„Das Stahlnetz stülpt sich über uns"

Die westdeutschen Polizei- und Geheimdienst-Computer (IV): Pannen und Mißbrauch

Wer sagt uns eigentlich", sorgt sich im Zimmer 4441 des Bundesamtes für Verfassungsschutz ein hoher Geheimdienstler, „daß ein Mann wie Guillaume nur das Kanzleramt unterwandern kann? Wer garantiert uns denn, daß hier bei uns im Haus nicht auch so einer sitzt?"

Die stete Furcht der Spionageabwehr, selber infiltriert zu sein, hat in den EDV-Räumen der Kölner Geheimdienstzentrale Einzigartiges entstehen lassen: Die Datenbank des „Nachrichtendienstlichen Informationssystems" (Nadis) ist unter Westdeutschlands 150 000 Computern jener „mit den vermutlich am weitesten vorangetriebenen Sicherungsvorkehrungen".

„Zugangskontrollen, Abgangskontrollen, Speicherkontrollen, Benutzerkontrollen, Zugriffskontrollen, Übermittlungskontrollen, Eingabekontrollen, Transportkontrollen, Organisationskontrollen" — neunfache Sicherung soll verhindern, daß ein unbekannter Agent auf Knopfdruck vieles von dem erfährt, was die bundesdeutschen Geheimdienste über ihre Gegenspieler im Osten wissen.

Die Nadis-Datengruppen, durchweg streng voneinander abgeschottet, sind nur Spezialisten zugänglich. Ihre Abfrageberechtigung müssen sie immer aufs neue durch kodierte Ausweise und wechselnde Paßworte nachweisen. Und sollte wirklich einmal ein Könner wie Heinz Felfe, der sich einst in den Bundesnachrichtendienst einschlich, „jede Menge Anfragen für die DDR starten und dann verschwinden", könnten die Kölner immerhin „rekonstruieren, was er mitgenommen hat".

Denn „jede Anfrage, jede Löschung, jede Veränderung", erklärt der Elektronik-Chef des Amtes, „wird maschinell dokumentiert, so daß noch nach Jahren bis auf die Sekunde genau rückgeschlossen werden kann, wer wann wie mit dem System umgegangen ist".

Ähnlich wie beim BfV soll es zugehen, wo immer Behörden heikles Wissen über Bürger speichern. Denn, so argumentieren Datenschützer, wenn schon sensitive Angaben über Verdächtigungen und Vorstrafen, Gesundheit und Gesinnung elektronisch erfaßt werden, dann sollten derlei Daten wenigstens perfekt gegen unbefugten Zugriff gesichert sein — weniger aus Spionagefurcht als aus Respekt vor den Persönlichkeitsrechten der Bürger.

Gerade die Sicherheitsbehörden dürften, fordert der hessische Datenschutzbeauftragte Professor Spiros Simitis, „nicht zu einer Art Schaltstelle werden", über die Internes „zu anderen Behörden oder zu Dritten gelangt". Denn bei Polizei und Geheimdiensten lagern millionenfach Personaldaten, die von den Betroffenen mangels eines Auskunftsrechts niemals auf ihre Richtigkeit überprüft werden können.

Datenband-Archiv: „Wollen Sie weitere Einzelheiten wissen?"

„Was die Polizei bekommt", verlangt Simitis, „muß auch bei der Polizei bleiben." Für Inpol, das „Informationssystem der Polizei", hat das Bundeskriminalamt denn auch ein „ebenso umfangreiches wie kompliziertes" Verfahren entwickelt, das nach den Worten des Bundeskripo-Präsidenten Horst Herold „den Zugang zum System durch Kodierungen, Berechtigungs- und Plausibilitätsprüfungen sichert, Antworten penibel selektiert und für Anfragen und Auskünfte ein Netz von Kontroll- und Überprüfungsroutinen knüpft".

Die Maschen sind mal enger, mal weiter — je nach Art der Informationen:

- ▷ Die gesamte Polizeiöffentlichkeit hat Zugang zu Inpol-Fahndungsdaten, entweder unmittelbar (über Terminal) oder mittelbar (per Funk-, Telephon- oder Telexkontakt mit einem Terminal);
- ▷ Sachbearbeiter etwa in Kripo-Kommissariaten dürfen darüber hinaus

Ein Mann auf dem Rückzug

Innenminister Baum und die Geheimdienst-Datenbanken

Am Montag letzter Woche meldeten Zeitungen und Rundfunkanstalten, was die Nachrichtenagentur „Associated Press" so zusammengefaßt hatte:

> Das Hamburger Nachrichtenmagazin DER SPIEGEL hält es für wahrscheinlich, daß Angaben über acht bis neun Millionen Menschen gespeichert sind. Das Blatt berichtet in seiner jüngsten Ausgabe, damit sei vermutlich jeder fünfte Erwachsene in der Bundesrepublik – „Überschneidungen berücksichtigt" – in den geheimen Datenbanken erfaßt ...

Die Bundesregierung reagierte am selben Tag. Nicht bestreiten konnte sie die Zahlenangaben des SPIEGEL. Gleichwohl ließ Innenminister Baum eine Erklärung veröffentlichen, die wie ein Dementi wirken sollte — aber keines war. Die Stellungnahme in der Version der Agentur Reuter:

> Das Bundesinnenministerium wies am Montag in Bonn entschieden den Vorwurf zurück, der Verfassungsschutz habe bei der Sammlung und Speicherung von Informationen rechtswidrig gehandelt . . . Demgegenüber hatte das Hamburger Magazin SPIEGEL in seiner neuesten Ausgabe behauptet, Nadis habe die Daten von etwa acht bis neun Millionen Bundesbürgern gespeichert*.

Zudem wies Baum auf den ersten Jahresbericht des Bundesdatenschutzbeauftragten Professor Hans Peter Bull hin. Dort heiße es zum Komplex Nadis:

> Eine zum jeweiligen Überprüfungszeitpunkt rechtsfehlerhafte Speicherung konnte ich nicht feststellen.

Diese Bemerkung Bulls allerdings erlaubt weniger Rückschlüsse auf Nadis als auf die Kontrollkapazitäten des Datenschutzbeauftragten. Über diese berichtet Bull im nächsten (von Baum nicht zitierten) Satz seines Jahresberichts:

> Zur Bewertung dieses Ergebnisses ist jedoch anzumerken, daß die Zahl der auf diese Weise durchgeführten Kontrollen noch gering ist und daß eine umfassende Nachprüfung in vielen Fällen . . . nicht möglich war (und ist).

Bull war im Geheimbereich auf „praktische Schwierigkeiten bei der Ausübung des Kontrollrechts" gestoßen. „Alle Ämter", urteilt der Regensburger EDV-Experte Professor Wilhelm Steinmüller, „haben enorme Möglichkeiten, die 16köpfige Datenschutztruppe des Bundes aufs Kreuz zu legen. Allein um das Programm eines nur mittelgroßen Computers ganz zu kapieren, braucht ein Fachmann mehrere Monate".

„Besondere Probleme" wirft für Bull die Rechtslage im Geheimbereich auf. Auch die Lösch-Praxis lasse zu wünschen übrig:

> Eine vollständige Bestandsüberprüfung in nicht zu langen Abständen ist, soweit ich sehe, in keinem Bereich bisher realisiert.

Zwar ist, was immer Bull an den Geheim-Computern kritisiert, durch „die geltenden Rechts- und Verwaltungsvorschriften" abgedeckt. Die Frage ist freilich, ob nicht ein Teil der Vorschriften unzureichend oder gar grundgesetzwidrig ist. Bull jedenfalls beanstandet beispielsweise, die Anweisungen über Weitergabe von Geheimdaten seien „nicht ausreichend". Für „fragwürdig" hält er den Zugang der Nadis-Behörden zu Inpol-Fahndungsdaten, deren Speicherung bei ihm teils „erhebliche Zweifel" auslöst.

Der Datenschützer resümiert, „daß über weitere rechtliche Regelungen nachgedacht werden muß, welche die Tätigkeit der Verfassungsschutzbehörden (wie auch der übrigen Nachrichtendienste) verfassungskonform ordnen".

Vor wenigen Wochen noch sprach Minister Baum ähnlich; allein bei der Polizei wollte er „Millionen Akten" vernichtet wissen. Nach Krach mit dem Kanzler und dem Versetzungsbegehren des BKA-Chefs Herold jedoch scheint der Innenminister den Rückzug angetreten zu haben. Ein „Prüfbericht" seines Hauses, dessen Vorwürfe gegen das BKA er teilweise nicht aufrechterhalten konnte, schwächte Baums Position zusätzlich.

Seither versäumt der einst so forsche Liberale („Stern": „Ein Mann räumt auf") kaum eine passende oder unpassende Gelegenheit, den Geheimbehörden sein „Vertrauen" auszusprechen.

Am selben Tag, an dem Baum sich zur SPIEGEL-Serie äußerte, beschloß der Bundesvorstand der FDP, dem Parteitag Mitte Juni einen Leitantrag zum Thema Datenschutz im Geheimbereich vorzulegen. Schwerpunkte: neue Vorschriften für die Ämter, mehr Kompetenzen für Bull.

* Reuter zitiert falsch: Die Zahlen bezogen sich auf Geheimdienst- und Polizei-Computer.

Daten aus dem Haft-, dem Daktyloskopie- und dem Straftaten-/Straftäter-Computer abfragen;

▷ einige Dutzend ausgewählter Spezialisten in Verfassungs- und Staatsschutzämtern schließlich können sich auch der „Pios"-Datei bedienen, die auf „Personen, Institutionen, Objekte, Sachen" aus der Terrorismus-Szene verweist.

Protokolliert wird bei der Polizei freilich nur ein Teil der Anfragen, beispielsweise an den Straftäter-Computer. Auskunftsersuchen an Pios oder an die Fahndungsdatei dagegen sind nicht im einzelnen rekonstruierbar. Und trotz aller Sicherungsvorkehrungen verbleibt „ein Bereich, in dem wir den Polizeibeamten Vertrauen schenken müssen" (Herold).

In genau dieser Zone geschehen immer wieder Pannen. Ursache sind in den meisten Fällen, wie ein hoher Kripo-Beamter formuliert, „nicht die Elektronenhirne, sondern menschliche Hirne".

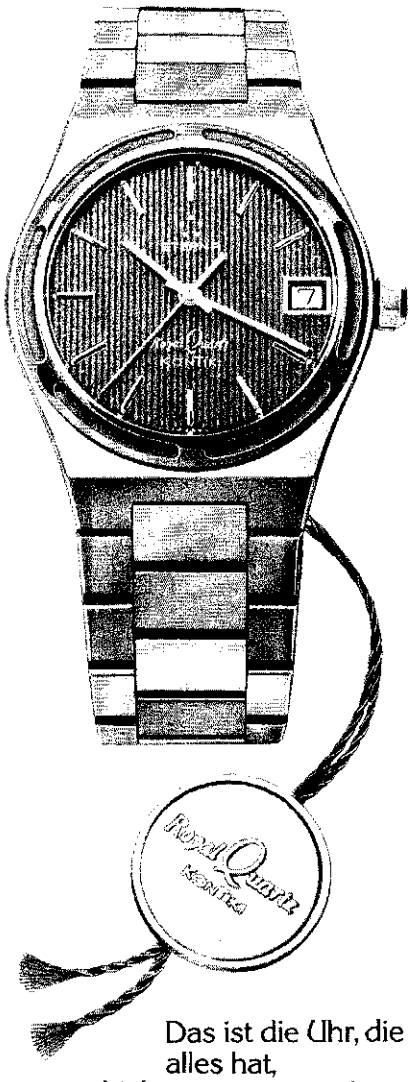
Entschuldbar vielleicht noch, wenn, so geschehen letztes Jahr in Koblenz, eine Fernschreiberin versehentlich einen Bericht über „Fahndungsmaßnahmen nach Terroristen" („VS-Vertraulich — Nur für den Dienstgebrauch") an einen Frankfurter Geschäftsmann tickert. Er wurde, als die Dame den Irrtum bemerkte, per Telex gebeten: „Bitte vernichten, war nicht für Sie bestimmt."

Gefährliche Folgen indes hätte haben können, was im Sommer 1977 in

* An einem Grenzschutz-Terminal.

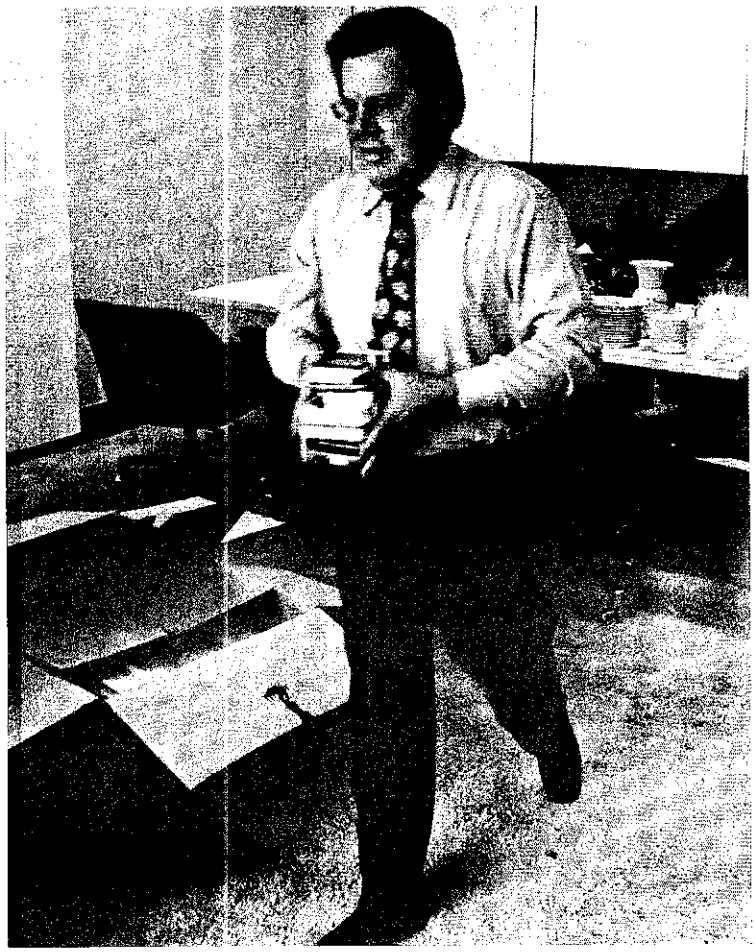
Freidemokrat Baum*
Vertrauen zum Geheimdienst

Für Menschen, die das Besondere suchen: Royal Quartz KonTiki. Eine echte ETERNA. Aus der Schweiz.



Das ist die Uhr, die alles hat, was es bisher zusammen in einer Uhr nicht gab. Wasserdicht wie eine Taucheruhr.
Dabei von höchster Eleganz und superflach.
Für Damen und Herren – in Edelstahl, Gold 18 Karat und Gold/Stahl.
Erhältlich nur in erstklassigen Fachgeschäften.

ETERNA
Die Uhr. Schönheit und Technik in Vollendung.



Spion Guillaume: Ostagenten im Verfassungsschutz?

München passierte: Dort fanden sich zwischen Haushaltsmüll Daten aus dem bayrischen Landeskriminalamt — darunter Blätter mit Observationsergebnissen und mit Anschriften von Bürgern, die der Polizei vertrauliche Hinweise gegeben hatten.

Die bislang größte Blamage aber fügte letztes Jahr der Bielefelder Kfz-Mechaniker Bodo Plasa, 31, der Polizei zu. Er demonstrierte, daß es jedermann möglich war, „unter Vorspiegelung einer Berechtigung" per Telephon „Informationen aus Datenbeständen des Inpol-Systems" zu ergattern, wie Bonns Innen-Staatssekretär Andreas von Schoeler vor dem Bundestag zugab.

Für zwanzig Pfennig Inpol-Daten ergattert.

Plasa hatte wissen wollen, warum sein Arbeitgeber mit den Lohnzahlungen in Verzug geraten war. Aus Neugier wählte er 54 51, die Nummer der Bielefelder Polizei, ließ sich die „EDV-Abteilung" geben und verlangte „mit markiger Stimme" eine „Personenüberprüfung".

Prompt erfuhr Plasa („Ich traute meinen Ohren nicht"), daß seinem damaligen Chef diverse Delikte — von Hehlerei bis zum Widerstand gegen Vollstreckungsbeamte — angelastet wurden. „Wollen Sie noch weitere Einzelheiten wissen", fragte ihn eine weibliche Stimme, „dann hole ich die Akte."

Ermutigt von diesem Erfolg, wiederholte Plasa sein Experiment „in verschiedenen Bundesländern" (Schoeler). Inpol-Daten für zwanzig Pfennig gab es, wie eine Stichprobe für die Illustrierte „Stern" erwies, unter anderem in Nürnberg und Osnabrück, Kempten und Schweinfurt, Wiesbaden und Heidelberg.

In Düsseldorf, eröffnete ein Polizei-Elektroniker letzte Woche dem SPIEGEL, können Außenstehende telephonisch nach wie vor Fahndungsdaten abrufen, „wenn sie zum Beispiel einen künstlichen Geräusch-Background unterlegten, der uns dann dazu verleiten könnte, sie als Insider zu betrachten". Aber: „Wer länger bei uns ist, kennt auch die Stimmen möglicher Anrufer. Ich persönlich mache so etwas nur gegen Rückruf. Eine bindende Verpflichtung gibt es aber nicht."

Solche Lücken im Sicherungssystem lassen sich relativ einfach schließen. In einigen Bundesländern hat die Polizei inzwischen, so Hessens Simitis, „täglich wechselnde Codeworte" eingeführt,

mit denen sich Anrufer zu legitimieren haben.

Verhindert wird auf diese Weise indes nur eine von vielen Mißbrauchsmöglichkeiten. Zwar läßt sich mit Zugangssperren und Codierungen gewährleisten, daß nur Polizeibeamte an Polizeidaten kommen. Diese Verfahren schließen aber nicht aus, daß ein zugriffsberechtigter Beamter die abgerufenen Informationen unrechtmäßig nutzt.

Datenschützer wie Simitis fordern daher eine generelle „Protokollierung der Übermittlung" und eine weitgehende „Beschränkung des Zugriffsrechts auf bestimmte, einer besonderen Auswahl unterzogene Beamte".

An Versuchen, Inpol-Daten unrechtmäßig zu verwenden, hat es nicht gemangelt. In Hamburg wurde ein mit Spielschulden belasteter Operator ertappt, der sich angeboten hatte, gegen Geld die Strafdaten mehrerer Personen zu löschen. Und in Kiel stand der Chefoperator der schleswig-holsteinischen Datenzentrale vor Gericht, der Zugang zur „Personenerkenntnisdatei" (PED) der Kripo hatte.

Privatdetektive zapfen Polizei-Computer an.

Ein Urlaubsbekannter hatte an den EDV-Mann telephonisch den Wunsch mehrerer Gangster herangetragen, ihre Personendaten gegen gute Bezahlung aus dem Computer verschwinden zu lassen. Als sich der Operator daraufhin — wie er beteuerte, „aus Neugier" — an den Daten zu schaffen machte, stellten ihn Fahnder zur Rede. Die Polizei nämlich hatte, aus anderem Anlaß, alle Telephonate seines Urlaubsbekannten abgehört. (Weil so erworbenes Lauschmaterial jedoch nicht gerichtsverwertbar ist, mußte der Operator schließlich freigesprochen werden.)

Besonders schnell scheinen Beamte sich zur Datenweitergabe an Privatdetektive und Werkschützer bewegen zu lassen, in denen sie offenbar Quasi-Kollegen sehen. In Hamburg etwa wurde ein Kriminalkommissariatsleiter zu einem Jahr Freiheitsstrafe mit Bewährung verurteilt. Er hatte unter anderem dienstlich bezogene Informationen aus Datensammlungen von Krankenkassen und Auskunfteien für insgesamt 3500 Mark an einen Privatdetektiv verkauft.

Ein Frankfurter Schöffengericht verurteilte im Januar einen Kripo-Beamten zu neun Monaten Freiheitsstrafe mit Bewährung, der den hessischen Polizei-Computer „Hepolis" angezapft und Vorstrafen-Daten für 1400 Mark an eine Auskunftei verkauft hatte. Die wiederum gab die gestohlenen Informationen an einen Supermarkt-Chef weiter, der damit seinen Betriebsratsvorsitzenden und zwei andere Mitarbeiter unter Druck setzen wollte.

In Köln machten Betriebsräte schon vor Jahren publik, daß der Werkschutzleiter des Kabel-Konzerns Felten & Guilleaume, ein ehemaliger Polit-Polizist, eine 1150 Blatt umfassende Geheimkartei mit Vorstrafen von Belegschaftsmitgliedern führte — Daten, die nur aus Polizeiarchiven stammen konnten.

In Duisburg wurden im letzten Herbst die beiden Geschäftsführer der landesweit tätigen Großdetektei Kocks zu je einem Jahr Haft mit Bewährung und 18 000 beziehungsweise 10 000 Mark Geldstrafe verurteilt. Sie hatten Kriminalbeamte bestochen, das Schnüffelinstitut — unter Decknamen und auf Bestellung — mit Amtsdaten zu versorgen; Kocks ist vor allem auf „extrempolitische Überprüfungen" von Arbeitnehmern spezialisiert.

Wohin Datenschutz-Versäumnisse letztlich führen können, offenbarte sich 1976 auf das drastischste in der Schweiz. Dort hatte der rechtslastige Werbefachmann und Reserve-Oberstleutnant Ernst Cincera jahrelang Angaben über rund 10 000 linke und linksverdächtige Eidgenossen sammeln können.

In Cinceras schwarzer Datei — die von schweizerischen wie deutschen Unternehmern, Militärs und Politikern konsultiert wurde — fanden sich, als seine Arbeit 1976 durch ein „Mini-Watergate" (so die Landespresse) bekanntwurde, Personalien von Beziehern linker Zeitschriften sowie Bankauskünfte, dazu vertrauliche Unterlagen aus dem Berner Verteidigungsministerium und zuhauf Kopien von Polizeipapieren.

Die Gefahr, daß durch Indiskretion oder Korruption Geheimes aus Geheimcomputern in falsche Hände gerät, wird wachsen, wenn sich, wie geplant, die Zahl der mit Inpol verbundenen Datenstationen (zur Zeit rund 1600) verzehnfacht. „Je mehr Terminals angeschlossen sind", warnt Simitis, um so größer sind die Mißbrauchsgefahren."

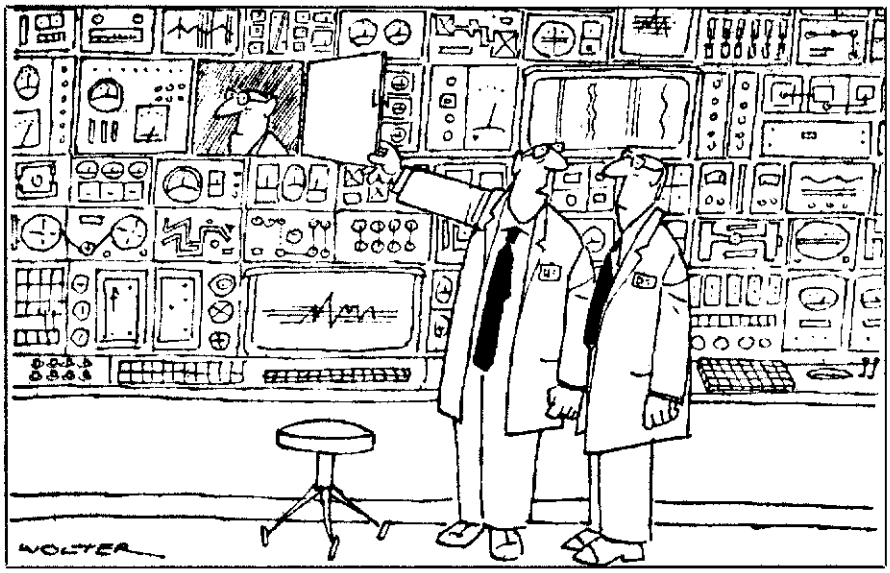
Zudem beunruhigt Datenschützer die Tendenz, den Polizisten am Endgerät den Zugriff zu immer mehr und immer umfangreicheren Daten zu gestatten. Am deutlichsten widerspiegelt der Zentrale Personen-Index (ZPI) des Inpol-Systems diese Entwicklung.

Schon jetzt verweist der ZPI auf mehr als zwei Millionen Kurz-Dossiers des BKA. Geplant ist, auch die Bestände der Landespolizeien, die zumeist eigene Indizes führen, auf den Bundescomputer zu übertragen. Der ZPI soll außerdem nicht nur mitteilen, *daß* und *wo*, sondern auch *welche* Erkenntnisse über jemanden vorliegen.

Jeder „Abfrageberechtigte" in Westdeutschland kann nach Abschluß der ZPI-Erweiterung über rund 3,5 Millionen Bundesbürger eine „Personenkurzauskunft" abrufen; sie soll laut Innenministerium „Kurzangaben über den Inhalt der anderen Dateien" des BKA enthalten.

„Aus polizeilicher Sicht", teilt das Ministerium mit, bestünden an der „Nützlichkeit" des ZPI „keine Zweifel". Aus der Perspektive von Datenschützern jedoch, notierte die Hamburger „Zeit", zeichne sich auch in dieser Datei schon das „Skelett des Großen Bruders" ab.

Politisch weitaus am riskantesten muten die Datenbanken der Geheimdienste an. Sie sind zwar perfekt gegen die Gefahr gesichert, von Unbefugten angezapft zu werden. Doch die Abfragebefugten hindert kaum etwas daran, die Computer einzusetzen, um etwa mißliebige Bürger mundtot zu machen — bewährtes politisches Kampfmittel nicht nur in den USA, deren Präsident



Kieler Nachrichten

„Ich habe die Fehlerquelle gefunden: ein total veraltetes Einbauteil"

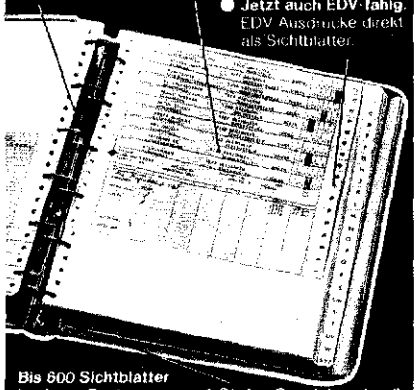
Das "Ein-Blick" Kartei-Buch

Das Novo-sicht-System macht Vertrieb und Organisation effektiver: es ist praktisch und übersichtlich, handlich und informativ, raumsparend und rationell. Daten, Umsätze, Termine, Gesprächspartner: Im Augenblick ist alles erfaßt.
Für den Außendienst, für Lager-, Lieferanten-, Personal-, Ersatzteil-Verzeichnisse.

Mechanik mit 1/2 oder 3/8" Abständen

Schuppenartige Blatt-Anordnung: Sekundenschnelles Zurechtfinden

● Jetzt auch EDV-fähig. EDV Ausdrucke direkt als Sichtblatter.



Bis 600 Sichtblätter in einem Buch: Jederzeit die gesamte Kundenkartei im Griff

2-Stufen-Spezialmechanik: Zum Schreiben und Blattauswechseln

NOVO sicht

rationalisiert den Vertrieb

NH 78/1a

Novo-sicht Ideale Buchkartei für Reisende. EDV-fähig

Novo-data EDV-Arbeitsbuch für ungetrennter/getrennte EDV-Listen

Novo-norm Ring-Handbuch für Kataloge, Arbeitsnormen usw.

Einsenden an
Novo Organisationsmittel GmbH
Abt. 65 Postf. 2069, 5300 Bonn 1

Bitte Informationen über:
● Novo-sicht ● Novo-data ● Novo-norm

Firma:

z. Händen:

Anschrift:

Nixon einst gezielt medizinische und polizeiliche Daten über seine innenpolitischen Gegner sammeln ließ.

Auch in der bundesdeutschen Nachkriegsgeschichte versuchten Parteipolitiker und die ihnen verbundenen „Seilschaften" in den Sicherheitsbehörden häufig aus ihrem Wissen politisches Kapital zu schlagen. Bereits 1954, in einer Verfassungsschutzdebatte des Bundestages, hatte Carlo Schmid vor der Gefahr gewarnt, daß Geheimdienst-Informationen mißbraucht werden könnten: „Man kann einen Menschen auch mit anderen Mitteln fertigmachen als mit Konzentrationslagern", sprach der Sozialdemokrat, „zum Beispiel damit, daß man ihn hinter dem Stacheldraht des Verdachts verschwinden läßt."

Der Bundesnachrichtendienst, der in den fünfziger und sechziger Jahren unter General Gehlen entgegen seinem politischen Auftrag auch „Inlandsaufklärung" betrieb, mischte sich immer wieder in die Bonner Politik ein — bisweilen, wie sich Ex-Verfassungsschützer Nollau erinnert, mit der Methode, „dem einen eine Frau und dem anderen SED-Kontakte anzuhängen".

Innerparteiliche Flügelkämpfe mit Material vom Verfassungsschutz.

Verfassungsschützer wiederum lieferten jahrelang zum Beispiel West-Berliner SPD-Politikern Material, mit dem sich innerparteiliche Flügelkämpfe bestreiten ließen; die dortige FDP forderte beim Geheimdienst Expertisen über neue Mitglieder an. In Hamburgs sozialliberaler Koalition kriselte es 1974, als der damalige Innensenator und heutige Bürgermeister Klose die Karriere des FDP-Fraktionsvize Gerhard Weber mit der Andeutung zu bremsen versuchte, der Linksliberale gelte dem Verfassungsschutz als „Sicherheitsrisiko".

In Bremen bemühten sich Landespolitiker im Wahlkampf 1971, mit windigen Polizeipapieren den linken Bremer Innen-Senatsdirektor Waldemar Klischies in die Nähe von BM-Terroristen zu rücken. Und in Bonn war letztes Jahr die mit Geheimdienst-Material angeheizte Kampagne gegen den SPD-Abgeordneten Uwe Holtz das vorerst letzte Glied in einer langen Kette ähnlich konstruierter Affären.

Solche Fälle veranlassen Datenschützer zu der Forderung, Geheim-Informationen dürften nicht allein durch amtsinterne Vorschriften und technische Vorrichtungen geschützt werden; vonnöten seien präzise formulierte Gesetze. Bislang ist die Weitergabe von „Erkenntnissen" an Dritte höchst unterschiedlich und unzureichend geregelt.

Nach Ansicht von Bundes-Verfassungsschützern ist es zulässig, wenn das

Geheimdienstler Nollau (1974)
„Dem einen eine Frau anhängen ...

Amt „Parteien, Gewerkschaften und Verbände" oder auch „wichtige Versorgungs- und Rüstungsbetriebe" über Extremistisches informiert. „Die Nachteile, die dem einzelnen, etwa einem Arbeitnehmer, entstehen können", müßten allerdings, so BfV-Regierungsdirektor Bernd-Dieter Kortmann, abgewogen werden gegen die „Bedeutung der Gefahr für den Staat".

Datenschützer dagegen möchten diese schwierige Abwägung nicht den Geheimdienstlern überlassen. Denn wenn Behörden Erkenntnisse beispielsweise an Firmen weitergeben, können Arbeitnehmer allzuleicht in eine ausweglose Lage geraten: Aufgrund dieser staatlichen Intervention droht ihnen in der Regel eine (mit Vorwänden begründete) Kündigung, deren Anlaß sie weder

Geheimdienstler Gehlen (1972)
... und dem anderen SED-Kontakte"

verwaltungs- noch arbeitsgerichtlich nachprüfen lassen können.

Zwar schreibt eine BfV-„Dienstvorschrift für die Auswertung" vor, daß an externe Stellen nur „gesicherte" Erkenntnisse weitergereicht werden dürfen. Werde im Einzelfall dennoch auch einmal Ungesichertes übermittelt, so seien stets die „Zweifel an der Richtigkeit" zum Ausdruck zu bringen.

Datenschützer Bull wendet jedoch ein, daß „selbst ein mit Vorbehalten versehener Bericht einer Verfassungsschutzbehörde im Ergebnis den Betroffenen nachhaltig belasten kann": „Die empfangenden Stellen werden das vorgelegte Material vielfach nicht mehr objektiv prüfen, sondern bereits die Tatsache, daß überhaupt Erkenntnisse vorliegen, zum Nachteil des Betroffenen verwerten."

Fehlleistungen können, etwa bei der Praktizierung des Radikalenbeschlusses, auch dadurch begünstigt werden, daß Verfassungsschützer „die Betroffenen nicht persönlich kennen" und ihnen häufig „relevante Unterlagen fehlen" (Bull).

Geheimdienstler unterlaufen den Willen des Gesetzgebers.

Bonns Datenschützer verweist denn auch auf eine Entscheidung des Oberverwaltungsgerichts Berlin. Das hat im letzten Jahr festgestellt, Geheimdienst-Informationen dürften erst dann Dritten überlassen werden, wenn das Material „den Schluß einer verfassungsfeindlichen, die demokratischen Freiheiten zielstrebig untergrabenden Hetze oder eines tätlichen Angriffs *zuverlässig*" begründe.

Nach Datenschützer-Ansicht sollte grundsätzlich jede Weitergabe geheimer Daten von Politikern verantwortet werden — ein Verfahren, wie es bislang lediglich einige Landesparlamente gesetzlich fixiert haben*.

Mit einem simplen Trick jedoch können Geheimdienstler in diesen Bundesländern den Willen des Gesetzgebers unterlaufen: Sie schicken das Material, ganz legal, an das Kölner Bundesamt oder an ein Landesamt, das derartigen Einschränkungen nicht unterliegt — „vielleicht sogar in Kenntnis des Umstandes, daß diese Behörden dann die Dritten, zum Beispiel Parteien, Gewerkschaften, Verbände, Betriebe, befreundete Dienste, informieren" (Verfassungsschützer Kortmann).

* Restriktive Vorschriften enthalten die Landesverfassungsschutzgesetze von Baden-Württemberg, Hamburg und Niedersachsen. Erkenntnisse dürfen dort an andere als staatliche Stellen grundsätzlich nicht weitergegeben werden; über Ausnahmen „zum Schutz der freiheitlichen demokratischen Grundordnung, des Bestandes oder der Sicherheit des Bundes oder eines Landes" entscheidet in diesen Ländern der Innenminister beziehungsweise -senator oder sein ständiger Vertreter. Bremen und Rheinland-Pfalz dagegen lassen eine Weitergabe grundsätzlich zu, Bremen allerdings nur mit Einwilligung des Innensenators.

Vollends zur Farce würden die vereinzelten landesrechtlichen Weitergabe-Beschränkungen, wenn — so Hamburgs Innensenator Werner Staak — das Bundesamt sich mit seiner Forderung durchsetzt, „Zugriff auf die in den Ländern gespeicherten Daten zu bekommen".

„Wir hielten es für falsch", protestiert der Sozialdemokrat, „wenn ohne unsere Zustimmung irgend jemand, meinetwegen in München, an unsere Daten herankommen könnte." Verzieht jemand aus der eher liberalen Hansestadt, wo „Demonstrationsdelikte und andere Jugendsünden nicht mehr relevant sind", in den schwarzen

Metall

Süden der Republik, so soll er, meint Staak, davor bewahrt werden, daß ihm via Köln sein Datenschatten folgt.

Auch aus anderem Grund kann sich, im Einzelfall, Daten-Transfer im Geheimbereich als riskant erweisen: Seit Informationen, dank EDV, Raum und Zeit überwinden können, haben sich die Tragweite und die Lebensdauer von Fehlern vervielfacht.

Unbehaglich stimmen Datenschützer Computer-Pannen jener Art, wie sie aus zivilen Datenbanken häufig bekanntwerden — etwa wenn das Mainzer Landesrechenzentrum dem lokalen Kardinal Hermann Volk in einem amtlichen Bescheid ein Kind zuschreibt, das im selben Arbeitsgang einem gleichnamigen Ehemann aus einem Mainzer Vorort elektronisch entführt wurde.

So grotesk solche Kardinalfehler anmuten, „so unangenehm wäre es", schreibt der Hamburger EDV-Autor Gerd E. Hoffmann, „wenn einem nicht vorbestraften Bürger Müller über den elektronischen Weg die Vorstrafen eines anderen Müller zugeschoben werden". Ob eine Bank dann Müllers Kreditwürdigkeit recherchiert oder ein künftiger Arbeitgeber Müllers Leumund — in der Regel würde der Verwechselte von dem Irrtum nichts erfahren.

Wie leicht jemand zu Unrecht sogar in den Nadis-Computer des Verfassungsschutzes geraten kann, bekam 1977 die Pirmasenser Lehramtskandidatin Angelika Boppel zu spüren. Als sie sich um einen Aushilfsvertrag als Sportlehrerin bewarb, eröffnete ihr die Bezirksregierung, sie könne die Stelle nicht bekommen. Vom Verfassungsschutz seien „Einwendungen" erhoben worden.

Frau Boppel habe — so der in Nadis registrierte Vorwurf — gemeinsam mit ihrem Bruder auf einem Pirmasenser Schulhof die von einem „Sozialistischen Arbeitskreis" herausgegebene Schülerzeitschrift „Knüppel aus dem Sack" verteilt. Erst als die Lehramtsbewerberin einen Anwalt einschaltete, stellte sich heraus, daß beim Verfassungsschutz, so ein Amtssprecher, „eine unangenehme Geschichte passiert" war: Ein V-Mann hatte die junge Frau schlicht mit einer anderen verwechselt.

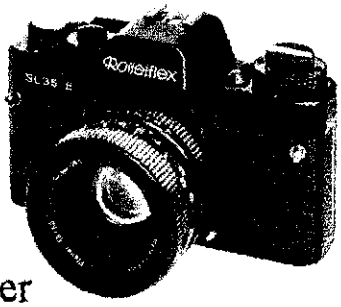
Pannen produzieren kann auch ein Verfahren, das im Jargon der Grauzone „Lumpenverwertung" heißt: Weil für Verfassungsschützer nicht das Legalitätsprinzip gilt und es ihnen daher freisteht, ob sie einen Tatverdächtigen bei der Staatsanwaltschaft anzeigen oder nicht, können sie mit Drohungen oder Versprechungen Auskünfte über das beobachtete Milieu erzwingen. Auch solche Hinweise, häufig unzuverlässig, landen in Nadis.

Doch selbst korrekt erhobene Daten können sich unter Umständen als lebensgefährlich erweisen — dann, wenn sie verkürzt oder verschlüsselt gespeichert, von Dritten abgerufen und prompt mißverstanden werden.

Auf welche Weise so entstandene „Datenkrüppel" zu Irrtümern führen können, erhellt ein Beispiel, das ein Beamter der Berliner Innenbehörde überliefert: In den Jahren des Aufbaus polizeilicher Datenbanken habe ein inter-

Sie erkennen.

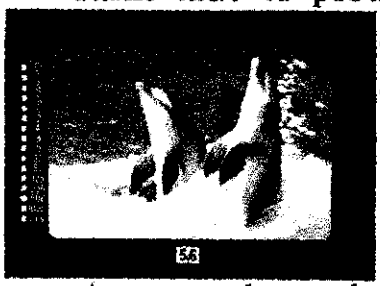
Hier geht es um die Entdeckung der neuen Rolleiflex SL 35 E.



„He Tom, neue Kamera?" sage ich. Sein Boot ist zurück. Zurück von den Delphinen. Er ist besessen von ihnen. Er studiert sie.

Auf der Kamera in seiner Hand lese ich Rolleiflex SL 35 E. Und ich bin gespannt: „Warum die?" Er: *„Sie liegt gut in der Hand."*

Später dann ein paar Einzelheiten: *„Auf dem neuesten Stand. Tut das Beste von sich aus. Ohne groß anzugeben. Vollelektronisch. Automatisch und manuell. Zeitautomatik von 16 sec bis Eintausendstel."* Und dann taut er plötzlich auf: *„Das Größte – Sonne voll drauf, sie springen, alles glitzert. Jetzt Wolke! Alles grau. Aber du behältst die Kamera vorm Auge. Nicht absetzen, um zu regulieren – vorm Auge regulierst du, und schießt. Du verlierst sie nicht, denn du siehst auf dem Sucherrahmen, was du regulierst. Du wählst Blende,, du siehst Blende – und Zeit leuchtet sofort und automatisch auf, rot auf dem Rahmen. – Und du folgst ihnen..."*



Das war Toms größte Rede. – Ergiebiger in den Details ist ein Rollei-Fachhändler! Fragen Sie ihn. Die Neugierde lohnt sich. Und dann: Nehmen Sie sie in die Hand! Entdecken Sie, was Fotografie heute leistet. Rolleiflex SL 35 E. Die neue vollelektronische Spiegelreflexkamera.

Nadis-Erfaßte Angelika Boppel
Vom V-Mann schlicht verwechselt

nes Kürzel je nach Bundesland Verschiedenes signalisiert — mal, daß jemand Inhaber eines Waffenscheins sei (etwa als Jäger), mal indes Gefährdung durch Gewalttäter: Vorsicht, Schußwaffengebrauch.

Werden „Bewertungen über Betroffene" gespeichert, müsse, fordert der Darmstädter Datenrechtler Professor Adalbert Podlech, stets „erkennbar sein, wer die Bewertung vorgenommen hat und wo die Erkenntnisse gespeichert sind, die der Bewertung zugrunde liegen".

Gefahr, wenn jemand „polizeibekannt" ist.

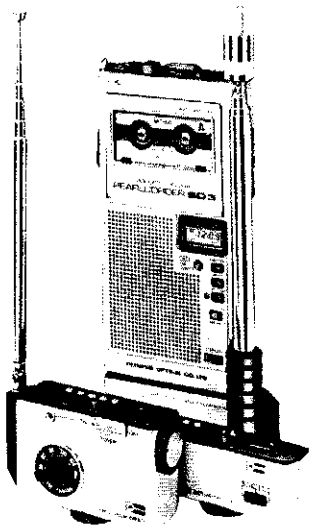
Kennzeichnungen wie „Simulant" oder „Süchtiger" dürfen nach Ansicht des Regensburger Datenschützers Professor Wilhelm Steinmüller „nur nach Durchlaufen eines Verfahrens in das System gelangen, das eine erhöhte Sicherheit gewährleistet". Sonst könne es geschehen, daß jemand von Polizisten als Schlägertyp eingestuft wird, nur weil er „vor zehn Jahren vielleicht ohne jedes Verschulden in eine Wirtshausschlägerei verstrickt und daraufhin polizeilich behandelt worden ist".

Selbst wenn es nicht elektronisch gespeichert ist, kann ein so harmlos anmutendes Prädikat wie „polizeibekannt" es in sich haben. Durch diese Krüppel-Information kam am 13.

Business, Time & Pleasure

Für Leute, die sich beim Genießen Zeit lassen.
Pearlcorder SD3, der faszinierende System-Radiorecorder mit gekoppelter LCD-Anzeige für die Funktionen: Zählwerk, Memory, Uhr, Stoppuhr, und Timer.

Verblüffend die Tontreue, exklusiv das Zubehör, z. B. adaptierbare UKW- oder MW-Tuner, Tonsensor für automatischen Aufnahme-Start/Stop etc. Mit umschaltbarer Bandlaufzeit der MICROCASSETTE, dem weltkleinsten Tonträger: von 2 x 30 auf 2 x 60 Minuten.
Olympus Optical Co. GmbH., Produktgruppe: Audio, Postfach 10 49 08, 2000 Hamburg 1, Tel.: 040/24 80 21



Pearlcorder SD3

April 1977 in Hessen der Schäfer Helmut Schlaudraff, 43, ums Leben.

An jenem Tage, kurz vor Einbruch der Dunkelheit, hatte Schlaudraff auf der Weide noch ein krankes Mutterschaf notschlachten müssen. Den Kadaver sowie zwei erfrorene Lämmer warf er auf einen Autoanhänger, den er auf einem Feldweg abstellte. Dann fuhr er mit seinem roten Mercedes 280 zum Abendessen in ein Restaurant.

Nachdem er gemeinsam mit zwei Bekannten das Gasthaus verlassen und den Hänger mit der stinkenden Ladung wieder angekuppelt hatte, wurde der Mercedes plötzlich von einem VW-Variant an den Straßenrand gedrängt. Ein Mann riß die Tür auf — „dann fiel ein Schuß", bezeugt eine Mitfahrerin, „es wurde kein Wort gesprochen".

Schlaudraff, von einer MP-Kugel am Hals getroffen, war sofort tot — Opfer nicht etwa eines Raubmordes, sondern wilder Informationsflüsse innerhalb der hessischen Polizei.

Denn eine Stunde zuvor hatten zivile Beamte in ihrem getarnten Fahrzeug „Nero 2/65" den abgestellten Anhänger mit den toten Tieren entdeckt und — weil in der Gegend 22 Schafe gestohlen worden waren — sogleich das Kennzeichen überprüft. Der Halter, ergab die gefunkte Kurzauskunft, sei „polizeibekannt".

Auf welche Weise freilich Schlaudraff polizeibekannt geworden war, teilte der Polizeifunk nicht mit, sondern, eine Woche später, ein Kripo-Sprecher: Der vermeintliche Viehdieb hatte „mehrfach Schafe aus seiner Herde als gestohlen gemeldet".

Tödliche Mißverständnisse könnten sich häufen, wenn erst ein Plan Realität ist, den Wiesbadener Terrorismus-Fahnder zur Diskussion gestellt wissen möchten: In „Not- und Krisenzeiten", „bei Schleyer II", müsse den „Frontdienststellen" das Recht eingeräumt werden, auch die Informationen der Terrorismus-Datei Pios abzufragen.

Während gegenwärtig der Pios-Computer — in dem auch Verdächtige sowie Kontaktleute gespeichert sind — wegen der Empfindlichkeit seiner Daten nur von privilegierten Polizisten befragt werden darf, sollen nach den BKA-Plänen „temporär" auch die Beamten vor Ort, beispielsweise bei Verkehrskontrollen, feststellen können, ob jemand in Pios erfaßt ist, etwa als „Ausweisverlierer".

„Taten suchen ihren Täter."

Ein solches Verfahren böte aus BKA-Sicht den Vorteil, daß bei Razzien und Ringfahndungen nicht mehr alle Angetroffenen und Aufgehaltenen mit gleicher Schärfe kontrolliert werden müßten. Die Beamten könnten sich vielmehr auf jene konzentrieren, bei denen ihr Terminal nach Personalien-Eingabe „per Blinklicht signalisiert: Pios-Person, telephonisch nachfragen, was anliegt".

Denkbar freilich, daß das Blinklicht in unübersichtlichen Situationen ohnehin nervöse Beamte zu Kurzschlußhandlungen verführt: Als fatal könnte sich dann schon erweisen, wenn der vom Computer Verdächtigte ahnungslos ein wenig zu rasch in die Tasche greift — um seine Papiere zu ziehen.

Schon heute können mißverständliche Computer-Daten jemandem zum Verhängnis werden, der als Tatverdächtiger (ohne je verurteilt worden zu

* Anfang Mai bei Nürnberg.

Terroristen-Fahndung*: Verschärfte Kontrollen gegen „Ausweisverlierer"?

Wenn alles auf den Magen schlägt

Magenerkrankungen sind ein ernsthaftes Problem unserer Zeit. Immer mehr Männer und Frauen leiden unter dem ständigen Druck der Umwelt. Vielfältige Erkrankungen des Magens sind die Folgen.

Ärger, bedingt durch Hektik und Streß, Alkohol und Nikotin greifen den Magen an und überlasten ihn, genauso wie zu schwere und reichhaltige Speisen. Die Folgen sind: Magendruck, Magenverkrampfungen, Sodbrennen, saueres Aufstoßen, Völlegefühl.

SPASMO-NERVOGASTROL® beseitigt Ihre Magenschmerzen rasch und wirkungsvoll. Der Magen normalisiert sich.
Nehmen Sie SPASMO-NERVOGASTROL® deshalb rechtzeitig.

Spasmo-Nervogastrol®
Tabletten
rechtzeitig einnehmen – hilft rasch!

rezeptfrei in Ihrer Apotheke

Anwendungsgebiete: Krampf- und Säureschmerzen bei akuten und chronischen Magenschleimhaut- und Zwölffingerdarmentzündungen, Sodbrennen. Gegenanzeigen und Anwendungsbeschränkungen: Grüner Star, Vergrößerung der Vorsteherdrüse im fortgeschrittenen Stadium. In der Schwangerschaft nur auf ärztliche Verordnung einnehmen. Bei entsprechender Veranlagung kann das Reaktionsvermögen beeinträchtigt sein.
LUDWIG HEUMANN & CO. GMBH NÜRNBERG

HEUMANN Arzneimittel

sein) in die Inpol-Straftaten-/Straftäter-Datei (SSD) aufgenommen worden ist. Dieses System hat zwar in den letzten Jahren gleichsam automatisch eine Unmenge von Verdächtigungen ausgespuckt, aber, von spektakulären Einzelfällen abgesehen, insgesamt nicht erreicht, was seine Schöpfer sich versprochen hatten.

„Sag mir, wie du einbrichst, und ich sage dir, wo du eingebrochen hast" — nach diesem Leitgedanken sollte der SSD-Computer bekannte Täter mit den Taten Unbekannter zusammenführen. Als wichtigste Kombinationshilfe galt der elektronisch erfaßte „modus operandi", die kriminelle „Handschrift".

Doch das Projekt „Taten suchen ihren Täter" (Herold) ist weitgehend gescheitert. Denn die „Handschrift" eines Kriminellen wechselt häufiger, als die BKA-Theoretiker es vermutet hatten. Die Tatbeschreibungen der ermittelnden Beamten haben sich obendrein großenteils als unbrauchbar erwiesen. Eine kriminalwissenschaftliche Untersuchung, die in der „Forschungsreihe" des BKA veröffentlicht worden ist, beschreibt die Grenzen solcher EDV-Ermittlungen*:

> Das zentrale Ziel, das mit der Entwicklung und probeweisen Einführung der SSD verfolgt wurde, bestand darin ... maschinenunterstützte Vergleiche von Tathergangsbeschreibungen zu ermöglichen, und zwar so effektiv, daß aufgrund der Vergleichsergebnisse möglichst verläßlich zwei oder mehr einander ähnliche Taten dem oder denselben Täter(n) zugeschrieben werden können.
>
> Derartige Feststellungen von Tatzusammenhängen vor dem Hintergrund der erfahrungsgestützten Annahme, daß Täter in ihren Tatbegehungsformen, -orten, -zeiten oder -zielen zu Perseveranzen tendieren, sind jedoch ... nur dann möglich und gleichzeitig verläßlich, wenn auch die Tathergangsrekonstruktion und deren Beschreibungen ... hinreichend verläßlich und genau sind.
>
> Dies aber, so zeigten die ... Analysen, ist in zahlreichen Fällen nicht gegeben.

Während das BKA-Management derzeit die SSD-Eingabevorschriften vereinfachen läßt, ziehen Datenschützer aus dem Mängelbericht die Schlußfolgerung, das Amt solle zumindest das ehrgeizige Vorhaben aufgeben, *sämtliche* mutmaßlichen Täter und *sämtliche* Taten bis hin zum Kaufhausdiebstahl im Computer zu speichern.

Computer-Leitmotiv: „Wer einmal lügt ..."

Denn zu groß sei die Gefahr, daß aufgrund ungenauer Eingaben Unschuldige, die früher einmal gefehlt haben, vom Computer immer wieder aufs neue verdächtigt werden — nach dem erbarmungslosen „Leitmotiv der SSD-Fahndung: Wer einmal lügt, dem glaubt man nicht, und wenn er auch die Wahrheit spricht" (Westdeutscher Rundfunk).

Sind im Inpol-System Angaben über Verdächtige gespeichert, fehlen häufig klärende Hinweise über die Intensität und den Grund des Verdachts. „Wird der Verdächtige später rehabilitiert", fordert Steinmüller, „so muß dies — schon im polizeilichen Interesse an einer aktuellen und richtigen Information — zu einer Löschung der Verdachtsmomente, zumindest zu einem klarstellenden Hinweis führen."

Mit der Pflege ihrer Datenbestände jedoch tun sich viele Dienststellen schwer. Überraschendes widerfuhr dem Freiburger Regierungsvizepräsi-

Hessischer Datenschützer Simitis
„Mehr Terminals, mehr Mißbrauch"

denten Werner Ackenheil, als er unlängst aus Anlaß seines Amtsantritts örtliche Polizeieinrichtungen besichtigte. In Besuchslaune tippte er seinen Namen in die „Black Box" ein, wie EDV-Leute ihre Elektronik-Kästen nennen — und fand sich polizeilich registriert: Vor einiger Zeit hatte jemand eine Beleidigungsklage gegen ihn erhoben; das Verfahren war jedoch eingestellt worden.

Offiziell gilt für Polizei-Dateien, daß Unterlagen über Täter und Verdächtige immer dann gespeichert bleiben, „wenn eine Prognose Anhaltspunkte dafür hergibt, daß die betreffende Person mit einiger Wahrscheinlichkeit wiederum mit den Gesetzen in Konflikt kommen wird". Dabei sind die Beamten, so BKA-Kriminaldirektor Jürgen Heiger, bemüht, „den Beurteilungsrahmen für die Prognose nicht zu eng

* H. Walter Schmitz: „Tatortbesichtigung und Tathergang. Untersuchungen zum Erschließen, Beschreiben und Melden des modus operandi. Mit einer Analyse der Dokumentationssprache der Straftaten-/Straftäterdatei". BKA-Forschungsreihe, Band 6; Wiesbaden.

Die Zarges-Box

Die Kiste der unbegrenzten Möglichkeiten

Ob Sie Tore oder Ringe schießen, Match- oder Eckbälle schlagen, Hürden oder Latten überspringen, ob Sie mitmachen oder zuschauen, gewinnen oder verlieren – es gibt die Idealbox für jede Sportausrüstung. Für Freizeit, Camping, Caravaning.
Die Zarges-Box. Verschließbar und stabil. Aus korrosionsfestem, stoßfestem Leichtmetall. In drei Größen: Mini. Midi. Maxi. In guten Sportgeschäften und im Eisenwarenhandel.

Da können alle einpacken

Zarges macht das Leben leichter

Leichtmetall-Konstruktionen
Transportsysteme · Leitern

ZARGES

Ich möchte mehr über die Zarges-Box wissen.
Bitte schicken Sie mir ausführliches Informationsmaterial und Händlernachweis.

Name: _____

Anschrift: _____

An Zarges Leichtbau GmbH · 8120 Weilheim
Telefon: 0881/87-1

SP/B 279

anzusetzen, damit nicht von vornherein nicht mehr zu schließende Ermittlungs- und Fahndungslücken entstehen".

Nach einer Kripo-Richtlinie aus dem Jahr 1969 müssen beispielsweise Fingerspuren einer Person erst bei deren Tod oder bei Vollendung des 90. Lebensjahrs ausgesondert werden — Regelungen, die Innenminister Baum (aber auch BKA-Chef Herold) „nach unserem heutigen Rechtsverständnis nicht mehr tragbar" erscheinen.

Für eindeutig rechtswidrig hält Hessens Datenschützer Simitis den Umstand, daß Polizei-Computer die anfragenden Beamten auch dann noch über Straftaten unterrichten, wenn die Verurteilung gemäß Bundeszentralregistergesetz (BZRG) bereits getilgt ist*.

Vorstrafen, die laut Gesetz im Justizregister gelöscht werden müssen, soll, argumentiert der Rechtswissenschaftler, auch die Polizei nicht als Begründung dafür heranziehen dürfen, daß jemand „nicht unbescholten oder nicht zuverlässig sei oder zur Begehung strafbarer Handlungen neige".

Nur solange eine Verurteilung nicht rechtskräftig ist, meint Simitis, sei „gegen das Festhalten dieser Verurteilung in den Kriminalakten nichts einzuwenden". Mit Eintritt der Rechtskraft aber werde das Urteil zugleich ins Berliner Zentralregister eingetragen, das auch der Polizei zugänglich ist; von diesem Zeitpunkt an sei eine Speicherung in den Polizei-Computern nicht mehr erforderlich und daher unzulässig.

„Löschen ist für viele ein Tabu."

Weit zurück hinter solchen Forderungen bleiben die Innenminister von Bund und Ländern, die demnächst neue Datenschutz-Richtlinien erlassen wollen. Grundlage ist ein im März von ihnen beschlossener „Musterentwurf" über die Führung „Kriminalpolizeilicher personenbezogener Sammlungen".

Das Papier sieht vor, daß „Regelaussonderungen" künftig „zwei Jahre nach dem Tod des Betroffenen" vorgenommen werden, ansonsten nach Vollendung des 70. Lebensjahres oder wenn „nach Aktenlage" zehn Jahre lang keine neuen Erkenntnisse angefallen sind.

Bei genauem Hinsehen weist diese Vorschrift eine Reihe von Lücken und Kann-Klauseln auf. Wenn es die Polizeipraktiker nur wollen, wird trotz des neuen Papiers vieles beim alten bleiben können.

Entgegen der „Regelaussonderung" nämlich gestattet eine Spezialbestimmung, daß Daten noch über das straffreie Jahrzehnt hinaus

* Laut BZRG darf eine Verurteilung nach Ablauf bestimmter Fristen (fünf Jahre bei Freiheitsstrafe bis zu drei Monaten, zehn Jahre bei Freiheitsstrafe von mehr als drei Monaten bis zu einem Jahr auf Bewährung, sonst 15 Jahre) dem Betroffenen im Rechtsverkehr nicht mehr vorgehalten und nicht zu seinem Nachteil verwertet werden.

aufbewahrt werden dürfen, wenn sie etwa „von besonderem Interesse" sind.

Zudem weist das Papier eine elegante Möglichkeit, die Vernichtung beispielsweise von Datenbeständen über Terror-Sympathisanten zu umgehen: Zulässig ist eine Übermittlung der „auszusondernden Unterlagen" an „andere Stellen" mit einer „weiter gehenden Aufgabenstellung". In Frage kämen die Geheimdienste.

Mit den vorgesehenen Vorschriften, räumt BKA-Präsident Herold ein, „könnte jede exzessive Anwendung legitimiert werden".

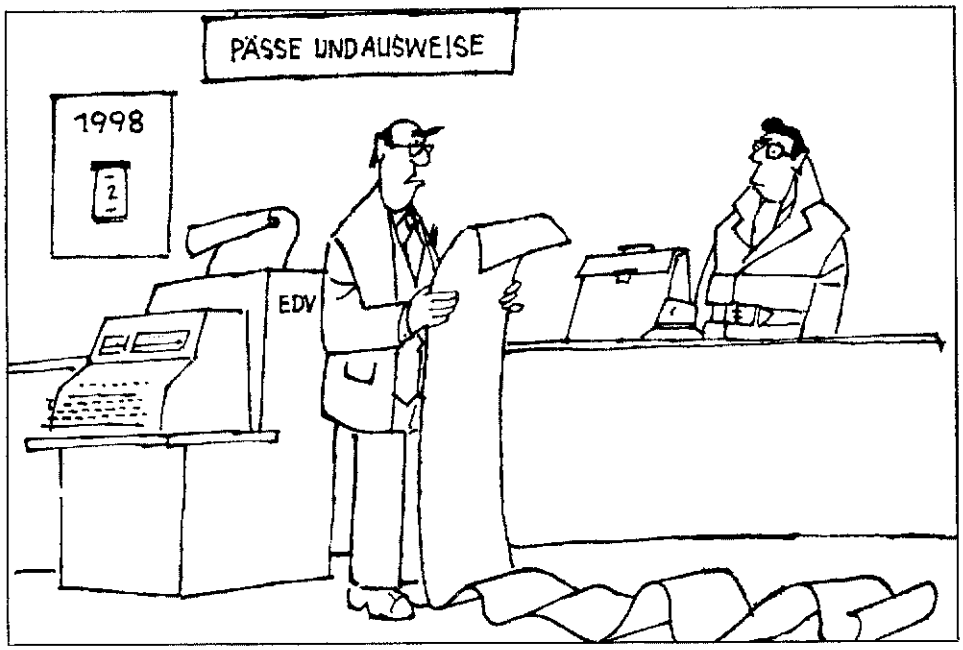
Während Herold versichert, er habe — ohne dazu gezwungen zu sein — bisher hin und wieder „alten Mist einfach weggeworfen", gilt es in den Geheimdiensten als geradezu unprofessionell,

Ob ein solches Lösch-Verfahren (dem auch die Länder zustimmen müßten) je funktionieren wird, steht dahin. „Das ist für uns eine Revolution", fürchtet ein liberaler BfV-Abteilungsleiter, „Löschen ist für viele ein Tabu."

Gegenwärtig jedenfalls würden im Kölner Bundesamt nicht einmal solche Daten aus der Welt geschafft werden können, die gesetzwidrig erfaßt worden sind und laut Gerichtsbeschluß gelöscht werden müßten.

Denn die komplizierten Sicherungsvorkehrungen, die Nadis vor Ostagenten schützen sollen, bewirken zugleich, daß unzulässig Gespeichertes zuverlässig vor Vernichtung bewahrt wird.

Verfassungsschutz-Präsident Meier läßt beanstandete Informationen zwar im Nadis-„Auskunftsbestand" löschen,



Kölnische Rundschau

„Stimmt es, daß Sie 1977 als Neunjähriger mit Ihren Eltern Urlaub in einem Ostblockstaat gemacht haben?"

eine einmal gewonnene Erkenntnis ohne Not zu vernichten. Ein BND-Mann: „Der Dienst vergißt nicht."

Zwar kann es sich, auch nach Auffassung Bulls, „im Bereich der Spionageabwehr als notwendig erweisen, Informationen über Jahrzehnte hinweg aufzubewahren". Daten über „Jugendsünden" hingegen könnten schon „nach relativ kurzer Zeit gelöscht werden".

Unter dem „Eindruck, um nicht zu sagen Druck" des Datenschutzgesetzes plant das BfV gegenwärtig ein „System der Zeitspeicherung" (Bull), das nach einer bestimmten Frist eine „Erforderlichkeitsprüfung für die weitere Aufbewahrung" in Gang setzen soll. „Wer 1956 als Jugendlicher kommunistische Flugblätter verteilt hat und seitdem nicht in Erscheinung getreten ist", beschreibt ein Verfassungsschützer das Vorhaben, „den könnte man wohl rausnehmen."

nicht aber in den Protokollbändern, die einen jeden Löschvorgang dokumentieren. Meiers Genehmigung vorausgesetzt, lassen sich diese Datenträger im „Ausnahmefall" jederzeit auswerten — wenngleich mit einem derzeit noch relativ langwierigen Verfahren.

Datenvernichtung auf solche Art, befürchtet EDV-Experte Steinmüller, bedeute in Wahrheit, „daß die Informationen auf den schnellen Speichern für den direkten Zugriff getilgt und statt dessen auf langsameren Speichern archiviert werden, bis in etwa fünf Jahren die rationelle Auswertung auch dieser Datenmassen gewährleistet wird".

Wer einmal in der Black Box ist, kommt so schnell nicht wieder raus.

Im nächsten Heft

Unternehmen Befa — Tausende unter elektronischer Beschattung — „Grenzüberwachung" für den Geheimdienst