selbst gar kein Schuldiger, sondern vor dem Eingang in den Computer muß im Grunde genommen die Zuverlässigkeit des korrekten Beamten stehen, die Neutralität des Denkens und die Sach- und Zielbezogenheit. Hier beginnt bereits das Risiko, wenn man zur präventiven Kriminalitätsbekämpfung Daten einspeichert und nicht erst beim Abfragen. Ich will damit nicht sagen, daß man diese Daten nicht braucht. Ich möchte nur auf die Schwierigkeiten hinweisen, die in der Vermutungs- und in der Erfahrungsebene liegen.

Als Beispiel möchte ich folgenden Fall anführen: Eine Kollegin, Landtagsabgeordnete aus Nordrhein-Westfalen, kommt mit ihrem jungen, langhaarigen und bärtigen Mann aus dem Urlaub zurück. An der Grenze wird ihr Wagen an die Seite gestellt und auseinandergenommen. Als die Prozedur beendet war, hat die Kollegin ihren Landtagsausweis gezogen und gefragt, warum nun gerade ihr Wagen untersucht worden sei. Darauf sagte man ihr: Entschuldigen Sie bitte, aber Ihr

Mann ist nach unserer Erfahrung ein so typischer Fall eines Verdächtigen für Rauschgifthandel oder Mitnahme von Hasch oder ähnliche Dinge, daß wir das einfach tun mußten. Etwa zur gleichen Zeit flogen die jungen Terroristen als Manager getarnt mit Hubschrauber über Deutschland. Sie sehen hieran, daß Erfahrungsschätze nur kurzlebig sind und daß der Beamte in der durchaus berechtigten Sorge, hier könne er einen solchen Mann vor sich haben, mit dem völlig falschen Erfahrungsschatz gearbeitet hat. Die Beweglichkeit dieses Beamten war sicher begrenzt. Denn wenn echte Transporteure von verbotenen Materialien in die Bundesrepublik bereits wissen, daß sie keinen alten verrosteten Wagen, keinen alten VW, keine langen Haare, keinen Bart haben dürfen, dann bleibt der Erfahrungsschatz noch eine Weile hängen und geht am tatsächlichen Täter vorbei. Deshalb muß man beim Sammeln von präventiven Daten noch viel stärker auf die Korrektheit, die Beweglichkeit und die Urteilsfähigkeit des Eingebenden achten als bei der repressiven Kriminalitätsbekämpfung, bei der man es ja mit Fakten und nicht mit Vermutungen zu tun hat. Die Fehlerquellen liegen mehr bei der Einspeicherung als in der späteren Nutzung. Hier ist es besonders wichtig, daß mit der größten Sorgfalt vorgegangen wird. Ich zweifle nicht daran, daß alle, die Daten speichern, wie Banken und Wirtschaftsunternehmen, Einwohnermeldeämter und Gesundheitsämter, Forschung und Wissenschaft und auch die Polizei den Willen haben, korrekt zu handeln. Dennoch bleibt die Notwendigkeit bestehen, wenn es sich um Erfahrungssätze und Vermutungen handelt, beim Speichern von Daten in der präventiven Kriminalitätsbekämpfung mit besonders großer Sorgfalt an die Dinge heranzugehen.

Ich darf abschließend noch die Einstellung meiner Fraktion im Landtag Nordrhein-Westfalen vorlesen, wie sie seinerzeit in der Diskussion des neuen Datenschutzgesetzes fomuliert wurde: "Gewiß dürfen und sollen wir nicht zulassen, daß etwa ein Straftäter oder Verfassungsfeind sich über das Auskunftsrecht zum Datenschutz Gewißheit über den Stand der Fahndung nach ihm und der Beobachtung verschaffen kann. Dies würde Verfassungsschutz, Kriminalpolizei, Steuerfahndung zu Unwirksamkeit und Ohnmacht verurteilen. Aber deswegen haben wir noch nicht die Legitimation, diese empfindlichen und notwendigerweise geheimen Bereiche auch der Kontrolle durch den Datenschutzbeauftragten zu entziehen. Nach unserer Konstruktion hat daher jeder Betroffene, der die Sammlung falscher oder nicht beweisbarer Daten in diesem Bereich oder ihre mißbräuchliche Weitergabe befürchtet, auch hier das Recht, den Datenschutzbeauftragten des Landes anzurufen. Dieser muß dann die Einhaltung des Datenschutzgesetzes, selbstverständlich unter Beachtung der Geheimhaltungsvorschriften, nach außen kontrollieren." Mit dieser Konstruktion ist uns eine vorbildliche Bewältigung dieses Zielkonflikts zwischen Geheimhaltungsbedürftigkeit und dem Schutz der Person gegenüber falsch gespeicherten Daten gelungen. Hier ist in dem

Zielkonflikt zwischen Ordnung und Freiheit die Vertrauensperson des Datenschutzbeauftragten eingeschaltet worden und es wäre interessant, den Datenschutzbeauftragten des Landes Nordrhein-Westfalen gleich einmal zu der Frage zu hören, wie sich die Zusammenarbeit zwischen ihm und der Polizei gestaltet hat und wie dieser Passus sich auf seine Arbeit auswirkt, daß er Daten überprüfen kann bei der Polizei, ohne dem Antragsteller konkrete Auskunft zu geben, und wie die Polizei auf solche für sie doch recht empfindlichen Nachfragen reagiert. Mir scheint, daß hier die Zusammenarbeit ganz besonders wichtig ist und der Abbau oder das Nichtentstehen von Mißtrauen entscheidend sein muß für eine gedeihliche Nutzung von Daten, die in einem solchen Ausmaß, wie es auch in dieser Tagung bekanntgegeben wurde, gesammelt werden. - Ich stelle immer wieder mit Erstaunen fest, daß bei der Handakte, bei der "Handdatei" das Mißtrauen gar nicht erst entstanden ist, obwohl da im intimen Bereich des Bearbeiters und eines ihm bekannten Bürgers viel schlimmere Dinge geschehen konnten und auch sicher passiert sind durch Unkorrektheit und Indiskretionen, als dies beim großen Computer in der Regel der Fall sein wird.

H. P. Bull

Ich war leider nicht in der Lage, diese Tagung von Anfang an zu besuchen, aber ich habe viele Presseberichte, einige Zusammenfassungen und das Referat von Herrn Dr. Boge gelesen und mir von meinen hier anwesenden Mitarbeitern weiteres berichten lassen. Es wird Sie vielleicht überraschen: Den meisten Äußerungen, die auf dieser Tagung zum Verhältnis von Datenschutz und polizeilicher Datenverarbeitung getan wurden, stimme ich ausdrücklich zu. Ich möchte insbesondere unterstreichen, was Herr Dr. Boge gesagt hat: "Die elektronische Datenverarbeitung muß sich stets ihrer tatsächlichen und rechtlichen Grenzen bewußt bleiben, um sowohl innerhalb der Polizei als auch in der Bevölkerung als wertvolles und unerläßliches Hilfsmittel der Verbrechensbekämpfung akzeptiert zu werden. Bei der Einrichtung und beim Betrieb polizeilicher Informationssysteme muß der Grundsatz 'Qualität vor Quantität' eingehalten werden... Selbst die komplexeste Datei kann nur verkürzte Informationen enthalten ... Es ist davor zu warnen, ... polizeiliche Maßnahmen und Entscheidungen ... allein auf Auskünfte aus einem DV-System zu stützen". So hat Herr Boge formuliert, und so ähnlich habe ich schon in zahlreichen schriftlichen und mündlichen Äußerungen formuliert, zuletzt in mehreren Vorträgen im Ausland, wo man sich zunehmend für das deutsche Datenschutzrecht und die Praxis der Datenschutzkontrolle interessiert.

Ich sehe es auch wie Herr Boge, daß "die Positionen von Polizei und Datenschutz gar nicht so weit voneinander entfernt sind, wie es manchmal scheinen könnte" - z.B. besteht gar kein Streit darüber, daß die meisten datenschutzrechtlichen Beanstandungen, die ich gegenüber den Sicherheitsbehörden ausgesprochen habe, begründet sind; die Behebung der Mängel ist mit erheblichem Aufwand eingeleitet und weit vorangebracht worden.

Auch was Herr Parlamentarischer Staatssekretär Spranger zu Beginn dieser Tagung ausgeführt hat, findet überwiegend meine Zustimmung. Ich bin insbesondere froh darüber, daß er sich gegen zu große Erwartungen an die Technik gewandt hat. In der Tat: Es bedarf, wie ich schon seit langem immer wieder gesagt habe, der "Spürnase" des erfahrenen Kriminalisten nach wie vor und vielleicht mehr denn je. Gegen "Übertreibungen" beim Datenschutz haben sich alle Datenschutzbeauftragten gewandt; soweit sie dennoch vorgekommen sind, z.B. weil manche Behörden das Melderecht falsch angewendet oder den Datenschutz als Vorwand für ganz andere Ziele benutzt haben, haben wir unsere Hilfe angeboten und vielfach Hinweise für eine richtige, sinnvolle Anwendung des Datenschutzrechts gegeben. Ich erinnere auch daran, daß wir uns immer gegen die Feststellung gewehrt haben, die Bundesrepublik sei ein "Überwachungsstaat", und daß wir in konkreten Problemkomplexen wie dem der Rasterfahndung eine differenzierte, letztlich auch von der Polizei als begründet anerkannte Meinung vertreten haben.

Interessanter freilich als das, was die Vertreter von Polizei und Innenministerium auf dieser Tagung erklärt haben, scheint es mir festzustellen, was sie nicht gesagt haben und was zwischen den Zeilen anklang. So hat sich Herr Spranger leider überhaupt nicht mit den konkreten Problemen bestimmter Datenverarbeitungsvorgänge bei den Sicherheitsbehörden befaßt, die meine Mitarbeiter bei ihren Kontrollbesuchen festgestellt haben und die ich gegenüber dem Bundesminister des Innern angesprochen habe. Im Innenausschuß des Bundestages konnte ich dazu - zum Teil in vertraulicher Sitzung - detaillierte Einzelangaben machen, und es haben mehrere mehrstündige Beratungen stattgefunden. An die Öffentlichkeit dringen aus solchen Sitzungen freilich immer vorwiegend pauschale und formale Aussagen, wie die, es habe "eine Kontroverse um den Datenschutz" gegeben.

Wenn Herr Spranger erklärt, Datenschutz habe "keinen absoluten Vorrang vor den Erfordernissen der öffentlichen Sicherheit", so ist das natürlich, wörtlich genommen, völlig zutreffend. Nur frage ich mich, warum Herr Spranger das so betont, obwohl er doch weiß, daß ein solcher Vorrang nirgends geschrieben steht und von niemandem verlangt wird. Er riskiert mit so akzentuierten Äußerungen, daß er

dahin mißverstanden wird, als habe der gesetzlich begründete Datenschutz regelmäßig zurückzutreten, wenn die Sicherheitsbehörden der Ansicht sind, eine Datenschutzvorschrift behindere sie unangemessen bei ihrer Arbeit. Dies wäre für mich und meine Kollegen nicht hinnehmbar: Es steht der Verwaltung nicht zu, zwischen den Erfordernissen ihrer eigenen Aufgabenerfüllung und der Anwendung gesetzlicher Vorschriften abzuwägen und sich etwa gegen die Anwendung geltenden Rechts auszusprechen. Nur da, wo der Gesetzgeber diese Abwägung nicht vorgenommen, sondern sie (z.B. durch Schaffung von Ermessensvorschriften) der Verwaltung überlassen hat, kann sich die Frage stellen, ob "der Datenschutz" hinter "der Sicherheit" zurücktreten muß.

Wenn wir weitere Fortschritte im Datenschutz erzielen wollen, ist es unbedingt notwendig, die konkreten Probleme konkret zu besprechen. Ich nenne - wegen der Zeitbegrenzung nur als Stichworte - einige Punkte, über die mit dem Ziel gemeinsamer Lösungen zu beraten ist:

- Registrierung "anderer Personen" als Beschuldigter und Verdächtiger (Nr. 4.2.11 Dateienrichtlinien),

- Spuren-Dokumentationsdateien und ihre Nutzung in anderen als den ursprünglichen Zusammenhängen,

- Auskünfte an andere Stellen ohne Kenntnis des aktuellen Standes verzeichneter Ermittlungsverfahren,

- on-line-Anschlüsse, z.B. Personen-Anfrage beim Kraftfahrt-Bundesamt (Gefahr eines Ersatz-Bundesmelderegisters), polizeilicher Zugriff auf das Ausländerzentralregister und das Bundeszentralregister,

- Gefahr des Unterlaufens der Kriterien zentraler Speicherung im Kriminalaktennachweis durch Rückgriff auf andere Dateien, insbesondere Daktyloskopie,

- beabsichtigte Dateien im Bereich Staatsschutz.

Um der Öffentlichkeit ein möglichst differenziertes Bild zu vermitteln, nenne ich auch die erzielten Fortschritte und die Ansätze zu einer positiven Weiterentwicklung, z.B.:

- Auskünfte an die Betroffenen nach KpS-Richtlinien; hier wurde übrigens auch der Beweis geliefert, daß mehr Transparenz die polizeiliche Arbeit nicht schädigt;

- Errichtungsanordnungen zu verschiedenen Dateien (trotz verbleibender Probleme ein Fortschritt);

- in einigen Bereichen inzwischen differenzierte Überprüfungs- bzw. Löschungsfristen;

- erhebliche Anstrengungen bei der Bereinigung von Altbeständen.

Gerade weil ich es - entgegen dem, was manche verbreiten - für unbedingt erforderlich halte, die fachlichen Beurteilungen der handelnden Beamten in die rechtlichen Überlegungen einzubringen, bedauere ich es, daß viele sich nur oder vornehmlich mit der angeblich unangemessenen Form der datenschutzrechtlichen Bemerkungen befassen. Auch Herr Dr. Boge hat dies am Dienstag wieder getan. Ich bestreite, unfair berichtet zu haben. Im Gegenteil habe ich mich manchmal gefragt, ob nicht deutlichere Worte nötig gewesen wären, wo ich es bei Andeutungen und Hinweisen belassen habe. Vereinzelt bekam ich sogar zu hören, ich sei angesichts der Fakten - wie ich sie z.B. im Innenausschuß des Bundestages ausbreiten konnte - in meiner Kritik noch sehr zurückhaltend gewesen. Aber davon abgesehen, beunruhigt mich ein Aspekt in der Äußerung von Herrn Dr. Boge sehr. Ich habe seinem Manuskript entnommen, daß er es offenbar auch für unangemessen hält, wenn bei der datenschutzrechtlichen Beurteilung "juristische Techniken" verwendet werden. Ich muß ihn fragen: welche anderen als juristische Techniken sollen wir Datenschutzbeauftragten denn verwenden? Wir haben Verwaltungsvorgänge am Maßstab des Rechts zu messen; sollen wir dies mit "politischen" Argumentationen tun? Das wäre für mich ein grundlegend falsches Amtsverständnis. Wir würden damit den festen Grund unter den Füßen verlieren und uns den jeweils aktuellen Opportunitätserwägungen ausliefern.

Selbstverständlich kann ich nur meine Rechtsansicht vertreten - die wirkliche, nicht nur "vorgeschobene", wie Herr Dr. Boge unterstellt. Sie werden doch nicht ernsthaft erwarten, daß ich immer gleich hinzufüge, die Gegenmeinung habe aber auch viel für sich. Handelt so eine Opposition im Parlament, ein Anwalt vor Gericht, ein Unternehmer in einer geschäftlichen Verhandlung, ein Staatsanwalt beim Abfassen einer Anklageschrift?

Ich bin nach wie vor bereit, mich belehren zu lassen, wenn meine Ansichten auf schwachen Füßen stehen sollten - aber ich werde es nicht hinnehmen, wenn jemand ohne konkrete Argumente versucht, rechtliche Überlegungen zum Schutz von Individualrechten zu disqualifizieren.

H. Weyer

Es ist unbestritten, daß zur Erfüllung der Aufgaben der Sicherheitsbehörden die Verarbeitung personenbezogener Daten, auch in automatisierten Verfahren, notwendig ist. Ebenso dürfte aber unbestritten sein, daß auch in diesem Bereich aus der Datenverarbeitung Gefahren für die Freiheitssphäre des einzelnen erwachsen können. Der Datenschutz, der diesen Gefahren begegnen soll, ist Grundrechtsschutz. Durch ihn sollen grundrechtlich geschützte Positionen des Bürgers gewährleistet werden.

Ich bin mir bewußt, daß Datenschutz und Aufgabenerfüllung der Sicherheitsbehörden oft in einem Spannungsverhältnis zueinander stehen. Hier wie auch in anderen Bereichen stehen sich verschiedene Rechtsgüter gegenüber, die gegeneinander abgewogen werden müssen. Diese Abwägung ist zunächst einmal Aufgabe des Gesetzgebers. Dieser hat zu bestimmen, inwieweit dem einen und inwieweit dem anderen Rechtsgut Vorrang einzuräumen ist. Dies ist in den Datenschutzgesetzen sowie in bereichsspezifischen Rechtsvorschriften wie etwa dem Steuergeheimnis oder dem Sozialgeheimnis geschehen, die Vorrang vor den Datenschutzgesetzen haben.

Die Schaffung bereichsspezifischer Datenschutzregelungen im Sicherheitsbereich ist eine schwierige Aufgabe. Sie verlangt eine sorgfältige Abwägung zwischen den Sicherheitsbelangen der Allgemeinheit und den Datenschutzbelangen der Bürger. Soweit und solange der Gesetzgeber sich noch nicht in der Lage sieht, eine solche Abwägung bereichsspezifisch vorzunehmen, müssen die allgemeinen Regelungen der Datenschutzgesetze jedenfalls durch bereichsspezifische Verwaltungsvorschriften konkretisiert werden. Der Erlaß der bundeseinheitlichen KpS-Richtlinien sowie der Dateienrichtlinien ist daher grundsätzlich zu begrüßen, wenngleich diese Regelungen noch nicht allen Anforderungen des Datenschutzes Rechnung tragen. Zu begrüßen ist insbesondere, daß die KpS-Richtlinien nicht zwischen Dateien und Akten unterscheiden, sondern für den Umgang mit personenbezogenen Daten ohne Rücksicht auf die Art der Datenverarbeitung die gleichen Maßstäbe festlegen. Es gilt, die neuen Richtlinien jetzt zunächst einmal in der Praxis zu erproben.

Aus der Vielzahl der Datenschutzfragen, die sich in meinem Zuständigkeitsbereich ergeben haben, möchte ich hier nur zwei herausgreifen.

Nach dem Datenschutzgesetz sind die Polizeibehörden nicht verpflichtet, einem Bürger auf Antrag Auskunft über die zu seiner Person etwa gespeicherten Daten zu geben. Diese Regelung ist von der Polizei in der ersten Zeit vielfach als Auskunftsverbot mißverstanden worden. Tatsächlich

bedeutet sie jedoch nur, daß die Polizei nach pflichtgemäßem Ermessen zu entscheiden hat, ob sie dem Auskunftsersuchen eines Betroffenen entsprechen will.

Ich habe seit Beginn meiner Tätigkeit bezweifelt, ob die frühere Praxis der Polizei, die Auskunft an den Betroffenen regelmäßig zu verweigern, in allen Fällen geboten war und ob sie in dem wohlverstandenen Interesse der Polizei lag. Durch die Erteilung der beantragten Auskunft wird vielen Menschen unbegründete Angst genommen und zum Abbau von Mißtrauen gegen die Arbeit der Polizei beigetragen, was letztlich auch ihrer Arbeit zugute kommt.

Es ist daher zu begrüßen, daß die Innenminister in den KpS-Richtlinien für die Ausübung des Ermessens bei der Auskunfterteilung eine Regelung getroffen haben, die sowohl den Datenschutzbelangen der Betroffenen als auch der Aufgabenerfüllung der Polizei Rechnung trägt. Danach wird Auskunft erteilt, ob und gegebenenfalls welche Unterlagen vorhanden sind, es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen.

Ich begrüße ausdrücklich, daß sich in meinem Zuständigkeitsbereich eine datenschutzfreundliche Auskunftspraxis der Polizei eingespielt hat, wobei auf die Unterstützung durch den Innenminister besonders hinzuweisen ist. Zu Beginn meiner Tätigkeit war in zahlreichen Fällen die Einschaltung des Landesbeauftragten für den Datenschutz notwendig, um die Polizeibehörden zur Auskunfterteilung zu veranlassen; nur in wenigen Fällen erwies sich die Auskunftsverweigerung als gerechtfertigt. In letzter Zeit ist die Zahl der Eingaben wegen Ablehnung der Auskunfterteilung stark zurückgegangen.

Nach dem Datenschutzgesetz hat ein Betroffener Anspruch auf Sperrung oder Löschung der zu seiner Person gespeicherten Daten, wenn ihre Kenntnis zur rechtmäßigen Aufgabenerfüllung nicht mehr erforderlich ist. Für den Bereich der Kriminalpolizeilichen personenbezogenen Sammlungen ist diese Generalklausel in den KpS-Richtlinien konkretisiert worden.

Die in den KpS-Richtlinien vorgesehenen Regellöschungsfristen beruhen auf einer verallgemeinernden Interessenabwägung. In Fällen von geringer Bedeutung ist eine Abkürzung der Regelfrist vorgesehen. Möglich ist aber auch eine Verlängerung, wenn Wiederholungsgefahr besteht oder andere schwerwiegende Gründe dieses gebieten. Darüber hinaus wird in den Richtlinien festgelegt, unter welchen Voraussetzungen im Rahmen laufender Sachbearbeitung auf jeden Fall zu löschen ist. So etwa dann, wenn die Ermittlungen oder eine der Polizei bekannte Entscheidung der Staatsanwaltschaft oder eines Gerichtes ergeben, daß der Betroffene die ihm vorgeworfene Tat nicht begangen hat oder kein begründeter

Tatverdacht mehr besteht. Dies setzt allerdings voraus, daß die Justiz die Polizei stets in dem erforderlichen Umfang über den Ausgang von Straf- und Ermittlungsverfahren unterrichtet.

Soweit ich bei Löschungsanträgen eingeschaltet war, konnte in der Mehrzahl der Fälle eine Löschung erreicht werden. In den Fällen, in denen datenschutzrechtlich nicht zu beanstanden war, daß sich Polizeibehörden dazu noch nicht in der Lage sahen, ist mir von den betreffenden Polizeibehörden eine erneute Prüfung der vorzeitigen Löschung nach angemessener Frist zugesagt worden. Insoweit bestehen in meinem Zuständigkeitsbereich keine grundsätzlichen Konflikte zwischen Polizei und Datenschutz.

Schwierigkeiten bereitet allerdings die Regelaussonderung, insbesondere die Bereinigung der Altbestände. Eine generelle Bereinigung bei allen Polizeibehörden hat noch nicht stattgefunden. Sie ist nach Auffassung der Polizeibehörden wegen des Umfangs der zu überprüfenden Bestände mit dem vorhandenen Personal kurzfristig nicht möglich, ohne die Erfüllung der Aufgaben zu gefährden. Ich habe allerdings Zweifel, ob diese Aussage immer zutrifft. Dabei sollte auch berücksichtigt werden, daß die Aussonderung eine Befreiung von unnötigem Ballast bedeutet und damit in vielen Fällen die Arbeitsbedingungen der Behörden verbessert.

Spätestens bei der Relevanzprüfung für die Einstellung in den KAN muß auch geprüft werden, ob eine Kriminalakte nach den KpS-Richtlinien auszusondern ist. Darüber hinaus müssen, soweit noch nicht geschehen, für die automatisierten Informationssysteme Laufzeitüberwachungen entwickelt werden. In Nordrhein-Westfalen ist mit der Realisierung im nächsten Jahr zu rechnen.

Das eingangs erwähnte Spannungsverhältnis zwischen Aufgabenerfüllung und Datenschutz bringt es mit sich, daß Verwaltung und Datenschutzbeauftragte den einander gegenüberstehenden Rechtsgütern unterschiedliches Gewicht beimessen. Beide haben jedoch die vom Gesetzgeber getroffenen Entscheidungen zu respektieren. Sofern das geltende Recht zu unbefriedigenden Ergebnissen führen sollte, muß der Gesetzgeber erneut entscheiden. Bis dahin ist das derzeit geltende Recht für alle Beteiligten bindend.

Zu der Bemerkung von Dr. Boge, die Verwendung juristischer Techniken diene nicht der Versachlichung der Diskussion: Die unabhängigen und nur dem Gesetz unterworfenen Datenschutzbeauftragten haben das Gesetz nach ihrer Rechtsüberzeugung auszulegen. Dabei bedienen wir uns der Auslegungsmethoden, die von der Rechtsprechung entwickelt oder anerkannt worden sind. Wenn wir dabei Wertvorstellungen

einfließen lassen, so sind es diejenigen, die das Bundesverfassungsgericht zu den Grundrechten auf Schutz der Menschenwürde und freie Entfaltung der Persönlichkeit sowie zu dem auf dem Rechtsstaatsprinzip beruhenden Verhältnismäßigkeitsgrundsatz formuliert hat. Ich meine allerdings, daß diese Wertvorstellungen für uns alle verbindlich sein sollten.

K. Bux

Die Datenschutzgesetze des Bundes und der Länder sind jetzt ungefähr vier Jahre in Kraft, die KpS-Richtlinien als Konkretisierung dieses Gesetzes für den Polizeibereich im Lande Baden-Württemberg 1 1/2 Jahre, in anderen Ländern etwa zwei Jahre. Wenn man berücksichtigt, welche Emotionen, welche politischen Diskussionen und welche unterschiedlichen Standpunkte zwischen dem Datenschutz und dem Sicherheitsbedürfnis bei Entstehung der Gesetze und der Richtlinien vertreten worden sind, sollte man ruhig schon jetzt eine Bilanz ziehen. Ich sehe meine Rolle hier auf dem Podium darin, aus der Sicht des Praktikers zu diesen Problemen Stellung zu nehmen.

Ich habe mich mit Kriminalisten in den unterschiedlichsten Funktionen unterhalten und sie nach Vor- und Nachteilen befragt. Als Ergebnis ist festzustellen, daß die Polizei dieser Bundesrepublik insgesamt den Datenschutz angenommen hat und in weiten Bereichen von der Notwendigkeit des Datenschutzes überzeugt ist. Die Polizei hat erkannt, daß durch den Datenschutz auch Sicherheitsinteressen verwirklicht werden. Als vorteilhaft wurde empfunden, daß wir tatsächlich von viel Makulatur befreit wurden; ohne den Druck der Öffentlichkeit und ohne den Druck der Datenschutzbeauftragten hätten wir uns nicht mit so viel Mühe und so rasch daran gemacht, unsere Archive zu durchforsten. Wir glauben auch, daß es sachgerecht war, die Ermittlungsergebnisse nicht mehr ungezielt an die verschiedenen Behörden und Dienststellen zu steuern. Während früher häufig Fernschreiben mit personenbezogenen Daten "an alle" gerichtet worden sind, ist die Polizei heute vorsichtiger und sensibler geworden. Wir begrüßen auch, daß als Ergebnis der öffentlichen Diskussion die Möglichkeit Dritter, Daten von der Polizei zu erhalten, weiter eingeschränkt worden ist. Schließlich haben wir in Baden-Württemberg mit Unterstützung der Landesbeauftragten für den Datenschutz es erreicht, daß die Justiz verpflichtet ist, in vollem Umfang die Polizei über den Ausgang des Verfahrens zu unterrichten durch Übersendung der Einstellungsverfügungen und Urteile mit voller Begründung, was uns sachgerechtere Entscheidungen über die Aufbewahrung von Daten und Akten ermöglicht.

Zu dem Problem des Datenschutzes im Bereich der Polizei sind aber auch sehr kritische Anmerkungen gemacht worden. Übereinstimmend wurde vermerkt, daß die tägliche Arbeit der Polizei durch eine Überinterpretation des Datenschutzgedankens in der Öffentlichkeit erschwert worden ist. So wurden z.B. Polizeibeamte, die nach einem Unfall ins Krankenhaus gingen, um die Personalien des Unfallopfers zu erfahren, abgewiesen mit dem Hinweis auf den Datenschutz. Kriminalbeamte, die im Krankenhaus die Personalien einer Krankenschwester feststellen wollten, weil diese eine Patientin betreut hat, während ihr ein wertvoller Ring gestohlen worden ist, erhielten keine Auskunft unter Berufung auf den Datenschutz. Eine Kriminalbeamtin, die in einer Schule nach Anschriften von Mitschülern eines vermißten Mädchens fragte, erhielt keine Auskunft, weil der Schulleiter datenschutzrechtliche Bedenken dagegen hatte.

Ich könnte diese Beispiele beliebig forsetzen. Alle Auskünfte waren rechtlich gesehen zulässig; ihre Ablehnung deutet auf eine erhebliche Verunsicherung der Öffentlichkeit hin. Diese Unsicherheit ist unseres Erachtens durch die erregte Diskussion in der Öffentlichkeit über den Datenschutz entstanden, wobei die Datenschutzbeauftragten des Bundes und der Länder hier z.T. durch zumindest mißverständliche Formulierungen in ihren Datenschutzberichten beigetragen haben. Gerade die in diesen Berichten häufig zum Ausdruck gebrachte Behauptung eines rechtswidrigen Verhaltens der Polizei im Hinblick auf die Beachtung der Datenschutzbestimmungen hat Behördenleiter und Funktionäre verunsichert. Auch sie möchten natürlich nicht an den Pranger gestellt werden und entscheiden sich im Zweifelsfalle, und solche gibt es im Datenschutzrecht verhältnismäßig viele, gegen eine Auskunft.
Wir von der Polizei sind einhellig der Auffassung, daß es gelingen muß, auch in der Öffentlichkeit die Dinge wieder in das rechte Lot zu bringen, damit die Verunsicherung und damit die Erschwerung der täglichen Polizeiarbeit einigermaßen abgebaut wird. Das kann aus unserer Sicht nur dadurch geschehen, daß diese Probleme weniger mit Schlagzeilen in der Öffentlichkeit diskutiert, sondern Sachprobleme mehr im Detail erörtert werden.

Kritische Anmerkungen werden auch von polizeilichen Praktikern zu den von den Datenschützern hier so lobend erwähnten KpS-Richtlinien gemacht. Diese Richtlinien enthalten zwei Regelungsbereiche, die nach wie vor als problematisch anzusehen sind. Es handelt sich dabei um die Aussonderungsbestimmungen und die Regelaussonderungsfristen. Nach den Datenschutzgesetzen ist dem Betroffenen grundsätzlich Auskunft zu erteilen, welche Daten über ihn gespeichert sind. Diese bindende Verpflichtung gilt jedoch ausdrücklich nicht für die Polizei. Insoweit ist vielmehr nach pflichtgemäßem Ermessen zu entscheiden, ob im Einzelfall Auskunft erteilt wird. Die KpS-Richtlinien bestimmen

in Ausfüllung dieses Ermessensspielraumes, daß dem Betroffenen Auskunft über gespeicherte Daten erteilt wird, es sei denn, daß die Belange des Bürgers hinter dem öffentlichen Interesse an dem Unterbleiben der Auskunft zurücktreten müssen. Diese Regelung ermöglicht nach den polizeilichen Erfahrungen eine Ausforschung der Polizei durch den meistens anwaltschaftlich beratenen Straftäter.
Zwar kann die Auskunft verweigert werden, wenn der Ausforschungszweck offenbar wird. Es brauchen dem Betroffenen dann keine Einzelerkenntnisse mitgeteilt zu werden. Der Betroffene kann allerdings oft gerade aus der Verweigerung der Auskunft schließen, daß bei der Polizei des Landes Erkenntnisse über ihn vorhanden sein müssen und sich darauf einstellen. In vielen Fällen ist das Ausforschungsziel jedoch nicht völlig sicher zu erkennen. Da dann kein Ablehnungsgrund vorliegt, wird Auskunft erteilt und damit die angestrebte Ausforschung verwirklicht. Dies ist nicht nur der Fall, wenn dem Anfragenden die über ihn bei der Polizei vorliegenden Erkenntnisse mitgeteilt werden. Schwerwiegender sind die Fälle, in denen der Straftäter durch eine Negativauskunft erfährt, daß die Polizei keine Erkenntnisse über ihn hat, wodurch er in seinem kriminellen Wirken bestärkt werden kann. Auch eine Pflicht, Auskunftersuchen zu begründen, würde an dieser Situation nichts ändern, da nur vorgeschobene Begründungen nicht widerlegt werden könnten.

Bei der Entscheidung, ob die Polizei zur Auskunft verpflichtet werden soll, ist abzuwägen zwischen dem legalen Informationsinteresse des Bürgers und dem Sicherheitsinteresse des Staates, das durch die Eröffnung von Ausforschungsmöglichkeiten über das polizeiliche Wissen durch den Straftäter sowohl im präventiven als auch im repressiven Bereich erheblich gemindert wird. Ich glaube, daß das Informationsbedürfnis des Bundesbürgers auf Übermittlung der über ihn gespeicherten polizeilichen Erkenntnisse viel geringer ist als das schlechthin angenommen wird. Vor der Eröffnung der Diskussion über den Datenschutz ging beim Landeskriminalamt Baden-Württemberg nicht eine Anfrage auf eine entsprechende Auskunft ein. Nachdem die Disskussion in der Öffentlichkeit erfolgt ist und wiederholt der Bundesbürger aufgefordert wurde, bei der Polizei doch entsprechende Nachfrage zu halten, sind ungefähr 800 solcher Anfragen eingegangen. Davon haben wir in ca. 220 Fällen die Auskunft wegen einer vermuteten Ausforschung verweigert. Die verbleibende Anzahl der Auskunftersuchen, die nebenbei nach abebben der öffentlichen Diskussion im Sinken begriffen ist, rechtfertigt m.E. das Bedürfnis auf Verpflichtung zur Auskunftserteilung dann nicht, wenn berücksichtigt wird, daß gerade Straftäter aus dem Bereich der organisierten Kriminalität und des Rauschgifthandels sich diese Auskunftsverpflichtung zunutze machen. Im Ergebnis

wird gerade im Bereich dieser Kriminalitätsart die präventive Wirkung gegen diese Straftäter durch die Ausforschbarmachung und damit durch die Berechenbarkeit einer möglichen polizeilichen Reaktion erheblich minimiert. Wir haben Anzeichen dafür, daß diese Ausforschung unter Zuhilfenahme bestimmter Anwaltsbüros bereits systematisch betrieben wird. Ich bin daher der Auffassung, daß sehr genau überlegt werden sollte, ob diese Art der Auskunftsverpflichtung der Polizei an den Betroffenen, die in den KpS-Richtlinien normiert ist, aufrechterhalten werden sollte oder ob man es nicht einfach bei dem ausdrücklichen Gebot des Gesetzgebers, wonach die Polizei zur Auskunftserteilung nicht verpflichtet ist, bewenden lassen sollte.

Der zweite Regelungsbereich der KpS-Richtlinien betrifft die Regelaussonderungsfristen. Die KpS-Richtlinien sehen eine regelmäßige Löschungsfrist von 10 Jahren bei Erwachsenen und von fünf Jahren bei Jugendlichen vor. Vor Inkrafttreten der KpS-Richtlinien betrug die Löschungsfrist 25 Jahre. Wenn ich die Entstehungsgeschichte der KpS-Richtlinien richtig sehe, dann sind die Entscheidungsgremien zu diesen Fristen gekommen ohne dafür eine echte analytische Basis zu haben. Nach meinen Informationen wird im Vollzug der KpS-Richtlinien und der damit verbundenen Vernichtung der Kriminalakten von vielen Kriminalisten die Befürchtung geäußert, daß durch die Vernichtung der Akten nach relativ kurzen Fristen wichtiges polizeiliches Informationsmaterial verlorengeht. Wir in Baden-Württemberg sind einmal diesem Verdacht nachgegangen. Im Rahmen einer programmierten Vernichtungsaktion über unser PAD-Verfahren haben wir im Bereich der Polizeidirektion Esslingen mit unserem System 1000 Wiederholungstäter ausdrucken lassen. Bei der Überprüfung dieser Ausdrucke stellten wir fest, daß in 109 Fällen die erfaßten jugendlichen Straftäter erst nach Ablauf von fünf Jahren wieder polizeilich in Erscheinung getreten waren. Hätten früher die KpS-Richtlinien in der jetzigen Form bestanden, wären in diesen 109 Fällen also die Akten bereits vernichtet gewesen, bevor eine Wiederholungstat der Polizei bekannt geworden ist.

Das Ergebnis dieser Überprüfung ist sicher nicht repräsentativ. Es könnte uns jedoch veranlassen darüber nachzudenken, ob die Fünfjahresfrist bei jugendlichen Straftätern tatsächlich sachgerecht ist.

Eine weitere Überlegung führt zu demselben Ergebnis:
Seit dem Jahre 1973 erfassen wir in einem automatisierten Verfahren sämtliche Strafanzeigen im sogenannten PAD-System. Nach Inkrafttreten der KpS-Richtlinien haben wir, durch ein entsprechendes Programm, sämtliche erfaßten Strafanzeigen, die fünf bzw. zehn Jahre zurücklagen und

bei denen in der Zwischenzeit kein weiterer Anzeigenvorgang vermerkt wurde, ausgedruckt und dem kriminalpolizeilichen Sachbearbeiter zur Prüfung der Frage, ob entsprechend den KpS-Richtlinien die Akten zu vernichten sind oder eine Verlängerung anzuordnen war, zugeleitet. Diese Prüfung wurde in 58.000 Fällen eingeleitet. In 51.000 Fällen wurde die Vernichtung der Akten angeordnet, in 7000 Fällen wurde die Aufbewahrungsfrist der Akten verlängert. Die Herbeiführung dieser Entscheidung über eine mögliche Verlängerung der Aufbewahrungsfrist stellt einen ganz erheblichen Arbeitsaufwand dar, muß doch in jedem Fall in sämtlichen Systemen und Karteien und Dateien geprüft werden, ob in der Zwischenzeit Erkenntnisse angefallen sind, die eine Verlängerung der Aufbewahrung rechtfertigen. Die Tatsache, daß in 7000 Fällen eine Verlängerung der Aufbewahrung angeordnet werden mußte, obwohl die entsprechende Person für die Dauer der regelmäßigen Aufbewahrungsfrist in Baden-Württemberg nicht mehr strafrechtlich in Erscheinung getreten ist, begründet m.E. ebenfalls die Vermutung, daß die Fristen zu kurz angesetzt sind. Bei einer Verlängerung der Aufbewahrungsfrist würde einmal das wichtige polizeiliche Informationsmaterial länger zur Verfügung stehen und so die Position der Polizei bei der Verbrechensbekämpfung verbessern. Auch wäre der immense Arbeitsaufwand, der mit der Vernichtung der Kriminalakten innerhalb der gesetzten Frist verbunden ist, dann erheblich zu reduzieren, wenn längere Fristen zur Verfügung stünden, weil damit auch die Vermutung, daß der betreffende Straftäter nicht mehr kriminell in Erscheinung tritt, erhärtet werden könnte, was eine Reduzierung des Arbeitsaufwandes bei der Überprüfung rechtfertigen könnte.
Ich meine, die Ansatzpunkte in Esslingen und eine Würdigung der zuvor genannten Zahlen sollten für uns Anlaß sein, einmal in eine analytische Prüfung einzutreten, ob die durch die KpS-Richtlinien vorgegebenen Fristen sich als richtig erwiesen haben, oder ob wir uns nicht wertvollen Informationsmaterials begeben, das die Möglichkeit zur Bekämpfung einer sich in Qualität und Quantität steigernden Kriminalität verbessert.

Schließlich wurde ich von den Praktikern noch auf einen vierten Problemkreis hingewiesen. Er betrifft die Abgrenzung der Kontrollbefugnis des Landesbeauftragten für den Datenschutz gegenüber der Polizei. Lassen Sie mich dieses Problem an dem Beispiel des bundesweit einzuführenden Kriminalaktennachweises (KAN) deutlich machen. Man wird in der Zukunft unterscheiden zwischen einem zentralen und einem dezentralen KAN. Das bedeutet, daß der zentrale, beim Bundeskriminalamt zu führende Kriminalaktennachweis nur unter bestimmten Voraussetzungen oder mit bestimmten Straftaten beschickt werden darf: bei Verbrechen oder Vergehen, die in § 100a StPO aufgeführt sind und ferner bei Straftaten, die gewohnheitsmäßig, gewerbsmäßig, überörtlich u.a.m., begangen worden sind. Es wird also in Zukunft

der polizeiliche Sachbearbeiter entscheiden müssen, ob ein Straftäter gewohnheitsmäßig, gewerbsmäßig usw. gehandelt hat. Diese Entscheidung ist sehr schwierig. Bei einer extensiven Kontrolle durch den Datenschutzbeauftragten müßte diese Sachentscheidung gegebenenfalls im Einzelfall belegt werden, was bei der Vielzahl der Straftaten einen immensen Arbeitsaufwand erwarten läßt. Ich bin der Meinung, daß man über die verschiedenen Probleme der Praxis mit den Datenschutzbeauftragten des Bundes und der Länder reden sollte. Dabei sollten Einzelprobleme getrennt diskutiert und die Bedürfnisse des Datenschutzes jeweils gegeneinander abgewogen werden. Vielleicht würde man auf diese Weise da und dort zu gerechtfertigten Korrekturen im Interesse der Sicherheit dieser Bundesrepublik kommen.

H. Boge

Ich habe eineinhalb Jahre lang versucht, das Thema Datenschutz auf den Boden der Wirklichkeit herunterzuholen. Sie haben sich vielleicht gewundert und manchmal auch gefragt, warum des Amt sich nicht zu diesen Fragen äußert. Dies ist ganz bewußt geschehen aus der Befürchtung heraus, in der Öffentlichkeit könne es falsch aufgefaßt werden, wenn dieses Thema immer wieder neu aufgelegt wird. Ich bin aber enttäuscht worden, weil mein Gegenüber nicht mitgezogen hat - ob bewußt oder unbewußt, lasse ich offen. Sicher ist der Datenschutzbericht eine Sache, die öffentlich behandelt werden muß. Aber dann bekomme ich gelegentlich Zeitungsausschnitte - beispielsweise von seiten einer Gewerkschaft - mit der Überschrift "Verfassungsschutz und Polizei speichern Daten rechtswidrig". Damit sind alle Bemühungen vergeblich. Natürlich kann auch der Referent falsch zitiert oder ausgelegt worden sein, aber dies hat in der Öffentlichkeit dazu geführt, daß man uns sehr kritisch gegenübersteht.

Herr Bull hat von den Schwierigkeiten in der Zusammenarbeit mit Behörden oder behördenähnlichen Einrichtungen gesprochen. Es ergeben sich aber auch Probleme im eigenen Bereich. Wenn ich Überlegungen über ein bestimmtes Konzept anstelle, kommt es vor, daß Mitarbeiter mir sagen: das ist müßig, das müssen wir gleich aufgeben, da tritt sofort der Datenschutzbeauftragte auf den Plan. Ob dies im Einzelfall eine Behauptung ist oder einer tatsächlichen Überzeugung entstammt, kann ich hier offenlassen. Jedenfalls ist dies die Stimmungslage. Draußen bei den Bürgern ist offensichtlich der Eindruck entstanden - ob bewußt gesteuert oder als Ergebnis der Diskussion -, die Polizei speichere in Sammelwut permanent Daten. Hiermit kann man sich auseinandersetzen. Wenn der Eindruck entsteht, wir würden permanent mit den Daten Mißbrauch betreiben, dann wird unser Verhältnis zur Öffentlichkeit ganz wesentlich belastet - und wir sind darauf angewiesen, ein gutes Verhältnis zur Öffentlichkeit zu haben.

Ich möchte noch eine Bemerkung zur Frage des Dialogs und der Interpretation anfügen. Bei meinen Besprechungen mit Vertretern des Datenschutzes über Fragen der Rechtsinterpretation habe ich es noch nie erlebt, daß mein Gegenüber gesagt hat: in diesem Punkt haben Sie recht. Vielmehr wird immer gesagt: das ist falsch, das ist unzulässig. Im Einzelfall liegt dem wohl auch eine eigene Interpretation zugrunde, denn ich glaube nicht, daß ein Datenschutzbeauftragter einen solchen Absolutheitsanspruch erheben kann, daß er allein die Weisheit besitze. Wie Sie wissen, kann man in der Rechtsmaterie über manches streiten und wir haben ja gehört, daß es sich um eine Rechtsmaterie handelt. Und dann kommt - und Herr Bull hat mich ja gebeten, konkret zu werden - der Hinweis: Ich bitte Sie, dies zu bereinigen, ich bitte Sie, die Beamten entsprechend

einzuweisen; wenn dies nicht geschieht, muß ich das Thema in den nächsten Datenschutzbericht aufnehmen. Das ist Nötigung. Wenn ich dann sage, daß wir bereits dabei sind, daß wir uns die größte Mühe geben und 30, 50, bis zu 100 Bedienstete des Amtes eingesetzt sind, um zu bereinigen, um diese Unebenheiten auszugleichen, da wir ja wissen, daß wir verschmutzte Bestände haben, dann höre ich: Das ist nicht meine Angelegenheit, machen Sie das mit Ihrem Ministerium klar. So ist die Situation, und das belastet natürlich das Verhältnis im Grundsätzlichen, und das schlägt tief durch. Ich war angenehm überrascht, als Herr Weyer sagte, er habe keine Konfliktfelder mit der Polizei. Vielleicht in bestimmten Bereichen, aber nicht im Grundlegenden. Entweder ist es auf Bundesebene nicht so, wie man es erwarten darf, oder dort ist etwas nicht in Ordnung.

H. P. Bull

Ich hatte die Absicht, auf Herrn Bux einzugehen, weil mir sein Beitrag in ganz besonderer und auffälliger Weise wert schien, hervorgehoben zu werden als nüchtern, sachlich, konkret - genau der Ansatz, auf dem man die Diskussion nach meiner Vorstellung und nicht erst seit heute führen sollte. Ich will jetzt nicht auf die einzelnen Punkte eingehen. Zu manchen Sachaussagen von Herrn Bux kann man sicher auch eine andere Meinung vertreten. Ich werde mich hiermit jetzt nicht näher befassen, da Sie alle offenbar erwarten, daß ich auf die Äußerungen von Herrn Boge stärker eingehe, wenn dies auch gegen meine Absicht ist und gegen das Konzept, das eigentlich mit dieser Tagung verfolgt wird, nämlich über Sachprobleme zu reden. Ich habe auch keinen Anlaß, hier meine Verhaltensweise in den letzten 5 Jahren oder seit Herrn Boges Amtsantritt zu rechtfertigen. Ich bestreite, daß ich kompromißunwillig gewesen sei. Es ist nicht richtig, und andere wissen das auch, daß ich nicht zum Gespräch bereit gewesen wäre. Im Gegenteil, ich habe versucht, dieses Gespräch gerade mit Herrn Boge zu führen. Leider ist es in der Form, die ich mir gewünscht hätte, nämlich über das Vorverständnis, über die Mißverständnisse und auch über die Stimmungslage zu sprechen, nicht zustandegekommen. Mir scheint es auch nicht möglich, in diesem Saal vor den Augen und Ohren der Interessierten über die Stimmung und die Bewußtseins- und Seelenlage des einen wie des anderen zu reden. Dies müßte in einem anderen Raum und zu anderer Zeit geschehen.

Ich möchte nur meine Enttäuschung darüber ausdrücken, daß immer noch nicht verstanden wird, welche Aufgabe wir wahrzunehmen haben und daß es hier um rechtliche, um verfassungsrechtliche und verwaltungsrechtliche Fragen geht, und daß immer noch nicht begriffen wird, daß der Gebrauch des Begriffs "rechtswidrig" für uns Juristen unverzichtbar ist. Wenn gesagt wird, wir sollten solche Begriffe in der Öffentlichkeit besser nicht verwenden, dann kann ich nur

erwidern, es hieße ja wohl den Teufel mit Beelzebub austreiben, wenn man ein vermutetes Mißverständnis in der Öffentlichkeit mit einer bewußt falschen Ausdrucksweise, einem Abgehen von dem klaren juristischen Begriff bekämpfen wollte. Statt über die unrichtige Bewertung korrekter Formulierungen zu streiten oder zu spekulieren, sollten alle Beteiligten alle mögliche Mühe darauf verwenden, das jeweils Gemeinte zu erläutern und gerade denen zu erläutern, die es falsch verstehen könnten. Ich tue dies. Wenn ein Zeitungsaufsatz, ein Interview oder ein Artikel über unsere Tätigkeit überschrieben ist mit den Worten "Verfassungsschutz und Polizei speichern Daten rechtswidrig", dann ist das doch richtig, denn es gibt ja solche Fälle. Wir haben hierfür intern in vielfältiger Weise die Belege gebracht und dann schließlich - in sehr abgemilderter Form - in den Tätigkeitsberichten. Dies kann uns keiner verwehren, und es ist ja wohl, wie auch Ihr Lachen bewiesen hat, eine etwas eigenartige Vorstellung, hier den strafrechtlichen Begriff der Nötigung einzuführen. Wenn wir etwas nicht hart und ohne Rücksicht beanstanden, sondern zur Diskussion bereit sind und Ihre Meinung dazu hören wollen, dann setzen wir uns ja damit auseinander und wollen wissen, ob das, was wir in einem Entwurf verfaßt haben, so richtig ist. Wir verhalten uns in vielen Zusammenhängen so, daß wir Entwürfe den angesprochenen Stellen zur Verfügung stellen und hinzufügen: Wenn Sie darauf nicht eingehen können, wenn Sie das nicht von sich aus schon bereinigen wollen, dann müssen wir das dem Bundestag berichten. Es ist unsere gesetzliche Pflicht, zu berichten, wir haben gar keine Wahl. Herr Wernitz hat soeben zu Recht betont, daß er als Abgeordneter entscheidenden Wert darauf legt, umfassend informiert zu werden. Von Sammelwut und dergleichen mehr habe ich nie gesprochen, und wenn der Eindruck entsteht, daß die Polizei ständig Mißbrauch betreibe, dann rechnen Sie das bitte nicht uns zu. Jeder, der zu lesen versteht, kann meine mündlichen oder schriftlichen Äußerungen, wie sie in der Presse oder sonstwo wiedergegeben sind, nachlesen. Dort werden Sie derartige Äußerungen nicht finden. Herr Herold hat mir seinerzeit freundliche Briefe geschrieben, als ich mich gegen eine in der Tagespresse vertretene Meinung gewandt habe, die Bundesrepublik sei ein Überwachungsstaat und hinter jedem stünde bereits ein Polizist. Ich habe seinerzeit einem Menschen gegenüber, der in manchen Dingen mit mir übereinstimmt und mit dem ich viele Meinungen teile, öffentlich eine sehr deutliche Erklärung zugunsten der Polizei abgeben. Das wird gerne vergessen, wenn bei Gelegenheiten wie der heutigen über die traurige Lage der Polizei nachgedacht wird.

Ich kann auch nicht umhin, Ihnen zu sagen - wohl wissend, daß ich hier keinen Beifall bekommen werde -, daß dies von seiten der Polizei eine Wehleidigkeit ist, die ihr gar nicht gut ansteht, die einer selbstbewußten, rechtsstaatlich denkenden Polizei nicht gut tut. Sie werden auch das Vertrauen in der Öffentlichkeit nicht verbessern, wenn Sie

immer wieder sagen, die bösen Datenschutzbeauftragten kritisierten zu viel. In der Öffentlichkeit wird man daraus den Schluß ziehen, daß Sie auf die eigentlichen Probleme nicht eingehen, daß Sie ausweichen wollen. Ich selbst sage das ja gar nicht, aber so wird es verstanden werden. Es trifft auch nicht zu, daß die Anlässe für öffentliche Diskussionen immer von uns geliefert werden. Erinnern Sie sich doch bitte daran, wer im Laufe dieses Jahres - von der Veröffentlichung des Tätigkeitsberichtes abgesehen - die Diskussion um den Datenschutz bei den Sicherheitsbehörden wieder besonders angeheizt hat, und zwar in einer Weise, die vielleicht wiederum den Sicherheitsbehörden in der Öffentlichkeit Minuspunkte eingebracht hat: es war der Herr Generalbundesanwalt.

H. Weyer

Ich möchte Herrn Boge insoweit widersprechen, als ich nicht gesagt habe, ich hätte keine Konflikte mit der Polizei im Lande Nordrhein-Westfalen. Ich habe vielmehr gesagt, daß in den Bereichen der Auskunfterteilung und der individuellen Löschung keine grundsätzlichen Konflikte bestehen. Zugleich habe ich erklärt, daß ich den Stand der Regelaussonderung und der Bereinigung der Altbestände nicht für zufriedenstellend und noch nicht für im Einklang mit den geltenden Vorschriften stehend halte. Es gibt auch noch andere Meinungsverschiedenheiten. Die Vertreter des Innenministeriums Nordrhein-Westfalen wissen dies. Ich kann in dieser kurzen Diskussion auf diese Felder nicht in allen Einzelheiten eingehen.

Zur Frage des Absolutheitsanspruches der Datenschutzbeauftragten: Ich glaube, daß kein Datenschutzbeauftragter einen solchen Anspruch geltend macht. Er ist jedoch von Gesetzes wegen dazu verpflichtet, seine Rechtsüberzeugung zum Ausdruck zu bringen. Natürlich kann ein Datenschutzbeauftragter sich auch irren. Ebenso kann eine oberste Landesbehörde, die in der Auslegung des Gesetzes die letztlich für die Polizei verbindlichen Weisungen erteilt oder beim Bund die zuständige oberste Bundesbehörde sich irren. Verbindlich können nur die Gerichte über die Auslegung einer Datenschutzvorschrift entscheiden. Die allerdings hören dann beide Seiten - sowohl die Datenschutzbeauftragten als auch die Exekutive. Ich habe den Eindruck, daß das, was die Datenschutzbeauftragten bisher zum Ausdruck gebracht haben, in der Mehrzahl der Fälle die Billigung der Gerichte gefunden hat, wenn es im Einzelfall einmal zu einem Streit gekommen ist. Wir stützen uns in unserer Motivation eben im wesentlichen auf die Rechtsprechung insbesondere des Bundesverfassungsgerichts zu bestimmten Grundrechten und zum Verhältnismäßigkeitsgrundsatz.

Ich möchte noch kurz auf die Ausführungen von Herrn Bux eingehen. Hier sehe ich einen Meinungsunterschied in der Frage der Auskunfterteilung und in der Frage der Löschung. Ich kann nicht akzeptieren, daß die Verweigerung der Auskunft über die Datenspeicherung ein legitimes Instrument der Abschreckung von Kriminellen ist. Dies findet m.E. im geltenden Recht keine Grundlage. Ebensowenig kann ich akzeptieren, daß das Interesse der Bürger, Auskunft zu erhalten, deswegen als minimal eingestuft wird, weil im Lande Baden-Württemberg nur 800 Personen von diesem Recht Gebrauch gemacht haben. Die Möglichkeit, dieses Recht in Anspruch zu nehmen, gibt aber weiteren Hunderten oder Tausenden von Bürgern die Sicherheit und das Gefühl, daß bei der Polizei alles in Ordnung ist und die Rechtmäßigkeit notfalls auch kontrolliert werden kann. Deshalb muß m.E. die Auskunfterteilung weiterhin so geregelt werden oder geregelt bleiben, wie die KpS-Richtlinien dies vorsehen. Ich kann hier auch keinen Gegensatz zu den Vorschriften der Landesdatenschutzgesetze über die Auskunfterteilung erkennen. Diese besagen nur, daß Auskunft nach pflichtgemäßem Ermessen zu erteilen ist, und die oberste Bundes- oder Landesbehörde hat zweifellos das Recht, dieses pflichtgemäße Ermessen näher zu begrenzen. Von dieser Möglichkeit hat sie Gebrauch gemacht.

Nun zur Frage der Löschung: Herr Bux hält die Fristen für zu kurz. Ich möchte nur darauf aufmerksam machen, daß in der Rechtsprechung eine gegenteilige Tendenz zu erkennen ist. In einem Urteil des Hessischen Verwaltungsgerichtshofs vom 13. September 1982 heißt es, daß möglicherweise die 10-Jahres-Frist zu lang bemessen ist. Wir haben nun die 10-Jahres-Frist und wir sollten die nächsten 5 Jahre einmal ausprobieren, wie sie sich bewährt. Auf keinen Fall kann ich den Gesichtspunkt der Arbeitsaufwendigkeit anerkennen, wenn es um die Frage der Löschung geht. Sie können nicht sagen, weil es zu arbeitsaufwendig ist, die Vorgänge zu überprüfen, deshalb müssen die 88% der Bürger, bei denen Sie gelöscht haben, auf diese Löschung verzichten und es hinnehmen, daß ihre Daten 25 Jahre bei der Polizei gespeichert werden. Ich weise in diesem Zusammenhang darauf hin, daß das Bundesverwaltungsgericht bereits 1967, also lange bevor es den Begriff Datenschutz gab, anerkannt hat, daß die persönliche Sphäre des Betroffenen - ich zitiere jetzt wörtlich - schon allein wegen des Bewußtseins stark berührt werden kann, von der Kriminalpolizei als möglicher Rechtsbrecher betrachtet zu werden. Seinerzeit ging es um die Aufbewahrung erkennungsdienstlicher Unterlagen. Man kann es bereits als gefestigte Rechtsprechung der Verwaltungsgerichte sehen, daß hier berechtigte Interessen der Bürger an der Nichtaufbewahrung vorliegen; deshalb kann man den Arbeitsaufwand nicht als entscheidendes Gegenargument in die Debatte einführen.

P. Laufs

Ich möchte zunächst das aufgreifen, was Herr Bull über die klaren juristischen Begriffe gesagt hat. Selbstverständlich müssen Verwaltungshandlungen sich am geltenden Recht messen lassen. Nun gibt es im Rahmen des Datenschutzrechts eine Fülle neuer unbestimmter Rechtsbegriffe wie z.B. berechtigtes oder überwiegend berechtigtes Interesse, schutzwürdige Belange, rechtmäßige Erfüllung der in der Zuständigkeit liegenden Aufgaben einer öffentlichen Stelle usw. All diese Begriffe sind auslegungsbedürftig, wobei uns die Rechtsprechung bisher sehr wenig geholfen hat, da dort nur eine geringe Zahl von Konflikten ausgetragen worden ist. Daß es bei der Auslegung der Begriffe durch die Betroffenen zu großen Differenzen kommt, kann niemanden überraschen. Herr Bux hat hier sehr anschaulich von Überreaktionen und Überinterpretationen gesprochen und es ist in der Tat zu bedauern, daß in vielen Fällen aus einem überzogenen, falschen Datenschutzverständnis heraus rechtlich zulässige und sachlich erforderliche Amtshilfe nicht geleistet worden ist. So sind polizeiliche Ermittlungsverfahren z.B. im Zusammenhang mit illegalem Waffenhandel, Diebstahl, Brandstiftung und anderen Delikten behindert worden, weil Meldeämter Auskünfte verweigert haben. Herr Bux hat vom Zeit- und Sachaufwand gesprochen, der zur Klärung dieser Situation erforderlich ist. Wer dies beklagt und hier Abhilfe schaffen möchte, dem sollte man nicht unterstellen, daß er den Datenschutz hier zurücktreten lassen wolle.

Die unbestimmten Rechtsbegriffe bedürfen der Auslegung und es stellt sich die Frage, ob wir der Notwendigkeit entsprechen können, alle DV-Vorgänge in diesem Bereich normativ zu regeln, ob wir überhaupt die Sachkenntnis haben, dies allgemein zu tun. Es wäre schlimm, wenn durch Richtlinien, die aus einer politischen Stimmungslage heraus erlassen worden sind, tatsächlich, wie Herr Bux an einem Beispiel ausführte, 11% ermittlungsrelevante Wiederholungstatbestände verlorengingen. Ich weiß nicht, ob es tatsächlich so ist. Bei der Interpretation der neuen, datenschutzrechtlichen Begriffe gibt es Konflikte, die wir nicht wegdiskutieren können. Der Bundesbeauftragte für den Datenschutz ist der Meinung, daß man Erlaubnistatbestände in bestimmten Bereichen eng auslegen soll. Man kann sie unvernünftig eng auslegen, man kann sie natürlich auch unvernünftig weit auslegen.

Nehmen Sie nur die Frage der on-line-Anschlüsse zwischen den Behörden. Ich bin nicht der Meinung, daß man dies in jedem einzelnen Fall des Auskunftsverfahrens normativ regeln muß und regeln sollte. Nehmen Sie Fragen der Amtshilfe zwischen den verschiedenen Sicherheitsbereichen - darüber haben wir ja auch im Innenausschuß sehr ausgiebig diskutiert. Denken Sie auch an die Frage der Zulässigkeit

von Verdachtsspeicherungen im Rahmen der Datei PIOS/Terrorismus. Hier kann man die Ansicht vertreten - und dies scheint auch die herrschende Auffassung zu sein -, daß man die Voraussetzung für die Zulässigkeit dieser Speicherungen nicht zu eng fassen sollte, denn sonst bestünde die Gefahr, daß die Datei ihren Zweck, das Terrorismussyndrom einzukreisen, nicht mehr erfüllen könnte. Ich gebe dem Bundesbeauftragten recht, wenn er verlangt, solche Daten sollten im Falle einer Weitergabe ihrer speziellen Zweckbestimmung gemäß behandelt werden. Hier sind wir uns einig. Schwierig wird es dann im Detail. Hier sind Ermessensentscheidungen zu treffen, und man sollte alle Beteiligten auffordern, sich mit Emotionen zurückzuhalten. Man sollte nicht bei einer Entscheidung, die einem zu weit erscheint, gleich von Rechtsverstößen sprechen, oder gar davon, daß man den Datenschutz nicht mehr ernst nehmen wolle. Soweit mein Appell.

A. Wernitz

Auch der Verlauf der heutigen Diskussion läßt die Anregung sinnvoll und vernünftig erscheinen, daß alle Beteiligten, und speziell auch die Vertreter des Datenschutzes und der Sicherheitsbehörden zwar nicht täglich, aber doch gelegentlich und kontinuierlich Dialoge unter vier Augen führen sollten. Das würde der Inneren Sicherheit und auch dem Datenschutz ohne Zweifel zugute kommen. Daß dieser Dialog hin und wieder in einem so großen Kreis stattfinden muß, das liegt auf der Hand. Meine herzliche Bitte an die Genannten geht dahin, daß sie sobald als möglich diesen Dialog fortsetzen oder aufnehmen. Dies würde zu einem Gewinn auf der Ebene des Bundes und sicher auch der Länder führen.

Formeln wie "Überinterpretation" oder "überzogener Datenschutz" muß ich ablehnen, weil sie diffus und im Grunde auch gefährlich und problematisch sind. Da wird etwas hineingelegt, was in der Substanz bei genauerer Prüfung nicht haltbar ist. Wir sollten miteinander überlegen, wie wir es erreichen können, daß das, was in der Substanz gesagt werden muß, so ausgedrückt werden kann, daß es in der Öffentlichkeit differenziert ankommt und verstanden wird und nicht als Schlaginstrument für oder gegen irgendetwas mißbraucht werden kann. Dies ist eine praktische Frage und manchmal auch eine Frage des Miteinanderumgehens von allen Seiten. Als wir im Innenausschuß über den vierten Tätigkeitsbericht des Bundesbeauftragten in drei Sitzungen mehrstündig beraten haben, haben wir die Seiten 21 und 22, wo es um die wesentlichen Problembereiche der Beanstandung ging, Position für Position anhand konkreter Fälle durchgearbeitet. Da waren wir uns im Ausschuß insgesamt, auch was die einzelnen Fälle angeht, weitgehend in der Beurteilung einig. Es scheint mir wichtig anzumerken, daß diese Arbeit dann, wenn es um konkrete einzelne Fakten, um die Arbeitsebene der beiden Bereiche geht und nicht so sehr

ums Prestige, wo man demonstrativ Positionen beziehen muß, manchmal leichter ist. Das müßte auch in die Spitzengremien durchschlagen.

Auch die Medien könnten hier gute Mithilfe leisten durch eine differenziertere Darstellung. Wir müssen auch wegkommen von sogenannten Skandalveröffentlichungen, denn die schaden sowohl dem Datenschutz als auch der Polizei und dem gesamten Bereich der Inneren Sicherheit. Das setzt jedoch ein hohes Maß an verantwortlichem Handeln voraus - nicht nur bei den Vertretern der Medien, sondern vor allem auch bei denen, die hier und dort bestimmte Dinge mit gewissen, nicht immer besten Absichten lancieren, um es einmal so auszudrücken.

Nun zu der von Herrn Bux angeschnittenen Frage der Löschungsfristen. Ich habe mit Interesse gehört, daß nach seiner Meinung die Fristen bei den KpS-Richtlinien zu knapp bemessen seien. Er hat dies insbesondere in Bezug auf die 5-Jahres-Frist präzisiert. Wenn ich es richtig sehe und in Erinnerung habe, dann ist der Weg in Richtung auf die KpS-Richtlinien doch wohl so verlaufen, daß das, was auf der politischen Ebene von der IMK verabschiedet wurde, in den vorausgehenden Phasen von den Praktikern weitgehend mitbestimmt wurde. Das heißt, daß man diese Frage eigentlich an die eigene Adresse zurückgeben müßte. Denn dies ist nicht vom Himmel gefallen, sondern von der Basis, wenn ich es so verkürzt formulieren darf, nach oben gegeben worden. Vielleicht kann man es auch von daher erneut aufrollen und in Frage stellen. Ich nehme dies jedenfalls mit Interesse zur Kenntnis.

Ich möchte aber auch ganz klar feststellen, daß wir mit dem Bundesdatenschutzgesetz und mit der Einführung der externen Kontrolle dem Bundesbeauftragten für den Datenschutz eine bestimmte Pflicht zu berichten gesetzlich auferlegt haben. Wir wünschen und benötigen diese Informationen von ihm, und er würde gegen den Auftrag des Gesetzes handeln, wenn er diese Dinge nicht darstellen würde. Das sollte auch nicht übersehen werden. Im übrigen stimme ich der Bemerkung von Herrn Boge zu, daß nicht alles, was machbar ist aus der Sicht der Polizei und der Sicherheitsbehörden, auch wünschenswert ist. Ich gehe aber noch weiter: Nicht alles, was technisch möglich ist, dürfen wir auch tun.

H. Neu

Ich möchte auf zwei Punkte eingehen. Herr Boge hat sich darüber beklagt, daß in der Presse vieles - sei es lanciert oder nur offen ausgesprochen in bestimmten Berichten - erschiene, was der Polizei schaden könne. Nun hat Herr Boge offensichtlich übersehen, daß der Pressesprecher des Bundeskriminalamtes die Formulierung "wer hier juristische Argumentationstechniken vorschiebt, erhebt einen Verbindlichkeitsanspruch" und die Formulierung "die Verwendung juristischer Techniken bei der Argumentation dient in diesem Fall ..." gebraucht hat. So schwierig ist es miteinander zu reden, selbst wenn die eigene Pressestelle eingeschaltet ist und nicht böswillige Journalisten.

Im übrigen ist nun einmal "Hund beißt Mann" eine Nachricht und "Mann beißt Hund" keine. Dem Journalisten steht oft wenig Raum für einen Artikel zur Verfügung, wenn er ihn auf die erste Seite bringen will, während er auf der dritten Seite ausführlicher berichten kann. Die Entscheidung, auf die dritte Seite zu gehen, kann für einen Journalisten auch eine Prestige-Frage sein, und darum ist manchmal die kürzere Meldung, die dann mit "Hund beißt Mann" überschrieben ist, auf der ersten Seite für ihn bedeutend interessanter und wichtiger als eine ausführliche detaillierte Darlegung des Problems auf Seite 3.

Wir sollten keine Empfindlichkeiten entwickeln, die aus Veröffentlichungen in den Medien herrühren und die eigentlich nicht durch den Bericht selbst oder die Diskussion unter den Fachleuten entstanden sind. Es wäre daher auch möglich, nüchterner zu diskutieren. Sie sollten sich auch nicht über die juristische Ausdeutung des polizeilichen Handelns durch den Datenschutzbeauftragten aufregen. Wenn es hier an Sachbezogenheit und Realitätssinn mangelt, dann ist dies nicht dem Datenschutzbeauftragten anzulasten, sondern es liegt im Recht begründet. Das Recht aber hat der Gesetzgeber gemacht und Sie müßten sich dann an meine beiden Kollegen wenden, die weiterhin mit der Herstellung von Recht beschäftigt sind. Wenn die Rechtsbegriffe zu unbestimmt sind, dann würde ich jetzt nicht versuchen, sie zu ändern, sondern ich würde das den Gerichten überlassen. Wer glaubt, daß ein unbestimmter Rechtsbegriff für ihn nicht handhabbar ist, der sollte sich an das Gericht wenden. Wenn er nun befürchten muß, daß dann der unbestimmte Rechtsbegriff noch enger auszulegen ist, als dies im Augenblick aus der Sicht des Datenschutzbeauftragten der Fall ist, dann verzichtet er womöglich darauf. Die Politik sollte erst eingreifen, wenn in Einzelfällen nachgewiesen wird, daß die unbestimmten Rechtsbegriffe nicht handhabbar sind.

Bei der Terrorismusbekämpfung halte ich die Verdachtsspeicherung im System PIOS für notwendig. Sie gehört zu den sehr sorgfältig zu handhabenden präventiven Maßnahmen. Es muß aber sichergestellt sein, daß z.B. bei einer Bewerbung für eine Stelle im öffentlichen Dienst solche Verdachtsmomente nicht Grundlage für eine Nichteinstellung sein können. Das ist zwar auch für mich ein unbefriedigendes Ergebnis, aber man sollte sich nicht auf den Verdacht der Nichtstaatstreue, sondern nur auf die Tatsache der Nichtstaatstreue stützen. Auch die vielen Prozesse, die von Bewerbern bis durch 6 Instanzen gewonnen wurden, deuten darauf hin, daß wir den nicht beweisbaren Verdacht nicht zur Möglichkeit der Ablehnung machen sollten. Die Forderung, die PIOS-Daten besonders sorgfältig zu behandeln und bei ihrer Weitergabe sehr umsichtig mit ihnen zu verfahren, erscheint mir daher richtig. Im übrigen kann als Ergebnis des Podiumsgesprächs festgestellt werden, daß die Sachunterschiede im Denken zwischen den Datenschützern und der Polizei vermutlich nicht groß sind.

Die rechtliche Bremse hingegen muß stark sein, wenn das gesetzte Recht ernst genommen werden soll. Wenn wir begriffen haben, daß der Datenschutzbeauftragte nicht böswillig oder realitätsfern handelt, wenn er das gesetzte Recht beachten will, und wenn das gesetzte Recht der Polizei zu wenig Möglichkeiten für erfolgreiches Handeln gibt, dann sollte man sich an die Adresse der Politik wenden. Es wäre bedauerlich, wenn durch ständige Reibungen am gesetzten Recht zwischen Datenschutz und Polizei die Arbeit der Polizei unerträglich behindert würde oder das Mißtrauen gegenüber den Datenschutzbeauftragten in der Bevölkerung nicht abgebaut werden könnte, denn das besteht ja auch.

Dr. A. Schoreit, Bundesanwalt beim Bundesgerichtshof, Karlsruhe

Als hier anwesender Vertreter des Generalbundesanwalts muß ich natürlich der Äußerung entgegentreten, daß der Generalbundesanwalt irgendetwas angeheizt habe. Ich betrachte dies als eine dieser persönlichen Entgleisungen, von denen schon wiederholt die Rede war und die der Sachdiskussion nur schaden können. Jeder, der den Generalbundesanwalt kennt, weiß, daß er nichts anheizt, daß er das Notwendige sagt, daß er aber auch dann mit seiner Meinung nicht zurückhält, wenn er glaubt, daß sie gesagt werden muß. Der zweite Punkt ist, daß ich leider gleich zu Anfang dieser Veranstaltung eine Konfrontation mit Stimmen aus der Justiz erleben mußte, die mich aus ganz bestimmten Gründen etwas mißgestimmt hat. Wir haben hier im Laufe der Woche die verschiedenen in Betracht kommenden Rechtsgrundlagen erörtert. Von allen Seiten ist immer wieder klargestellt worden, daß es repressive und präventive Maßnahmen gibt.

Als Jurist muß ich dann prüfen, welches die Voraussetzungen der präventiven Maßnahmen sind. Das ist die polizeiliche Generalklausel. Die Voraussetzungen der repressiven Maßnahmen sind in der Strafprozeßordnung geregelt. Wenn diese Voraussetzungen nicht gegeben sind, sind die betreffenden Maßnahmen nicht gerechtfertigt. Man kann aber nicht sagen: Es gibt zwei Grundlagen und wir lassen dahingestellt, welche der beiden Anwendung findet. Man kann sich auch nicht auf die Vermutung der Rechtmäßigkeit berufen. Man muß für jede einzelne Maßnahme die dafür geltende Grundlage kennen und sie zumindest nennen können. Dabei ist die Beweisfrage noch ein anderes Problem. Ich halte es im Interesse der Rechtsstaatlichkeit für unverzichtbar, daß man die Gesetzmäßigkeit polizeilichen Handelns auch in diesem Bereich garantiert. Dies ist mein großes Anliegen, das ich an anderer Stelle bereits konkretisiert habe und das auch sicher in Zukunft noch weiter konkretisiert werden wird. Ich hoffe, daß wir darüber grundsätzlich Einverständnis erzielen.

Dr. R. Leuze, Datenschutzbeauftragte des Landes Baden-Württemberg, Stuttgart

Ich möchte auf den Beitrag von Herrn Bux eingehen. Er hat gezeigt, daß ein Hauptproblem im richtigen Lesen der KpS-Richtlinien liegt. Daran fehlt es meinen Beobachtungen zufolge leider immer wieder. Die Polizei meint, die Regelfristen seien ganz feste Fristen und es gäbe keine Ausnahme nach oben oder nach unten. Das ist mir bei meinen Kontrollen immer wieder entgegengehalten worden. Ich kann Ihnen nur empfehlen, die Möglichkeiten und den Spielraum, die die Kps-Richtlinien Ihnen einräumen, auch zu nutzen. Besonders deutlich wird dies bei der Aussonderung der Akten von Jugendlichen. Hier heißt es in den KpS-Richtlinien lediglich, - ich zitiere wörtlich - daß spätestens nach 5 Jahren zu prüfen ist, ob auszusondern ist. Niemand zwingt Sie, auszusondern.

Zweiter Punkt: Seit über einem Jahr bitte ich die Polizei, Fälle auf den Tisch zu legen, wo sie die Beobachtung gemacht hat, daß der Datenschutz ihre Arbeit tatsächlich erschwert. Die Frage, ob der Datenschutz die Polizei beeinträchtigt oder nicht, können wir nicht abstrakt diskutieren, sondern nur anhand von konkreten Beispielen. In meinem Bericht habe ich ausgeführt - und ich wiederhole dies hier -, daß ich bereit bin, über jeden Fall zu diskutieren und allem nachzugehen. Daher meine Bitte an Herrn Bux, daß die Esslinger Studie, von der ich heute erstmals höre, auch dem Datenschutzbeauftragten zugeleitet wird.

Dritter Punkt: Nicht alle, die Auskunftsersuchen stellen, sind, wie Herr Bux sie bezeichnet hat, polizeiliche Gegner. Es mögen solche dabei sein, aber es geht auch um Menschen, die in einer echten Notlage sind. Dies bitte ich auch zu bedenken.

Nun zum letzten Punkt. Herr Bux, Sie sprachen die Befürchtung aus, ich würde meine Kontrollbefugnisse ausdehnen und im Rahmen des KAN prüfen, ob ein Sachverhalt die Eingabe in den zentralen KAN rechtfertigt. Hier muß ich mit aller Deutlichkeit sagen: Sie sollen mit der Gewißheit nach Hause gehen, daß ich das prüfen werde. Denn es ist mein gesetzlicher Auftrag zu prüfen, ob die Richtlinien und Entscheidungen der Innenminister-Konferenz im polizeilichen Bereich bei der Datenspeicherung eingehalten werden. Dazu gehört auch, daß wir uns darüber unterhalten, ob im konkreten Fall die Eingabe in den zentralen KAN berechtigt war oder nicht.

Dr. R. Riegel, Regierungsdirektor beim Bundesbeauftragten für den Datenschutz, Bonn

Ich möchte auf einen Punkt zu sprechen kommen, der in dieser Tagung und auch im Podiumsgespräch sehr stark vernachlässigt wurde und der das tägliche Brot des Datenschutzes ausmacht, nämlich die Arbeitsebene. Ich will die Vernachlässigung der Arbeitsebene, der täglichen Kooperation trotz Konfrontation, des täglichen Zusammenwirkens in der Auseinandersetzung an dem Beispiel von Interpol deutlich machen. Herr Dr. Boge hat diesen Komplex heute morgen in einer Weise dargestellt, die Zweifel offen läßt und gestern ist er noch deutlicher und gleichfalls zweifelhaft dargestellt worden von Herrn Tolksdorf.

Ich darf mit dem zweimal geäußerten Satz beginnen, daß es geradezu absurd sei, etwa gegen die Notwendigkeit der internationalen Verbrechensbekämpfung anzugehen. Ich darf Sie auffordern, hierzu etwa den ersten Satz zur Interpolproblematik im vierten Tätigkeitsbericht zu lesen. Dort heißt es, daß wir selbstverständlich die Notwendigkeit anerkennen, daß dies aber nicht bedeuten kann, daß man sich nicht mit dem datenschutzrechtlichen Problem auseinandersetzt.

Zweiter Punkt: Es wurde hier - und dies betrifft die Arbeitsebene von Herrn Tolksdorf und auch von Herrn Boge - gesagt, daß man sich auf Seiten des BKA inzwischen bemüht habe, zu Regelungen zu kommen, die inzwischen von der Generalversammlung bei Interpol beschlossen worden seien und die einen durchaus tragfähigen Kompromiß darstellten. Warum wird dann verschwiegen, daß seit 1979 auf Anregung des BKA Gespräche mit dem Bundesbeauftragten für Datenschutz stattgefunden haben und Entwürfe hin- und hergegangen

sind, ungeachtet der grundsätzlichen Rechtproblematik, die wir hinsichtlich des Generalsekretariats bei Interpol verschieden sehen mögen. Das ist etwas ganz anderes. Aber im Hinblick auf die tägliche praktische Arbeit und das täglich Notwendige bestand in etwa 95% dessen, was ausformuliert und verabschiedet wurde, praktisch Einigkeit zwischen dem Bundesbeauftragten, dem BKA und dem BMI. Die letzte gemeinsame Besprechung hat im Frühjahr vor der Generalversammlung in Torremolinos stattgefunden. Warum wird dies nicht gesagt? Ich darf es hier nachholen, und bin dankbar für die Gelegenheit. Warum wird auch nicht erwähnt, daß wir uns bei unserer Interpolprüfung, die wir in diesem Jahr gesondert angestellt haben, um zu erfahren, ob unsere Vorschläge und Forderungen vernünftig sind, über die hierbei als problematisch erkannten Fälle im Prinzip einig waren. Es ging lediglich darum, in welcher Form die Probleme beseitigt werden sollten, denn daß es deren sehr viele gibt, wird doch wohl niemand bestreiten. Sie beginnen bereits bei dem riesigen Umfang des Auskunftsverkehrs, den wir ebensowenig bestritten haben wie den riesigen Arbeitsanfall beim BKA überhaupt.

Nun zum letzten Punkt. Es wird oft behauptet, der Bundesbeauftragte bringe immer alles gleich in die Öffentlichkeit. Ich kann hier nicht die vielen großen und kleinen Fälle aufzählen - was leider von der Seite, die es besser wissen muß, nicht geschehen ist - in denen wir gesagt haben: Hauptsache, es ist jetzt in Ordnung und dann wird nicht mehr darüber gesprochen. Viele Kollegen, die mit uns täglich zu tun haben, wissen das. Auch hier geht es bis in die Spitze, und jetzt wende ich mich an Herrn Schoreit, etwa zum Thema Rasterfahndung, das hier kontrovers diskutiert wurde. Einer Ihrer Kollegen hat sich wiederholt bei mir persönlich dafür bedankt, wie fair sich der Bundesbeauftragte gerade in der Diskussion um die Rasterfahndung verhalten hat, wo dieser den Mantel auch darüber gedeckt hat, daß in verschiedenen Auskunftsfällen einige kleinere Pannen passiert sind; Pannen, die bereits bei der Bundesanwaltschaft begonnen haben, nämlich etwa bei falsch formulierten, falsch beantragten und falsch erlassenen Gerichtsbeschlüssen.

Zum Abschluß möchte ich noch folgendes sagen: Wir haben uns in aller Regel geeinigt und werden uns auch künftig einigen, auch dort, wo wir die rechtsgrundsätzlichen Probleme beiseite schieben müssen, weil wir die materiellen Probleme der Praxis anerkennen. Dies ist hier alles zu kurz gekommen. Ich bedanke mich, daß Sie mir die Möglichkeit gegeben haben, dies hier auszuführen und habe jetzt nur noch den Wunsch, daß in Zukunft bei derartigen Tagungen die Einseitigkeit nicht so groß bleibt. Ich kann nur anbieten - und hier spreche ich auch für Herrn Bull und

für mein ganzes Referat -, daß es von uns aus so vernünftig und so gut und auch so hart und so fair weitergehen soll wie bisher. Ich gehe davon aus, daß dies auch von den Kollegen im BKA so akzeptiert wird.

L. Seeber, Oberstaatsanwalt, Kammergericht Berlin

Ich halte es nicht für sehr sinnvoll, wenn wir hier uns gegenseitig versichern, welche lieben Menschen wir doch alle sind oder auch nicht. Wir sollten vielmehr konkrete Fragen stellen, und ich habe zwei Fragen an Herrn Bull:

Auf dieser Tagung ist bereits gefragt worden, ob im repressiven Bereich, also im Justizbereich, die Generalnormen der StPO ausreichen. Ich bin der Auffassung, daß dies der Fall ist; das wird jedoch mitunter bestritten. Welcher Meinung sind Sie, lieber Herr Bull? Glauben Sie, daß das, womit Eberhard Schmidt im Jahre 1952 seinen bekannten Vortrag vor dem Bundesgerichtshof geschlossen hat, auch heute wieder gilt? Er rief damals aus, ein wenig resignierend im Anblick unserer so leidigen Historie: Der Positivismus ist tot, es lebe der Positivismus!

Zweite Frage: Wie sehen Sie das Dilemma der Polizei, die, wie Herr Boge angekündigt hat, die präventiven und repressiven Daten untrennbar 'vermaschen' will, die aber zugleich der Justiz, als deren verlängerter Arm, die Möglichkeit geben muß, auf den repressiven Datenbestand gezielt und filterlos durchzugreifen. Halten Sie diese Vermaschung für vertretbar, und wenn ja, wie wollen Sie den Durchgriff der Justiz sicherstellen; genau, wie es Gesetz und Recht befehlen, um in diesem sensiblen Bereich die Rechtsförmlichkeit zu garantieren und die Verantwortung der Justiz nicht zur leeren Phrase werden zu lassen? Ist die Vermaschung etwa eine Masche?

Dr. K. U. Kersten, Ministerialrat im BMI, Bonn

Meine Bemerkung ist speziell an Herrn Bux gerichtet, der von einigen, wohl ersten und möglicherweise noch nicht repräsentativen Erfahrungen mit der Anwendung der KpS-Richtlinien gesprochen hat. Wie Sie wissen, haben die Innenminister des Bundes und der Länder im Januar 1981 einvernehmlich die KpS-Richtlinien verabschiedet, wobei man sich durchaus bewußt war, daß mit diesen Regelungen Neuland betreten wird. Wenn man z.B. Aussonderungsfristen von 25 Jahren auf 10 Jahre herabsetzt, dann wird deutlich, daß hier ein ganz neuer Abschnitt begonnen wird. Deshalb haben die Innenminister einvernehmlich gesagt, daß sie sich nach einer gewissen Erprobungszeit erneut zusammensetzen wollen, um unter Berücksichtigung der Erfahrungen der Praxis diese Richtlinien u.U. in dem einen oder anderen Punkt

zu modifizieren. Dies sollte m.E. ein Anlaß sein, die Bemerkungen, die Herr Bux hier gemacht hat, sehr ernst aufzunehmen und für solche Überprüfungen vorzumerken, wie auch beabsichtigt ist, die Anmerkungen der Datenschutzseite zu einzelnen Bestimmungen der KpS- und Dateienrichtlinien in diese spätere Überprüfung mit einzubeziehen. Herr Professor Bull hat das Stichwort der Speicherung von anderen Personen bereits genannt. Dies ist nie bestritten, und ich halte es nicht für angebracht, hier, wo wir das erste Mal mit diesen Argumentationen konfrontiert werden, gleich fertige Meinungen zu präsentieren und zu sagen, dies komme nicht in Betracht. Man sollte alle Argumente von beiden Seiten in diese beabsichtigte Überprüfung, die auch stattfinden wird, einbeziehen und dann entscheiden, ob alles beim alten bleibt oder ob Modifikationen erforderlich sind.

J. Zeiger, Kriminaldirektor im BKA

Ich möchte zunächst auf das Argument von Herrn Wernitz eingehen, die Praxis sei ja in der Vorbereitungsphase an der Festsetzung der heutigen KpS-Fristen beteiligt gewesen. Das trifft zu: Die Praxis war beteiligt. Aber jeder, der weiß, wie die Dinge damals in den Ausschüssen gelaufen sind, weiß auch, daß diese Fristen von der Praxis nur zur Kenntnis genommen und nicht von ihr vorgeschlagen worden sind. Soviel zur Beteiligung der Praxis an der Festlegung der Fristen in den KpS-Richtlinien.

Ich möchte nun in zwei Punkten auf die Ausführungen von Herrn Professor Bull und Herrn Weyer eingehen. Herr Professor Bull, Sie haben Ihren Tätigkeitsbericht erwähnt, in dem Sie die bei Ihren Prüfungen ermittelten Mängel festgestellt und dem Bundestag dargestellt haben. Sicherlich ist das aus Ihrer Sicht so richtig. Wir hätten uns aber gewünscht, daß der andere Teil dessen, was Ihre Mitarbeiter bei uns festgestellt haben - und Herr Riegel hat es soeben nachgeholt -, nämlich die großen Anstrengungen, die die Polizei zur Durchsetzung der an sie herangetragenen Forderungen unternommen hat, ebenfalls in diesem Tätigkeitsbericht enthalten sein sollten.

Zweiter Punkt: In Ihrer Entgegnung auf die Ausführungen von Herrn Dr. Boge zur juristischen Argumentation haben Sie gesagt, daß Sie selbstverständlich juristisch argumentieren müssen. Das ist aus Ihrer Sicht sicherlich richtig, und die Grundsätze, nach denen sie bei Ihren juristischen Würdigungen verfahren - nämlich Verhältnismäßigkeit und Erforderlichkeit - sind selbstverständlich unbestritten. Aber daraus, wie Sie dann diese Grundsätze und die Begriffsinhalte, die Sie ihnen unterlegen, auf konkrete

Sachverhalte projizieren, ergeben sich doch die Streitpunkte, über die wir gelegentlich verschiedener Meinung sind. Wir wünschen uns von Ihnen, daß Sie gelegentlich auch unsere Auffassung akzeptieren und daß Sie nicht Ihre Auffassung als die allein seligmachende darstellen.

A. Wernitz

Ich will hier nicht noch einmal auf die einzelnen Beiträge eingehen. Wenn über die KpS-Richtlinien gesagt wurde, daß man sie von seiten der Praktiker nur zur Kenntnis genommen habe, dann hätte es vielleicht auch verschiedene Möglichkeiten gegeben, einmal die Warnlampe aufleuchten zu lassen, wenn bei der Praxis grundsätzliche Bedenken bestanden. Ich wollte nur auf diesen Tatbestand hinweisen.

Im übrigen meine ich, daß wir, die wir in der Gesetzgebung tätig sind, auf manches, was an Kritik und an Widerstand in Richtung Bundesbeauftragter für den Datenschutz geäußert wurde und was es an Reibungsflächen zwischen der Institution der Datenschutzbeauftragten bzw. des Bundesdatenschutzbeauftragten und den Sicherheitsbehörden gibt, sehr genau achten müssen, denn wir sind bei dem, was zum Teil hier ad personam gesagt wurde, im Grunde auch immer mitangesprochen. Im Grunde genommen müssen wir uns als Mitglied der Legislative immer darüber im klaren sein, daß wir auch unser Teil beizutragen haben, vor allem im Rahmen der anstehenden Novellierung des Bundesdatenschutzgesetzes. Hierfür habe ich aus dieser Tagung erneut einiges mitgenommen.

P. Laufs

Ich möchte zum Abschluß feststellen, daß tatsächlich in der Praxis draußen die Zusammenarbeit zwischen den Vertretern des Datenschutzes und den Betroffenen, wie das auch für den Umweltschutz gilt, in der Regel sehr konstruktiv ist und auch zu Ergebnissen führt. Neu ist nur die Rolle der Betroffenen, die sich sehr oft als Bittsteller fühlen und den Kontrolleur zu sehr als Bürde empfinden. Der Mathematiker Hilbert hat einmal gesagt, eine neue mathematische Theorie begreifen lernen hieße, sich an sie zu gewöhnen. Wenn das schon in der Mathematik so ist, wieviel mehr muß es dann für eine neue Rechtsmaterie gelten. Man kann nur wünschen, daß nach diesem Gewöhnungsprozeß ein partnerschaftliches Verhältnis entsteht und offenkundig wird, daß der Datenschutz in der Tat nicht die alles überlagernde höchste Kontrollinstanz in unserem Lande ist.

H. P. Bull

Ich darf wieder mit einer Zustimmung beginnen, Herr Laufs. Auch ich bin immer der Meinung gewesen, daß wir nicht die oberste Kontrollinstanz sind. Ich will mein Amtsverständnis noch einmal etwas deutlicher machen. Wer dieses Amt eines Kontrolleurs übernimmt und eine neue Rechtsmaterie ins Bewußtsein bringen soll, der kann sich nicht zum Ziel setzen, beliebt zu sein bei denen, die er kontrollieren soll. Es war nie mein Ziel, Beliebtheit zu erringen, Wähler zu gewinnen oder irgendwelche freundlichen Stimmungen mir gegenüber zu produzieren, sondern ich habe immer in Kauf genommen, daß meine Tätigkeit für die Betroffenen ärgerlich ist. Das ist meine Aufgabe, und ich habe ein interessantes Amt, das mir Gelegenheit gibt, mich für verfassungsmäßige Grundwerte aktiv einzusetzen. Ich bin sicher, wenn ich in meinen Berichten erheblich freundlicher formuliert und noch mehr Streicheleinheiten verteilt hätte, als ich es getan habe, und wenn ich mit großen Worten gesagt hätte, daß ich die Anstrengungen der Polizei oder auch des Verfassungsschutzes, gesetzestreu zu handeln, anerkenne, dann wäre die Diskussion heute wahrscheinlich genauso gelaufen. Denn natürlich hätten auch irgendwo die Worte "rechtlich bedenklich" oder "nicht unbedenklich" gestanden. Und dann hätte Herr Boge oder wer immer gesagt, das sei aber zu hart, das schüre das Mißtrauen der Bevölkerung gegen die Polizei.

Ich kann nicht verhindern, daß der Hinweis auf rechtstaatliche Bedingungen bei denen, die meinen, sie hätten sie bisher schon erfüllt oder die sich vorhalten lassen müssen, es sei nicht alles so gut gelaufen, Ärger hervorruft. Das ist normal. Andererseits muß ich aber auch darauf beharren und bestehen, daß diese Kritik ausgesprochen wird. Ich darf einmal eine andere Instanz zitieren, die sicher auch irgendwelcher Linkslastigkeit oder Einseitigkeit ganz unverdächtig ist. Der Deutsche Richterbund schreibt in einer seiner Presseerklärungen, nur das Vorbild unbedingter rechtsstaatlicher Integrität aller staatlicher Institutionen könne dazu beitragen, die mit Recht zu beklagende Staatsverdrossenheit vieler junger Menschen abzubauen. Das wird übrigens gesagt in einem Zusammenhang, der den politischen Parteien unangenehm sein dürfte: Parteienfinanzierung, Amnestiepläne u.ä. werden dort kritisiert. Ich halte dies in vielen anderen Zusammenhängen für ebenso gegeben und unterschreibe diese Aussage.

Wenn wir - und darin sind wir uns doch sicher alle einig - wollen, daß dieser Staat von allen, gerade auch den jungen Bürgern getragen und bejaht wird, dann führt es nicht weiter, einander vorzuwerfen, daß die Kritik zu weit gehe und daß die rechtsstaatlichen Bindungen zu stark betont würden. Das Ziel muß vielmehr sein, diese Bedingungen so stark wie möglich zu betonen und sich daran zu halten.

Deshalb werden Sie, wenn Sie die Kontrollinstanzen schelten, gerade dieses Vertrauen nicht stärken, das Sie sich zu Recht wünschen. Ich habe auch in meiner allerersten Erklärung noch vor Amtsantritt einer Zeitung gegenüber gesagt, unberechtigtes Mißtrauen müsse abgebaut werden. Meine Aufgabe ist es, die Gründe für berechtigtes Mißtrauen auszuräumen und unberechtigten Ängsten entgegenzuwirken. Daran habe ich mich gehalten. Wenn Sie etwas in derselben Richtung tun wollen, dann sollten Sie nicht so verfahren wie z.B. anläßlich unseres vierten Berichts, auf dessen Inhalt Sie nur in Einzelheiten eingegangen sind, sondern deutlich den ganzen Text allen, die sich dafür interessieren, zur Verfügung stellen, ihn erläutern und sagen, in welchen Punkten Sie anderer Meinung sind und in welchen Sie mit uns übereinstimmen. Dies wäre auch ein kleiner Beitrag zur Entschärfung der Diskussion. Ich könnte ja fast überheblich werden, wenn ich hier höre, daß ich mit meinen vier Mitarbeitern im Sicherheitsbereich um die 10 000 Polizeibeamte in der Bundesrepublik so völlig verunsichert haben sollte, daß ihr Bild in der öffentlichen Meinung schwankt oder verdunkelt ist. Das scheint mir doch abwegig.

Herrn Bux möchte ich noch entgegenhalten, daß das Ergebnis des Esslinger Experimentes, bei dem von 1 000 Akten nach einiger Zeit 109 noch etwas Polizeirelevantes enthielten, nämlich Informationen über Leute, die polizeilich wieder in Erscheinung getreten sind, noch nicht bedeutet, daß Sie unbedingt auf diese Informationen angewiesen waren. Das Argument für sich allein trägt nicht. Erst wenn Sie hinzufügten, diese und jene Information hätte zusätzlich ein bestimmtes Gewicht gehabt und Sie hätten bestimmte Täter ohne die Information nicht bekommen, wäre Ihre Argumentation vollständig gewesen. Dieser Teil müßte also, wenn es darauf ankäme, nachgeholt werden. Ich meine, wir sollten nicht auf der Grundlage einer kurzfristigen Beobachtung dieser Entwicklung nun schon wieder einen Anlauf zu Änderungen machen. Wenn die Frist 20 oder 30 Jahre betrüge, dann könnte im 21. oder 31. Jahr auch noch etwas von Bedeutung hinzukommen, das bei fristgerechter Löschung nicht mehr zu berücksichtigen wäre. Die Polizei bekommt zum Glück vielfältige Informationen auf andere Weise, und das soll auch so bleiben.

Damit komme ich auf die Einleitung zurück. Herr Spranger hat zu Recht betont, und andere haben es bestätigt, daß die reine Suche beim Computer in der Datensammlung nicht weiterhilft. Sie werden vielmehr immer darauf angewiesen sein, zielstrebig nach eigenem Plan mit kriminalistischen Methoden zu fahnden, und das kann Ihnen keine Datenverarbeitung abnehmen.

H. Weyer

Ich möchte nur kurz auf die Ausführungen von Herrn Zeiger eingehen, der mich angesprochen hatte. Sie können sicher sein, daß ich bei meinen Prüfungen die Argumente der Polizei zur Erforderlichkeit und zur Verhältnismäßigkeit zur Kenntnis nehme, ernst nehme und würdige. Wenn sie mich überzeugen, sage ich dem Bürger auch, daß die Polizei in einem solchen Fall recht hat. Dafür muß ich manchmal auch Schelte in Kauf nehmen; auch dies ist unvermeidlich. Das erfährt die Polizei dann allerdings nicht. Es darf aber nicht geschehen, daß die Prüfungen in ein Verfahren gegenseitigen Gebens und Nehmens einmünden. So etwas wäre mit der Rolle einer unabhängigen Kontrollinstanz schlechterdings unvereinbar. Der Datenschutzbeauftragte hat nun einmal die Aufgabe, Verstöße gegen Datenschutzvorschriften festzustellen, falls solche nach seiner Überzeugung vorliegen. Dabei kann er sich nichts abhandeln lassen. Wenn er Verstöße festgestellt hat, muß er dies auch offen aussprechen, auch in seinen Tätigkeitsberichten.

D. Küster, Ltd. Kriminaldirektor im BKA

Ich möchte den stillen Vorwurf von Herrn Dr. Riegel aufgreifen. Wenn gefordert wird, daß vom Bundesdatenschutzbeauftragten abweichende Auffassungen auch im Tätigkeitsbericht angeführt werden sollen, dann muß auch zugegeben werden, daß es auf der Arbeitsebene Gespräche zwischen den Mitarbeitern des Bundesdatenschutzbeauftragten und mit ihm selbst gegeben hat. Ich bestätige also ausdrücklich, daß diese Gespräche stattgefunden haben. Ich möchte aber auch bestätigen, daß es grundsätzliche Differenzen nach wie vor gibt; diese sollten auch in dieser Arbeitstagung ausgetragen werden.

K. Bux

Ich möchte zu dem Vorgetragenen noch zwei Bemerkungen machen:

Die erste betrifft die Löschungsfristen. Ich habe mich nicht dafür ausgesprochen, daß die Fristen auf 20 oder 25 Jahre verlängert werden sollen. Es gibt m.E. aber Anhaltspunkte dafür, daß möglicherweise die Fristen nicht richtig gesetzt sind. Wir sollten eine analytische Prüfung darüber vornehmen - das Material dazu haben wir oder es kann zumindest erhoben werden -, ob wir mit diesen Fristen zurechtkommen oder nicht. Für eine solche Prüfung müßte natürlich auch Material ausgewertet werden, das nach den KpS-Richtlinien zur Vernichtung heransteht. Es muß ja auf Akten zurückgegriffen werden, die nach Ablauf der Frist zu vernichten sind, damit daraus der Nachweis erbracht werden kann, in wieviel Fällen, in welchen Fällen und warum dieses Material später wieder zur Aufklärung von Straftaten erforderlich wwerden könnte. Ich meine, daß man die Entscheidung über die Fristen zu einem gegebenen Zeitpunkt auf eine saubere wissenschaftliche Basis stellen sollte; zur Aufbereitung des Materials bedürfte es natürlich auch der Unterstützung der Datenschutzbeauftragten.

Meine zweite Bemerkung betrifft die Ausführungen zur Auskunftserteilung. Ich meine, daß eine Abschreckung des Straftäters vor der Durchführung von weiteren Straftaten vor allem dadurch erreicht wird, daß er aus Angst vor einem möglichen polizeilichen Wissen über sein Handeln eine Überführung befürchtet. Wenn wir ihm nun die Türen zum polizeilichen Wissen öffnen - und dies wird, wie dargelegt, durch die Auskunftsverpflichtung ermöglicht - dann kann er sein Handeln auf das polizeiliche Wissen ausrichten, zumindest subjektiv wird das Risiko des Straftäters, bei seinem strafbaren Handeln überführt zu werden, vermindert.

H. Bull

Ich möchte noch kurz auf die beiden Fragen von Herrn Seeber eingehen. Zur ersten Frage: Der Satz "Der Positivismus ist tot, es lebe der Positivismus" trifft sicher nach wie vor zu. Ich lese die StPO allerdings so, daß in ihr keine Generalklausel zur Vornahme sämtlicher polizeilichen Ermittlungsmaßnahmen enthalten ist, sondern so, daß dort wesentliche Punkte, etwa die Observation, die polizeiliche Beobachtung und weiteres, was zur Informationsverarbeitung gehört, nicht geregelt sind. Ich meine, daß hier ein erheblicher Regelungsbedarf besteht.

Zweiter Punkt: Vermaschung der Daten, die zu Ermittlungszwecken gesammelt worden sind mit solchen, die zu Gefahrenabwehrzwecken gesammelt werden oder doppelte Funktion dieser Daten. Dies ist ein Beispiel dafür, daß ich der Ansicht der Polizei gefolgt bin und mich habe überzeugen lassen, daß hier ein sehr starkes Bedürfnis besteht, das rechtlich auch begründbar ist. Aus diesem Grunde und nicht aus irgendwelchen anderen, die mir gelegentlich unterstellt werden, scheint mir hier trotz gewisser möglicher Bedenken die Zulässigkeit der Datenverarbeitung durch die Polizei gegeben.

H. Neu

Der letzte Teil der Diskussion war zum Teil bestimmt von Empfindlichkeiten, die aus dem bisherigen Tagungsverlauf herrühren. Die sollten wir einmal beiseite lassen.

Was die Statistik von Baden-Württemberg über die Löschungsfristen angeht, so reicht es m.E. nicht aus, wenn man feststellt, daß 11% in 5 Jahren doch wieder aktenkundig geworden sind. Man muß dann auch prüfen, in welcher Weise, so z.B. ob beim ersten Mal ein Autodiebstahl, beim zweiten Mal eine Schlägerei oder wieder ein Autodiebstahl vorlag. Das ergibt dann ein anderes Bild. Das Argument, es wäre auch für die Justiz notwendig zu wissen, daß vorher schon etwas vorgelegen hat, damit man dies bei der zweiten oder dritten Straftat richtig würdigen könne, kann natürlich nicht ziehen. Hierfür sind die Justizakten da, und wenn dort etwas gelöscht wird, dann soll der Richter das nicht mehr berücksichtigen. Man sollte also nicht argumentieren, daß die Justiz am Nichtlöschen bei der Polizei interessiert wäre, wenn sie selbst verfügt, daß bei ihr getilgt oder gelöscht wird. Nun zur Frage der Auskunftspflicht. Die Argumentation ging zum Teil dahin, daß die Anwort "Wir haben zwar etwas, aber wir geben es dir nicht" den Straftäter darauf aufmerksam mache, daß die Polizei hinter ihm her ist. Der Bescheid, daß keine Daten vorliegen, zeige ihm hingegen, daß die Polizei noch nichts wisse. Ich meine, man sollte dies nicht dramatisieren. Ich

glaube überhaupt, daß auch heute vieles, was in Wirklichkeit nur eine lästige geringe Behinderung für die Arbeit der Polizei darstellt und ein Umdenken erfordert, dramatisiert worden ist und daß das Datenschutzgesetz der Polizei sehr wohl die Möglichkeiten für eine gute Arbeit läßt. Wenn sie nicht versucht, sich daran vorbeizustehlen, dann wird sie sich auch am schnellsten darauf einstellen können. Wer versucht, eine Rechtslage zu ignorieren, der wird Schwierigkeiten bekommen - sei es beim Beauftragten für die Bundeswehr, sei es beim Beauftragten für den Datenschutz. Wer sich bemüht, damit zu leben, der wird am ersten reibungslos weiterarbeiten können, und das sollten wir uns eigentlich vornehmen.

Schlußwort

Edwin Kube

Fast auf den Tag genau vor 10 Jahren, am 13.11.72, wurde das elektronische Informationssystem für die Polizei - INPOL - in Betrieb genommen. Das Bundeskriminalamt wollte dies nicht zum Anlaß für eine Jubelfeier nehmen, sondern vielmehr im Rahmen der alljährlichen Arbeitstagungen für eine kritische Bestandsaufnahme und für eine intensive Diskussion der derzeit drängendsten Probleme nutzen.

Im einzelnen war es ein ganzes Spektrum von Zielen, die mit dieser Veranstaltung verfolgt wurden. So war es beispielsweise ein besonderes Anliegen, die Öffentlichkeit über wesentliche Inhalte der Datenverarbeitung bei der Polizei zu informieren. Herr Lindlau hat uns vor Augen geführt, wie leicht es in der Bevölkerung zu Angst und Mißtrauen kommen kann, wenn die polizeiliche Datenverarbeitung und das kriminalistische Vorgehen aus einer blinden ideologischen Position heraus oder von fachlich inkompetenten Personen kritisiert wird, wenn seitens der Polizei zu wenig Aufklärung und sachliche Information betrieben wird, wenn die Polizei bei ihrer Selbstdarstellung den Eindruck der Omnipotenz erweckt und wenn dann in der Bevölkerung die Begrenztheit polizeilicher Eingriffe nicht mehr gesehen wird. Die anwesenden Vertreter der Medien werden mit ihrer Berichterstattung über diese Tagung sicherlich zum Abbau eines Teils der Ängste beitragen. Präsident Dr. Boge stellte in seinen "Thesen zur Funktion und Bedeutung der Datenverarbeitung bei der Polizei" die EDV als ein unentbehrliches Hilfsmittel für die Verbrechensbekämpfung heraus, das nicht nur der Abbildung konventioneller Strukturen und Abläufe dient, sondern auch neue Möglichkeiten der Handhabung und Verknüpfung komplexer Datenbestände schafft: Einzelne DV-Anwendungen dürften nicht "Inseln" bleiben, ein "Funktionsverbund" müsse polizeiliche Arbeit effektiver gestalten. Ziel polizeilicher Datenverarbeitung sei vor allem die wirksame Unterstützung vor Ort, beim Sachbearbeiter oder der dortigen Polizeiführung. Dr. Boge betonte zudem, daß die Anwendung von Computern bei der Polizei auch für den Bürger - z.B. durch schnellere Personenüberprüfungen oder durch "programmiertes Vergessen" bei Wegfall des Speicherungsgrundes - Vorteile bringt. Das von Herrn Küster vorgestellte "Konzept für Fortentwicklung des polizeilichen Informationssystems INPOL" bietet die Garantie, daß diese Ziele und Aufgaben auch in Zukunft kontinuierlich weiterverfolgt werden. So soll das Gesamtsystem mit seinen Subsystemen durch Unterstützung

der Verbrechensbekämpfung der Gewährleistung der inneren Sicherheit dienen; die Teilung des Systems in INPOL-Bund und INPOL-Land dürfte wohl den Befürchtungen einer wachsenden Omnipotenz der Polizei durch EDV weitgehend den Boden entziehen. Es ist abzuwarten, wie sich diese Struktur auf die Verbrechensbekämpfung auswirkt. Mit dieser Entwicklungsrichtung i.S. einer informationellen Trennung befinden wir uns - wie wir dem Vortrag von Frau Gehnich entnehmen konnten - in Übereinstimmung mit entsprechenden Überlegungen in Schweden. Das dort geplante neue EDV-System soll in erster Linie bestimmte Datenmengen für die Bezirke zugänglich machen, und nur ganz spezielle Informationen sollen in zentralen Dateien erfaßt werden.

Konkrete Anwendungsmöglichkeiten der Datenverarbeitung bei der tagtäglichen polizeilichen Arbeit liegen - das machte uns Herr Lehmann deutlich - sowohl für den Streifendienst als auch für den Ermittlungsdienst und für Führungsaufgaben in der Bewältigung großer Informationsmengen, der Beschleunigung des Nachrichtenflusses, der Vermeidung von Mehrfacherfassungen und der Entlastung von Routinearbeiten.

Der Erleichterung der Arbeit vor Ort kann sicherlich auch der unmittelbare Zugriff auf die Datenbestände anderer Behörden dienen. Es war daher ein weiteres Ziel unserer diesjährigen Arbeitstagung, mit Vertretern von Justiz- und Ordnungsbehörden - die für die Polizei in erster Linie von Bedeutung sind -, einschlägige Erfahrungen auszutauschen. Mit besonderem Interesse haben wir von Herrn Julich über erste Erfahrungen des Kraftfahrt-Bundesamtes mit dem Zentralen Verkehrsinformationssystem ZEVIS gehört, dessen gesamte Realisierung für 1984/85 vorgesehen ist und mit dem das Kraftfahrt-Bundesamt die Voraussetzungen für einen Informationsverbund mit der Polizei geschaffen hat. Auch auf seiten der Strafjustiz befinden sich elektronische Datenverarbeitungssysteme im Aufbau. Dr. Ernesti hat uns - aus justitieller Sicht - vor allem die rechtliche Problematik der (teilweisen) Überführung des von jeher bestehenden Informationsverbundes zwischen Staatsanwaltschaft und Polizei beim Ermittlungsverfahren in einen elektronischen Datenverbund erläutert. Besondere Bedeutung kommt in diesem Zusammenhang nach Auffassung von Justizvertretern dem Rechtscharakter der auszutauschenden Daten zu. Stichwort: Strafverfolgungsdaten seien Justizdaten. Offensichtlich ist bei den beiden Institutionen das Problem Justizdaten und die Frage der Möglichkeit der Trennung bzw. der Abgrenzung zwischen Präventiv - und Strafverfolgungsdaten, was offensichtlich im Ansatz mittelbar mit dem noch immer problematischen Verhältnis Staatsanwaltschaft - Polizei zusammenhängt, weitgehend ungeklärt.

Prinzipiell sieht die Polizei auch Strafverfolgungsdaten als "ihre" Daten an.

Ich habe in meinem Beitrag versucht, deutlich zu machen, daß die Rechtsgrundlagen der polizeilichen Datenverarbeitung dogmatisch im einzelnen noch weitgehend ungeklärt sind, auch wenn eine solide rechtsstaatlich geprägte Grundlage für die EDV vorhanden ist. Dabei habe ich bedauert, daß sich die Polizei - etwa in Fachbeiträgen - zu wenig um die rechtliche Durchdringung ihres Aufgabenfeldes bemüht.

Umfassende rechtliche Probleme wirft nach wie vor der Datenschutz auf. Unsere Tagung sollte deshalb auch dazu dienen, diese Diskussion weiterzuführen. Die Beiträge von Professor Simitis und Vizepräsident Tolksdorf haben zwar - wie nicht anders zu erwarten - in zahlreichen Einzelfragen die unterschiedlichen Positionen herausgestellt; dies betraf z.B. die Rechtsgrundlage für die Befugnis zur Informationsverarbeitung und die Frage der Zulässigkeit von Direktanschlüssen zu anderen Behörden. Bemerkenswert scheint mir aber, daß von beiden ausdrücklich vor einer Polarisierung von Datenschutz auf der einen und Sicherheit auf der anderen Seite gewarnt wurde. Ich darf in diesem Zusammenhang daran erinnern, daß schon in seiner Eröffnungsansprache der Parlamentarische Staatssekretär Spranger ausführte, die Einbindung der Sicherheitsbehörden in den Rechtsstaat garantiere die persönliche Freiheit des Bürgers und damit auch seine berechtigten Interessen in bezug auf den Datenschutz; Sicherheit und Freiheit seien daher in unserer Gesellschaft keine Gegensätze, es gehe vielmehr darum, daß der Staat Sicherheit und inneren Frieden gerade um der Freiheit willen zu gewährleisten habe.

Vielfältige Fragen sind - auch in interessanten Beiträgen aus dem Plenum - beim Podiumsgespräch diskutiert worden. Die Beiträge sind uns aktuell in Erinnerung; ich brauche sie nicht zu skizzieren. Vor allem fiel mir dabei jedoch auf, daß offensichtlich eine erfreuliche Klimaverbesserung zwischen den verschiedenen Seiten eingetreten ist, auch wenn manche Beiträge mit besonderem persönlichen Engagement und pointiert abgegeben worden sind. Betonen möchte ich hier die Forderung von politischer Seite, daß der Dialog zwischen Sicherheitsorganen und Datenschutz eine Daueraufgabe sein sollte.

Lassen Sie mich zum Abschluß meiner zwangsläufig sehr knappen Übersicht über die vergangenen drei Tage noch auf einen letzten Themenkreis unserer Veranstaltung zu sprechen kommen: Angesichts der immensen technologischen Entwicklungsanstrengungen, die uns Professor Krückeberg - wohl notwendigerweise sehr abstrakt - vor Augen geführt hat, stellt sich die Frage der Nutzung der anwendungsbezogenen technischen Forschung und Entwicklung nach Umfang, Zeitpunkt und Qualität in der Polizei. Vieles läßt sich wohl z.Z. noch nicht exakt einschätzen, zumal gerade auch hier der Kostenfaktor eine bedeutsame Rolle spielt. Bereits vorhandene wissenschaftliche Erkenntnisse können nur teilweise aufgegriffen und, z.T. allerdings beispielhaft, vorangetrieben werden. Als Exempel sei der rechnergestützte Handschriftenvergleich genannt.

Noch einige Sätze zu den Gruppendiskussionen.
In der Gruppe "Technisch-wissenschaftliche Datenverarbeitung und Forschung im BKA" stellte Dr. Bunge neue Möglichkeiten der polizeilichen Datenverarbeitung dar: die rechnergestützte Verarbeitung und Analyse von menschlichen Stimmen, von Handschriften und Photographien. Übereinstimmend wurde die Notwendigkeit solcher Forschungen bei der Polizei akzeptiert, wobei vor überzogenen Erwartungen gewarnt wurde. Mit dem Problem, daß viele Sachbearbeiter durch die Einführung der EDV eine starke Veränderung ihres Arbeitsplatzes und Aufgabenablaufs erlebt haben, befaßte sich unter der Leitung von Herrn Stuff eine weitere Gruppendiskussion. Als besonders bedeutsam wurden etwa die optimale Gestaltung des Arbeitsplatzes und die Benutzerfreundlichkeit der Systeme hervorgehoben; beides dürfte in direktem Zusammenhang mit der Anfragehäufigkeit durch die Sachbearbeiter stehen. Das auch hier intensiv diskutierte allgemeine Problem der Akzeptanz von EDV-Systemen in der Polizei bildete den Ausgangspunkt für die Erörterungen in der dritten Diskussionsrunde über "Ausbildungs- und Informationsprobleme aus der Sicht der Aus- und Fortbildung und aus der Sicht der Anwendung". Einvernehmen konnte hier dahingehend erzielt werden, daß die notwendige Einbeziehung der EDV in die polizeiliche Sachbearbeitung nur dann gewährleistet werden könne, wenn im Rahmen des fachspezifischen Unterrichts die jeweils einschlägigen EDV-Aspekte integriert behandelt werden. Hier wie auch bei den notwendigen Fortbildungsmaßnahmen sei die ausschließliche Hilfsmittelfunktion der EDV zu verdeutlichen.

Das sicherlich interessante, ich möchte behaupten faszinierende Panorama, das in den letzten Tagen vor Ihnen ausgebreitet worden ist, könnte den Gedanken an Perfektionierung um jeden Preis nahelegen. Ich möchte daher zum Abschluß betonen, daß auch die Polizei Fragen der Ethik bei der Anwendung der Datenverarbeitung nicht vernachlässigen darf; Herr Küster hat in der Diskussion nach seinem Vortrag offen zugestanden, daß es hier bei der Polizei sicherlich einen Nachholbedarf gibt. Auch für uns muß gelten, wie es vorhin Präsident Dr. Boge unterstrichen hat: Nicht alles, was machbar ist, sollte auch realisiert werden. Die Optimierung der polizeilichen Funktionsfähigkeit findet ihre Legitimation und ihre Begrenzung in der Wertordnung unserer Verfassung.

Mir bleibt noch, im Auftrag des aus akutem Anlaß verhinderten Präsidenten Dr. Boge, allen Vortragenden, allen an den Arbeitsgruppen und an den Diskussionen Beteiligten, dem Auditorium, den Kollegen, Mitarbeiterinnen und Mitarbeitern, die alle zum Gelingen der Tagung beigetragen haben, meinen herzlichen Dank auszusprechen. Allen Gästen des Bundeskriminalamtes wünsche ich eine gute Heimfahrt.

Verzeichnis der Verfasser

Boge, Heinrich, Dr. jur.

Präsident des BKA (seit April 1981). Zuvor (ab Oktober 1978) Ministerialdirektor und Abteilungsleiter P (Polizeiangelegenheiten) im Bundesministerium des Innern. Im Polizeidienst seit 1950; neun Jahre Polizeipräsident in Hannover; langjährige Lehrtätigkeit an der Landespolizeischule Niedersachsen, zuletzt als Leiter des Schulstabes und Vertreter des Schulleiters in Exekutivangelegenheiten.

6200 Wiesbaden, Thaerstraße 11

Bull, Hans Peter, Dr. jur.

Bundesbeauftragter für den Datenschutz (seit 1978); o. Professor für Öffentliches Recht an der Universität Hamburg (seit 1973). Zuvor: wiss. Assistent an der Handelskammer Hamburg und an der Universität Hamburg; 1972 Habilitation für Staats- und Verwaltungsrecht; Mitarbeit am Aufbau des Fachbereichs Rechtswissenschaft II der Universität Hamburg.

5300 Bonn-Bad Godesberg, Stephan-Lochner-Str. 2

Bunge, Ernst, Dr.-Ing.

Ltd. wiss. Direktor im BKA; Leiter der Gruppe "Technische Forschung und Entwicklung" im BKA. Zuvor Projektleiter und Senior Scientist im Philips Forschungslabor Hamburg; parallel dazu Lehrbeauftragter an der Universität Hamburg. Freier wiss. Gutachter für das BMFT. Zahlreiche Veröffentlichungen und Patente über angewandte Mustererkennung und Sprecheridentifizierung.

6200 Wiesbaden, Thaerstraße 11

Bux, Kuno

Präsident des LKA Baden-Württemberg (seit 1971). 1949 bis 1953 Schutzpolizei- und Kriminalbeamter. 1960 bis 1964 Staatsanwalt in Ellwangen/Jagst und Stuttgart; ab 1964 Stellvertreter des Leiters des LKA BW. Veröffentlichungen u.a. zu polizeilichen Organisationsproblemen und Fahndungsmaßnahmen.

7000 Stuttgart 50, Taubenheimstraße 85

Ernesti, Günter, Dr. jur.

Leitender Oberstaatsanwalt bei der Staatsanwaltschaft bei dem Schleswig-Holsteinischen Oberlandesgericht; Abteilungsleiter I; Leiter der Arbeitsgruppe EDV beim Generalstaatsanwalt; Rechtsprechungsübersichten, Einzeluntersuchungen.

2380 Schleswig, Gottorfstraße 2

Gehnich, Anna-Greta

Abteilungsdirektor im Reichspolizeiamt Schweden. Von 1966 bis 1981 Leiter der Systemgruppe für die Entwicklung polizeilicher Informationssysteme. Seit Anfang 1981 als Systemexperte mit der Entwicklung eines Projekts für ein neues Informationssystem beauftragt, das an die Stelle mehrerer bisheriger EDV-Systeme treten soll.

S - 102 26 Stockholm, Box 12256

Gnad, Thomas

Kriminaldirektor, Ständiger Vertreter des Direktors der Hessischen Polizeischule (seit 1979); zuvor (1975 bis 1979) Leiter der Abteilung "Kriminalpolizeiliche Ausbildung" an der Hessischen Polizeischule; davor Abteilungsleiter (Ermittlungs- und Meldedienst) beim Hessischen LKA. Eintritt in die hessische Polizei 1953.

6200 Wiesbaden, Schönbergstraße 100

Julich, Horst

Ltd. Regierungsdirektor im Kraftfahrt-Bundesamt; Eintritt in den Bundesdienst 1966; Justitiar und Organisationsreferent beim Kraftfahrt-Bundesamt bis 1974. Seitdem Leiter der Abteilung Zentrale Dienste, der u.a. das Referat "Datenverarbeitung" angehört. Leiter eines mehrjährigen Entwicklungsprojekts im Auftrag des BMFT.

2390 Flensburg, Fördestraße 16

Kaesehagen, Hans-Georg

Polizeipräsident in Mainz (seit 1968); 1956 - 1957 Jurist beim Verband der Textilindustrie Westfalen, Münster; ab 1957 in der allgemeinen inneren Verwaltung Rheinland-Pfalz, 1958 - 1968 Referent im Innenministerium Rheinland-Pfalz (Zivile Notstandsplanung und Katastrophenschutz).

Krückeberg, Fritz, Dr. rer. nat.

Institutsleiter am Institut für Informationssysteme und Grafische Datenverarbeitung der GMD; o. Professor an der Universität Bonn (seit 1970). Fachliche Arbeitsgebiete: Angewandte Mathematik für die Informatik, die Praxis der Gestaltung und Einführung von Büroinformations- und -kommunikationssystemen. Studium der Mathematik und Physik, Industriemathematiker in der BASF (Ludwigshafen), Dozent und Rechenzentrumsleiter an der Universität Bonn, 1970 bis 1981 wissenschaftlich-technischer Geschäftsführer der GMD.

5205 St. Augustin 1, Postfach 12 40

Kube, Edwin, Dr. jur.

Abteilungspräsident im BKA, Leiter der Abteilung "Kriminalistisches Institut"(seit April 1982); zuvor Leiter der kriminalistisch-kriminologischen Forschungsgruppe im BKA. Lehrbeauftragter der Universität Gießen. Bis 1974 Professor für Verwaltungslehre an der Fachhochschule für öffentliche Verwaltung, Kehl. Veröffentlichungen insbes. zu kriminalistisch-kriminologischen Fragen; Tagungsleiter.

6200 Wiesbaden, Thaerstraße 11

Küster, Dieter

Leitender Kriminaldirektor im BKA; Leiter der Abteilung Datenverarbeitung im Bundeskriminalamt. Kriminalbeamter seit 1965. Vorsitzender der Kommission DV-Planung der Arbeitsgemeinschaft der Leiter der Landeskriminalämter mit dem Bundeskriminalamt (AG Kripo).

6200 Wiesbaden, Thaerstraße 11

Laufs, Paul, Dr.-Ing.

Mitglied des Deutschen Bundestages (seit 1976); Mitglied des Innenausschusses. Diplomingenieur; 1963 bis 1967 wiss. Assistent am Institut für Aerodynamik und Gasdynamik und 1967 - 1973 Lehrbeauftragter für Hyperschallströmungen an der Universität Stuttgart; seit 1967 Angestellter bei IBM Deutschland.

5300 Bonn, Bundeshaus

Lehmann, Gerd

Polizeidirektor im LKA Nordrhein-Westfalen; Dezernent für ADV-Unterstützung bei Führung und Einsatz. Zuvor (1973 - 1975) Schutzbereichsleiter beim Polizeipräsidenten in Düsseldorf, davor Tätigkeit im Einsatzreferat des Innenministeriums Nordrhein-Westfalen.

Düsseldorf, Völklinger Straße 49

Lindlau, Dagobert

Chefreporter beim Bayerischen Rundfunk. Nach einer Ausbildung beim Spielfilm und bei der Zeitung seit 1954 beim Fernsehen tätig - u.a. als Leiter der Sendungen Report und Tagesschau, als Berichterstatter aus den USA und dem Nahen Osten, als Moderator des "Weltspiegel"; daneben schriftstellerische Arbeit für Bühne und Film.

8000 München 2, Rundfunkplatz 1

Neu, Herbert

Ehemal. stellvertr. Leiter der FDP-Fraktion im Landtag Nordrhein-Westfalen und deren innenpolitischer Sprecher (bis 1980).

4224 Hünxe, Dorfstraße 1

Simitis, Spiros, Dr. jur.

Hessischer Datenschutzbeauftragter (seit 1975); o. Professor f. Bürgerl. und Arbeitsrecht an der Universität Frankfurt a.M. (seit 1969). Gastprofessuren in London (1966) und Berkeley (1975), ständige Gastprofessur an der Universität Yale. 1966 - 1981 Generalsekretär der Intern. Zivilstandskommission. Buchveröffentlichungen auf dem Gebiet des Datenschutzrechts; Mitherausgeber eines Kommentars zum Bundesdatenschutzgesetz.

6200 Wiesbaden, Mainzer Straße 19

Spranger, Carl-Dieter

Parlamentarischer Staatssekretär im Bundesministerium des Innern (seit Okt. 1982). Mitglied des Deutschen Bundestages ab 1972. Seit 1977 Rechtsanwalt, zuvor Landgerichtsrat (ab 1969), davor u.a. Staatsanwalt und hauptamtl. Assistent für Zivilrecht an der Universität Erlangen-Nürnberg.

5300 Bonn, Graurheindorfer Straße 198

Stuff, Hans-Georg

Kriminaldirektor im KPA Schleswig-Holstein, Leiter des Dezernats Informationsverarbeitung. Eintritt in die Polizei 1951; seit 1968 mit der Entwicklung und Einführung polizeilicher Informationssysteme in Schleswig-Holstein beauftragt. Als Mitglied der Kommission Planung an der INPOL-Entwicklung beteiligt. Veröffentlichungen zu diesem Themenkreis in polizeilichen Fachzeitschriften.

2300 Kiel, Mühlenweg 166

Tolksdorf, Herbert

Vizepräsident des BKA (seit Okt. 1981); zuvor (ab 1979) Hauptabteilungsleiter, davor Leiter der Abteilung Datenverarbeitung im BKA (1972 - 1979). Bis 1972 Leiter des Fachbereichs Ausbildung im BKA, davor (1959 - 1964) Lehrtätigkeit an der Polizei-Führungsakademie Hiltrup.

6200 Wiesbaden, Thaerstraße 11

Wernitz, Axel, Dr. rer. pol.

Mitglied des Deutschen Bundestages (seit 1972), Vorsitzender des Innenausschusses. Zuvor, nach Studium der Wirtschaftswissenschaften, Geschichte und Publizistik an der Universität Erlangen-Nürnberg, Examen als Diplomkaufmann und Promotion; 1967 Akademischer Rat der Universität Regensburg; 1970 - 1972 Mitglied des Bayerischen Landtages.

5300 Bonn, Bundeshaus

Weyer, Heinrich, Dr. jur.

Landesbeauftragter für den Datenschutz Nordrhein-Westfalen (seit September 1979). 1960 - 1963 Bundeskartellamt; 1963 - 1969 Senatsverwaltung für Finanzen des Landes Berlin; 1969 - 1970 Bundesministerium des Innern; 1970 - 1979 Senatsdirektor der Senatsverwaltung für Bundesangelegenheiten des Landes Berlin.

4000 Düsseldorf 1, Elisabethstraße 12