

Stellungnahme der ARGE DATEN zu

Lauschangriff und Rasterfahndung

(Entwürfe der Bundesministerien für Justiz und Inneres)

Die ARGE DATEN ist schockiert darüber, daß die Absicht besteht, Lauschangriff und Rasterfahndung in der bevorstehenden Sondertagung des Nationalrats noch rasch durchzudrücken. Diese Absicht kann nur als zweifelhaftes Wahlkampfmanöver angesehen werden, bei dem der Bevölkerung das Gefühl vermittelt werden soll, daß etwas gegen die Kriminalität getan wird. Weder der Lauschangriff noch die Rasterfahndung sind dafür aber geeignete Mittel.

Der Lauschangriff kann überhaupt nur bei bestimmten Formen der organisierten Kriminalität (etwa Schutzgelderpressung) wirkungsvoll sein. Gegen die nicht organisierte Massenkriminalität und auch gegen die Briefbombenattentäter ist der Lauschangriff nicht geeignet. Pro verurteilter Person werden beim Lauschangriff bis zu 100 unbeteiligte Personen abgehört. Darüber hinaus verbreitet allein die Möglichkeit des Lauschangriffs Unsicherheit: Da zwangsläufig auch Unschuldige abgehört werden, kann jeder vom Lauschangriff betroffen sein.

Die Rasterfahndung ist zur Bekämpfung organisierter Kriminalität völlig ungeeignet. Bei politischen Delikten (z. B. den Briefbomben) kann sie nur zu Ergebnissen führen, wenn man massiv in die Privatsphäre zehntausender unbescholtener Bürger eingreift und systematisch Daten wie Vereinsmitgliedschaften, Zeitschriftenabonnements, Veranstaltungsteilnahmen etc. abgleicht. Das steht in keinem Verhältnis zum angestrebten Ergebnis. Die Möglichkeit des Mißbrauchs erhobener Daten kann nicht ausgeschlossen werden. Da der vorgeschlagene Entwurf keine brauchbaren Kontrollmechanismen vorschlägt, könnte jede Regierung das Instrument der Rasterfahndung (unter dem Vorwand der "Terrorismusbekämpfung") auch zur Bespitzelung politischer Gegner einsetzen.

Bei der diesbezüglichen Enquete wurde der Entwurf des Justizministeriums von der Mehrzahl der Experten als Diskussionsgrundlage, aber noch nicht als beschlußreif angesehen. Der Entwurf des Innenministeriums, der der Polizei praktisch schrankenlose Ermächtigungen gegeben hätte, stieß auf einhellige Ablehnung. Eine ausführliche Diskussion über den nun geänderten Entwurf wäre dringend nötig, ist aber bis zur Sondertagung nicht mehr möglich.

Forderungen der ARGE DATEN

Die ARGE DATEN fordert daher mit Nachdruck, daß auf Rasterfahndung und Lauschangriff verzichtet wird. Auf keinen Fall sollte das Gesetz nun noch rasch beschlossen werden. Sinnvollerweise wäre eine Neuregelung der polizeilichen und gerichtlichen Ermittlungsmethoden im Rahmen der schon seit geraumer Zeit diskutierten Reform des strafrechtlichen Vorverfahrens.

Auf die Rasterfahndung sollte völlig verzichtet werden. Stattdessen sollte über verbesserte Möglichkeiten beim EDV-Einsatz in der Polizei diskutiert werden. Viele Formen der EDV sind datenschutzrechtlich völlig unproblematisch und wesentlich nützlicher als die problematische Rasterfahndung (siehe Kapitel 3.2.).

Statt der Einführung des Lauschangriffs sollten zunächst andere Maßnahmen in Angriff genommen werden, die nicht in die Grundrechte eingreifen. So sind z. B. die Möglichkeit des Zeugenschutzes noch völlig unzureichend geregelt. Bei den Hauptfeldern der organisierten Kriminalität (Drogen, Eigentumskriminalität, Schlepperunwesen) sind nicht-polizeiliche Methoden in den Vordergrund der Kriminalitätsbekämpfung zu stellen: Liberalisierung von Bagatelldelikten im Drogenbereich, Alarmanlagen oder Wegfahrsperrren gegen Einbruchs- oder Autodiebstähle, Abschaffung jener Willkürmaßnahmen, die Ausländer dazu verleitet, sich Schleppern anzuvertrauen.

Bei der Telefonüberwachung und dem schon derzeit zulässigen "kleinen" Lauschangriff (Abhören in Anwesenheit eines verdeckten Ermittlers) gibt es noch große Probleme. Es gibt z. B. keine Untersuchungen darüber, wieviele unschuldige Personen abgehört werden bzw. inwieweit die Überwachungsmaßnahmen tatsächlich zu Verurteilungen führen. Daher sollte zuerst eine akzeptable Regelung für die Telefonüberwachung und den kleinen Lauschangriff gefunden werden, bevor der große Lauschangriff eingeführt wird.

Alternativmaßnahmen

Anstatt fragwürdige und in die Grundrechte massiv eingreifende Methoden zur Bekämpfung der Kriminalität einzuführen, sollte man sich auf Maßnahmen konzentrieren, die weniger problematisch sind.

- Die **Ausrüstung der Polizei** für herkömmliche Ermittlungsarbeit sollte verbessert werden. Anstatt teure

Computer und Software für die Rasterfahndung einzukaufen sollten lieber Computer für die Alltagsarbeit der Polizei (etwa das Verfassen und geordnete Ablegen von Protokollen, Anzeigen etc.) angeschafft werden. Im Bereich der Bundespolizeidirektionen wird z. B. teilweise noch nicht einmal das Meldewesen automationsunterstützt geführt.

- Nach deutschem Vorbild könnte ein **Bundeskriminalamt** mit Experten der verschiedensten Disziplinen eingerichtet werden. Gerade die Briefbombenermittlungen haben gezeigt, daß die Polizei zu wenige bzw. in vielen Fachbereichen gar keine Wissenschaftler (Chemiker, Sprengstoffexperten, Historiker, Psychologen) beschäftigt.
- Die in Österreich vorgesehenen Maßnahmen zum **Zeugenschutz** sind verbesserungswürdig. So ist es zwar möglich, Zeugen über Video so einzuvernehmen, daß ihre Identität nicht erkennbar ist. Die Identitätsdaten sind aber nicht von der Akteneinsicht ausgenommen, sodaß der Beschuldigte oder sein Anwalt dennoch leicht den Namen des Zeugen herausfinden können. - In den USA wird bei Schutzgelderpressung jener Person, die als erste zur Polizei geht und Anzeige erstattet, von vornherein zugesichert, daß sie nicht im Akt aufscheint und nie als Zeuge einvernommen werden wird.
- Viele Verbrechen lassen sich über **technische Maßnahmen** leichter bekämpfen als mit polizeilichen Methoden. So konnte die Einführung von Wegfahrsperren die KFZ-Diebstähle wirksamer bekämpfen als der Versuch strikter Grenzkontrollen.
- Die hauptsächlichen Tätigkeitsbereiche der organisierten Kriminalität sind **Drogenkriminalität, Prostitution** und das **Schlepperunwesen**. Gegen den Drogenmißbrauch haben sich Aufklärung, die Straflosigkeit für leichte Drogen oder Bagatelldelikte und die kontrollierte Abgabe von Ersatzdrogen als effizienter erwiesen als der rigorose Einsatz polizeilicher Mittel. Daher wird auch von Seiten der Polizei immer öfter eine Abkehr von der derzeitigen Drogenpolitik gefordert. Auch bei der (schon weitgehend liberalisierten) Prostitution könnte eine Verstärkung der Rechtsstellung von Prostituierten eine Abnahme der Kriminalität bewirken. Das Schlepperunwesen beruht hauptsächlich darauf, daß die österreichischen Ausländergesetze und ihr Vollzug oft willkürlich sind und sich manche Ausländer eher Schleppern anvertrauen als einem Behördenverfahren mit fragwürdigem Ausgang.

In den meisten Bereichen der organisierten Kriminalität stehen daher bessere Bekämpfungsmethoden als der Lauschangriff zur Verfügung.

1. Lauschangriff

1.1. Schon vorhandene Probleme

Die Problematik der vorgeschlagenen neuen Ermittlungsmethoden zeigt sich vor allem auch dann, wenn man die Probleme der schon derzeit verwendeten Methoden betrachtet:

Telefonüberwachung: Fast alle beantragten Telefonüberwachungen werden auch genehmigt. Teilweise erfahren die Untersuchungsrichter nur mündlich von der "Notwendigkeit" der Telefonüberwachung ("Gefahr im Verzug") und erteilen die Genehmigung telefonisch. Die Richter, die die Genehmigung erteilt haben, erfahren nie, ob die Überwachung ein brauchbares Ergebnis gebracht hat. Es gibt auch keine Untersuchungen darüber, inwieweit Telefonüberwachungen zu Verurteilungen führen bzw. wieviel Unschuldige abgehört werden.

Kleiner Lauschangriff: Seit 1993 gibt es im Sicherheitspolizeigesetz die Ermächtigung, Bild- und Tonaufzeichnungsgeräte verdeckt einzusetzen. Dabei muß ein Beamter anwesend sein (das unterscheidet den "kleinen" vom "großen" Lauschangriff). Die gesetzliche Regelung umfaßt nicht mehr als drei Sätze (§ 54 Abs. 3 und 4 SPG). Eine begleitende Forschung oder eine Kosten-Nutzen-Analyse gibt es nicht. Ebenso wenig eine richterliche Kontrolle. Die Regelung wird auch von Polizeijuristen als völlig unzureichend angesehen.

1.2. Probleme des Lauschangriffs

Der "große" Lauschangriff hat im Gegensatz zum "kleinen" vor allem das Problem, daß regelmäßig eine große Zahl von völlig unschuldigen Personen abgehört wird - eine deutsche Untersuchung spricht von **77 abgehörten Personen pro Verurteilung**. Auch hier ist zu bedenken, daß zum Zeitpunkt des Lauschangriffs alle abgehörten Personen, auch der Verdächtige selbst, als unschuldig anzusehen sind. Tatsächlich endet etwa die Hälfte der Lauschangriffe ohne Verurteilung.

Das Recht auf Achtung des Privatlebens (Art. 8 MRK) und das Grundrecht auf Datenschutz (§ 1 DSG) - beide stehen im Verfassungsrang - erlauben Eingriffe nur, wenn sie verhältnismäßig sind. Zur **Verhältnismäßigkeit** eines Eingriffs gehört jedenfalls einmal, daß er geeignet ist, ein bestimmtes Ziel (hier insbesondere die Verhinderung und Aufklärung strafbarer Handlungen) zu erfüllen. Angesichts der Erfahrungen in anderen Staaten (in den USA spielt der Lauschangriff bei den Ermittlungen gegen die organisierte Kriminalität nur eine untergeordnete Rolle) ist die Eignung des Lauschangriffs zur Verbrechensbekämpfung fragwürdig.

Der Grundsatz der Verhältnismäßigkeit erfordert aber über die Eignung der Maßnahme hinaus, daß sie auch notwendig ist. Da die organisierte Kriminalität in Österreich zum Glück wesentlich schwächer auftritt als in den meisten anderen Staaten (und insbesondere in Italien und den USA) ist auch die **Notwendigkeit** des Lauschangriffs höchst fraglich.

Mit der Einführung von verdeckten Methoden geht der Staat vom Prinzip des fairen, offenen und täuschungsfreien Strafverfahrens ab. Auch das Prinzip des Selbstbeschuldigungsverbots wird unterlaufen.

Die ARGE DATEN lehnt aus allen diesen Gründen den großen Lauschangriff klar ab. Auch der kleine Lauschangriff ist problematisch und sollte stärkeren Schranken unterworfen werden als bisher.

1.3. Schutzmaßnahmen

Wird der Lauschangriff aber eingeführt, dann sollten auf jeden Fall massive Schutzmaßnahmen vorgesehen werden, die einen Mißbrauch dieses Instruments oder den fahrlässigen Eingriff in Grundrechte wenigstens in vertretbaren Grenzen halten.

- Der Lauschangriff soll nur zulässig sein, wenn er zur **Aufklärung** einer schweren Straftat unbedingt notwendig ist. "**Vorbeugende**" Lauschangriffe sind nicht akzeptabel. Daher muß der Gesetzesentwurf des Innenministeriums von vornherein abgelehnt werden.
- Der Verhältnismäßigkeitsgrundsatz gebietet, daß der Eingriff in das Grundrecht zur Aufklärung der Straftat **unentbehrlich** sein muß. Der Lauschangriff darf in jedem einzelnen Fall nur das letzte Mittel sein. Die vom Justizministerium gewählten Formulierungen "erforderlich erscheint" bzw. "aussichtslos oder wesentlich erschwert" (§ 149d) sind daher zu weit und verfassungswidrig.

- Die Straftaten, zu deren Aufklärung der Lauschangriff eingesetzt werden darf, müssen im Gesetz aufgezählt sein. Es darf sich **nur** um **schwerste Straftaten** handeln. Dem Vorschlag des Justizministeriums (Strafdrohung über zehn Jahre) kann hier zugestimmt werden. Völlig inakzeptabel ist das Konzept des Innenministeriums, das gravierende Grundrechtseingriffe gegen die "organisierte Kriminalität" (OK) vorsieht und unter OK alles verstehen will, was von "mehr als drei Menschen" begangen wird.
- Der Lauschangriff darf sich **nur gegen dringend verdächtige Personen** richten. Er darf nicht von vornherein gegen Personen gerichtet sein, die mit dem Verdächtigen voraussichtlich in Kontakt treten werden, wie im BMJ-Entwurf vorgesehen ist (§ 149d (1) Z. 2 lit. b).
- Personen, die nicht als Zeugen einvernommen werden dürfen oder sich entschlagen können, sollen nicht abgehört werden dürfen. Werden sie unbeabsichtigt dennoch abgehört, so muß es für die mit ihnen geführten Gespräche ein **Beweisverwertungsverbot** geben. Das darf nicht nur für Rechtsanwälte, sondern muß insbesondere auch für Angehörige gelten.
- Außerdem soll der Lauschangriff **nur außerhalb von Wohnungen** durchgeführt werden dürfen (siehe Kapitel 1.4.). Auch in Italien darf der Lauschangriff nur in Räumlichkeiten durchgeführt werden, bei denen der dringende Verdacht besteht, daß dort die verbrecherische Tätigkeit ausgeübt wird - nicht dort, wo man erwarten kann, daß der Mafiaboß mit seiner Ehefrau über den "Beruf" spricht.
- Eine **begleitende Forschung** soll die Zweckmäßigkeit des Lauschangriffs feststellen. Das Gesetz soll befristet beschlossen werden, dann soll das Parlament prüfen können, ob die durchgeführten Lauschangriffe etwas gebracht haben, was die Schwere der Grundrechtseingriffe überwiegt. Daher ist die **Berichtspflicht nach amerikanischem Vorbild** (siehe auch Kapitel 1.5.) eine unbedingt notwendige Begleitmaßnahme zur jedem Grundrechtseingriff. In diesem Zusammenhang ist auch das im Strafprozeßrecht sonst so hochgehaltene Öffentlichkeitsprinzip zu denken, das leider nur bei Verhandlungen beachtet wird. Auch im Vorverfahren und gerade bei Grundrechtseingriffen besteht ein Bedarf nach öffentlicher Kontrolle. Diese wird am besten durch die Berichtspflicht und die wissenschaftliche Analyse und parlamentarische Beratung der Berichte gewährleistet.

- Bei unzulässigen Überwachungen sollen die Betroffenen das Recht auf **immateriellen Schadenersatz** haben. Daß es in Österreich (außer beim Schmerzensgeld) kein Recht auf immateriellen Schadenersatz gibt, zeigt sich im gesamten Datenschutzbereich immer wieder als Problem. Viele Bürger, die sich an die Arge Daten wenden, können mit Recht nicht verstehen, warum nach einer Datenschutzverletzung als einzige Konsequenz ein Bescheid der DSK erlassen wird.

1.4. Recht auf Wohnung

Für die freie Entfaltung des Menschen ist es notwendig, daß ihm ein Raum verbleibt, in den er sich unbeobachtet zurückziehen sehen und wo er in Ruhe gelassen wird - ein Raum, wo der Mensch "sich selbst besitzt". Das leitet das deutsche Bundesverfassungsgericht aus dem Recht auf Würde des Menschen und aus dem Recht auf Wohnung ab. In Deutschland ist staatliches Abhören daher prinzipiell nur außerhalb von Wohnungen zulässig.

Oberste Aufgabe des liberalen Rechtsstaats ist es, seinen Bürgern Freiheitsrechte zu gewähren. Auch die Verbrechensbekämpfung ist nicht Selbstzweck, sondern dient dazu, die Freiheiten der einen gegen die Übergriffe anderer zu schützen.

Das Grundrecht auf Wohnung, wie es in Österreich im Hausrechtsgesetz, in Art. 8 MRK und in gewissem Sinn auch in § 1 DSG verankert ist, verlangt auch, daß jeder Mensch die Sicherheit hat, daß seine Wohnung vom Staat unangetastet bleibt. Sobald auch nur in wenigen Fällen pro Jahr unschuldige Personen in ihrer Wohnung überwacht werden, bewirkt dies ein berechtigtes Unbehagen bei vielen anderen, die ebenfalls Opfer einer solchen Überwachung werden könnten.

Auch die Schwarzseherkontrollen der Post bewirken ein solches Unbehagen. Viele Menschen (die z. B. gar keinen Fernseher besitzen) wollen zu Recht nicht, daß ein Kontrollor ihre Wohnung betritt und durchsucht. Diese Kontrollen sind für die Betroffenen aber wenigstens als solche erkennbar. Die Möglichkeit unangekündigter und unsichtbarer Überwachung ist im Vergleich zu den Schwarzseherkontrollen um vieles bedrohlicher und würde das Grundrecht auf Achtung der Wohnung auch bei jenen Menschen einschränken, die gar nicht überwacht werden.

Wenn der große Lauschangriff eingeführt wird, dann sollte ihm daher auf jeden Fall ein **Grenze** durch das **Grundrecht auf Wohnung** gesetzt werden. Dabei sollte ein materieller

Wohnungsbegriff verwendet werden, der nicht darauf abstellt, wie die Räumlichkeiten aussehen, sondern darauf, wie sie (zum Zeitpunkt der Überwachung) genutzt werden.

Als Wohnung soll jener Bereich definiert sein, wo jemand übernachtet, wo er mit seinem Ehepartner, seinem Lebensgefährten oder seiner Familie zusammenlebt oder sich mit Freunden zu geselligem Beisammensein trifft. Wohnung in diesem Sinn soll auch das Hotelzimmer sein, das jemand mit seiner Familie im Urlaub bezieht, - ebenso jeder andere Raum, in dem die betroffene Person das Gefühl haben muß, sich mit engen Angehörigen ungestört unterhalten zu können. Dieser Bereich soll unter gar keinen Umständen abgehört werden dürfen. Im Zweifel muß mit dem Lauschangriff zugewartet werden und mit anderen Ermittlungsmethoden überprüft werden, ob es sich um eine Wohnung handelt.

Nicht als Wohnung im Sinn der vorgeschlagenen Definition anzusehen wären etwa Büros oder Fahrzeuge, die geschäftlich genutzt werden. Keine Wohnung wären auch Räume, die zwar normalerweise bewohnt werden, aber nach Angabe von Informanten an einem bestimmten Tag für ein Treffen von Mafiabossen angemietet wurden.

Bei der Auslegung des Wohnungsbegriffes soll jedenfalls darauf geachtet werden, daß das Vertrauen der Bevölkerung in die Polizei ein wertvolles Gut ist, das nur allzu leicht verspielt werden kann. (Man denke nur an den Freispruch im Prozeß gegen O. J. Simpson, der zu einem guten Teil auf dem Mißtrauen der Geschworenen gegenüber der Polizei beruhte.) Daher sollte auch außerhalb von Wohnungen bei Gesprächen, die erkennbar privaten oder persönlichen Inhalt haben, der Lauschangriff prinzipiell sofort abgebrochen werden.

Alle Bürger müssen die Gewißheit haben, daß der Staat zwar Verbrechen bekämpfen, aber unter keinen Umständen in ihr Privatleben eindringen will.

1.5. Verfahren

- Telefonüberwachung, kleiner und (falls er tatsächlich eingeführt wird) großer Lauschangriff sollten jeweils **nur zur Aufklärung** von Straftaten eingesetzt werden dürfen und daher nach dem selben Regelungsmodell in der Strafprozeßordnung (und nicht im Sicherheitspolizeigesetz) verankert werden. **Keinesfalls** soll (wie nach den Vorstellungen des Innenministeriums) ein Lauschangriff "**zur Vorbeugung**" oder "zur Abwehr von Gefahren" eingesetzt werden dürfen. Das gilt auch für den kleinen Lauschangriff, dessen derzeitige Regelung viel zu weit

geht. Das Mitschneiden von Gesprächen ist ein gravierender Eingriff in die Privatsphäre des Betroffenen und daher nur gerechtfertigt, wenn gegen den Betroffenen der dringende Verdacht vorliegt, daß er eine Straftat begangen hat - nicht die bloße Vermutung, daß er eine Straftat begehen könnte.

- Für die Entscheidung sollen in allen Fällen **Richter** und nicht die Polizei zuständig sein. Dabei soll ein Richterergremium eingesetzt werden, das derartige Entscheidungen häufiger trifft und daher erfahrener ist. Es wäre daher sinnvoll, statt den Ratskammern (16 in Österreich) die vier Oberlandesgerichte damit zu betrauen. Nur beim kleinen Lauschangriff sollte bei Gefahr in Verzug die Entscheidung bei den Untersuchungsrichtern liegen können.
- Die Betroffenen sollen (wie in Dänemark) durch einen von Amts wegen bestellten **Anwalt** vertreten sein, der ihre Interessen vertritt und Rechtsmittel einlegen kann. Sobald die Überwachung nicht mehr notwendig ist, sollen alle Betroffenen (vor allem die unschuldig Mitabgehörten), soweit sie bekannt sind, verständigt werden. Sie sollen dann selbst ein **Rechtsmittel** einlegen können. (Sinnvoll wäre als Beschwerdeinstanz der OGH - vgl. die Grundrechtsbeschwerde.)
- Alle Abhörmaßnahmen dürfen nur **zeitlich begrenzt** genehmigt werden. (Das ist in den USA und in Italien selbstverständlich, bei uns gibt es weder bei der Telefonüberwachung noch beim kleinen Lauschangriff und auch nicht im Entwurf zum großen Lauschangriff eine gesetzliche Höchstgrenze). Die Frist soll nur verlängert werden dürfen, wenn sich die abgehörte Person als "sprudelnde Quelle" erweist - nicht wegen Erfolglosigkeit.
- Die abgehörten Gespräche sollen vom Untersuchungsrichter sofort in "belastende" und "nicht belastende" eingeteilt werden. Nur die belastenden dürfen in Schriftform übertragen und zum Akt genommen werden. Die anderen sind nach Abschluß des Verfahrens (und evtl. geprüfter Beschwerden von Betroffenen) zu vernichten.
- Der Untersuchungsrichter (bzw. der Staatsanwalt) soll nach Abschluß der Ermittlung einen **detaillierten Bericht nach amerikanischem Vorbild** legen. Dieser Bericht soll den Richtern vorgelegt werden, die die Entscheidung gefällt haben, und in anonymisierter Form für die wissenschaftliche Forschung bzw. parlamentarische Behandlung veröffentlicht werden.

Im Bericht soll klargestellt werden: Wer hat die Entscheidung gefällt? Welcher Verdacht lag vor? Wie lange hat die Überwachung gedauert? Wieviele Gespräche wurden abgehört? Wieviele davon wurden als belastend eingestuft? Wieviele Personen wurden abgehört? Wieviele wurden als Unbeteiligte eingestuft? Gegen wieviele Personen wurden Vorerhebungen oder Voruntersuchungen eingeleitet, wieviele wurden in U-Haft genommen, wieviele wurden verurteilt?

Die im Entwurf des Justizministeriums vorgesehene Berichtspflicht entspricht diesen Anforderungen bei weitem nicht. Beim kleinen Lauschangriff und der Telefonüberwachung fehlt sie völlig.

- Für die bei einem Lauschangriff bzw. einer Telefonüberwachung gemachten **Zufallsfunde** muß ein strenges **Verwertungsverbot** gelten. Die Polizei darf nicht dazu verleitet sein, die richterliche Genehmigung eines grundrechtlich problematischen Eingriffs möglichst weit "auszunützen". Daher soll für die Verwertung von Zufallsfunden dieselbe Grenze gelten wie für den Lauschangriff bzw. die Telefonüberwachung selbst. Eine Ausnahme kann für Delikte vorgesehen werden, die in engem Zusammenhang mit jenem Delikt stehen, für das die Überwachung genehmigt wurde.

1.6. Sonderfall Geiselnahme

Eine besondere Anwendungssituation des Lauschangriffs besteht bei der Geiselnahme. Es sollte zulässig sein, daß die Polizei etwa ein vom Geiselnahmer gefordertes Fluchtfahrzeug verwanzt. Dabei ist es aufgrund der klaren Interessenslage auch nicht nötig, einen Richter in die Entscheidung einzubinden.

Dabei soll das Gesetz aber nicht eine allgemeine Formulierung enthalten, wie im Entwurf des BMJ, sondern klar die Situation der Geiselnahme ansprechen. (Außerdem sollte diese eine Regelung im SPG und nicht in der StPO verankert werden.)

Außerdem darf nicht vergessen werden, daß es sich bei der Überwachung immer noch in einen Eingriff der Persönlichkeitsrechte der Überwachten handelt. Den Betroffenen muß daher eine Beschwerdemöglichkeit (etwa an den UVS oder die DSK) eingeräumt werden. Die Beschwerde muß dabei gegen alle Umstände der Überwachung gerichtet werden können. So soll die Geisel sich zum Beispiel beschweren können, wenn die Polizei die Überwachung so durchführt, daß

auch Journalisten der Boulevardpresse die - für die Geisel vielleicht peinlichen - Gespräche mithören können.

2. Observation

Alles zum Lauschangriff gesagte gilt auch für die Observation, die derzeit überhaupt nicht gesetzlich geregelt ist.

Die längerfristige Observation im Sinne eines "Überwachens rund um die Uhr" ist ein schwerwiegender Eingriff in das Grundrecht auf Achtung des Privatlebens und die persönliche Bewegungsfreiheit und daher ebenso fragwürdig wie der große Lauschangriff.

Wenn tatsächlich ein Bedarf nach längerfristiger Observation besteht, dann soll sie an dieselben Voraussetzungen wie der große Lauschangriff gebunden sein und zur Aufklärung eines dringenden Verdachts, niemals aber vorbeugend zulässig sein.

Die einfache, kurzfristige Observation einer Person durch die Polizei ist naturgemäß weniger problematisch, bedarf aber ebenfalls einer gesetzlichen Regelung. Es ist nicht richtig, daß es sich dabei um keinen Grundrechtseingriff handelt. Natürlich ist auch hier das Grundrecht auf Achtung des Privatlebens berührt.

In diesem Zusammenhang zeigt sich das Problem, daß nach dem österreichischen Verfassungsrecht kein Rechtsschutz gegen "einfaches Verwaltungshandeln" besteht. Es besteht bloß Rechtsschutz gegen Befehls- und Zwangsakte. Da "bloßes Fotografieren", "bloßes Beobachten", "bloßes Befragen von Nachbarn" weder Befehle sind noch dabei Zwang auf den Betroffenen ausgeübt wird, besteht hier kein Rechtsschutz. § 88 Abs. 2 SPG schafft nur notdürftig Abhilfe, da diese Bestimmung einerseits verfassungsrechtlich abgesichert werden müßte und andererseits auf die Sicherheitsverwaltung beschränkt ist. Die Tätigkeit der Polizei im Bereich der Strafjustiz und alle der Gerichtsbarkeit zuzurechnenden Akte sind von diesem Rechtsschutz nicht erfaßt.

3. Rasterfahndung

Die Rasterfahndung greift in noch viel stärkerem Maß als der Lauschangriff in Grundrechte ein. Bei einem Lauschangriff ist pro Verurteilung mit bis zu 100 unschuldig abgehörten Personen zu rechnen. Bei der Rasterfahndung können Zehntausende oder Hunderttausende betroffen sein.

3.1. Rasterfahndung bringt nichts

In Europa ist ein einziger Fall erfolgreicher Rasterfahndung überliefert. Damals ging die deutsche Polizei davon aus, daß RAF-Terroristen in konspirativen Wohnungen leben, sich nicht polizeilich anmelden und keine Bankkonten führen - daher ihren Strom bar bezahlen. Deshalb wurden die Daten der barzahlenden Stromkunden mit der Meldevidenz verglichen und unter den so verdächtigten Personen tatsächlich RAF-Terroristen gefunden. Der Erfolg basierte hauptsächlich darauf, daß man wußte, wonach man suchen muß.

Seit damals werden in Deutschland keine Rasterfahndungen mehr durchgeführt. Gesetzliche Regelungen gibt es überhaupt nur in Deutschland, Dänemark, Frankreich und den Niederlanden.

Das Wesen der Rasterfahndung besteht darin, nicht konkret verdächtige Personen zu suchen, sondern aus irgendwie "auffälligen" Daten überhaupt erst einen Verdacht zu konstruieren. Bei der Rasterfahndung greift die Polizei auf externe Daten zu. Im wesentlichen ist die Methode der Rasterfahndung angewandte Wahrscheinlichkeitsrechnung. Man verknüpft Datenbestände, um eine Liste von Personen zu erzeugen, in der der Täter mit erhöhter Wahrscheinlichkeit enthalten ist. Dabei ist einerseits klar, daß fast alle oder alle der durch Rasterfahndung ermittelten Personen unschuldig sind. Andererseits ist der Erfolg der Rasterfahndung davon abhängig, ob man klare Kriterien hat, mit deren Hilfe man die Täter eingrenzen kann.

Eine in größerem Stil durchgeführte Rasterfahndung würde im Ergebnis zu einer demokratiefeindlichen, biedermeierähnlichen Stimmung führen. Die Bürger hätten Angst, aufzufallen und damit ins Zielfeld von Rasterfahndungsmaßnahmen zu gelangen.

Zur Bekämpfung von organisierter Kriminalität ist die Rasterfahndung ohnehin völlig ungeeignet, da es keine Datenbestände gibt, die z. B. überdurchschnittlich viele Drogenschmuggler oder Autoknacker enthalten.

Zu einem Ergebnis kann Rasterfahndung nur bei politisch motivierter Kriminalität führen - in Österreich kommen dabei nur die Briefbombenattentate in Frage. Für eine auch nur ansatzweise erfolgversprechende Rasterfahndung müßten allerdings in großem Umfang Gesinnungsdaten gesammelt werden: Wer ist Mitglied welcher Vereine? Wer abonniert welche rechtsgerichteten Zeitschriften? Wer besucht welche einschlägigen Veranstaltungen? Wer trifft sich mit wem zum Gedankenaustausch? Das wäre ein unerträglicher Eingriff in

die Privatsphäre und in die Rechte auf Versammlungsfreiheit, Vereinsfreiheit und Meinungsäußerungsfreiheit.

Die fragwürdige Hoffnung, durch derart massive Eingriffe in Grundrechte die Briefbombenattentate aufklären zu können, rechtfertigt die Eingriffe keineswegs. Vielmehr muß eine rechtsstaatliche Demokratie die Grundrechte über alles andere achten. Soweit in Zeitschriften, Vereinen oder Veranstaltungen nationalsozialistische Wiederbetätigung, Verhetzung oder dergleichen begangen wird, sind diese zu verbieten und strafrechtlich zu verfolgen. Wenn ein Verein oder eine Zeitschrift aber legal sind, dann darf niemand durch die Angst vor staatlicher Beobachtung davon abgehalten werden, dem Verein beizutreten oder die Zeitschrift zu abonnieren.

3.2. EDV-Einsatz bei der Polizei

Im persönlichen Gespräch mit Verantwortlichen des Innenministeriums zeigt sich: Im wesentlichen geht es der Polizei gar nicht darum, die Ermächtigung zur Rasterfahndung zu bekommen, sondern einfach darum, verstärkt EDV einsetzen zu können. Die Möglichkeiten des Sicherheitspolizeigesetzes, das Datenverknüpfungen pauschal verbietet (§ 53 Abs. 2), werden von der Polizei als zu gering angesehen.

Die ARGE DATEN ist der Ansicht, daß es sinnvoll ist, über eine Änderung zu diskutieren und die Befugnisse der Polizei in gewisser Weise auch auszuweiten. Eine solche Diskussion erfordert aber Zeit und die Einbeziehung möglichst vieler Diskussionspartner - insbesondere auch der Datenschutzexperten des Bundeskanzleramts, des Datenschutzrates, der Plattform Grundrechte und der Arge Daten. Die Vorschläge des Innenministeriums, praktisch unbeschränkt auf Daten aus "allen verfügbaren Quellen" zugreifen zu dürfen, schießen weit über jedes vertretbare Ziel hinaus.

Die Diskussion ist leider weitgehend dadurch geprägt, daß zwischen verschiedenen Methoden der Datenverarbeitung nicht unterschieden wird. Wir versuchen im folgenden, zwischen unproblematischen und problematischen Formen des EDV-Einsatzes zu unterscheiden:

- **Überhaupt kein Datenschutzproblem** sehen wir dort, wo es einfach darum geht, der Polizei die Möglichkeiten moderner **Büroautomatisation** zu bieten: Textverarbeitung, Datenbanken zur Unterstützung der Aktenablage oder zur Information, wo sich welches Beweismittel befindet, usw. Diese Form von EDV-Einsatz muß zwar (wie jedes

Behördenhandeln im Rechtsstaat) gesetzlich geregelt werden, ist aber unproblematisch. Bei der Wahl der entsprechenden Programme soll den ermittelnden Beamten möglichst große Freiheit gegeben werden. Eine Ausnahme von der Registrierung jeder einzelnen Datenverarbeitung beim DVR wäre daher sinnvoll. Es ist aber notwendig, diese Freiheit auf die Büroautomatisation zu beschränken, damit sie nicht mißbraucht werden kann, um gesetzliche Schranken bei problematischeren Formen des EDV-Einsatzes zu umgehen. Außerdem sollten es polizeiinterne Datenschutz- und Datensicherheitsbeauftragte geben.

- Ebenfalls sinnvoll ist das **Durchrastern polizeiinterner Datenbestände**, um z. B. Serientäter zu finden. So kann ein Abgleich aller Einbruchsdiebstähle mit geeigneten Programmen etwa ergeben, welche dieser Diebstähle von denselben Tätern begangen worden sein könnten. Die ermittelnden Beamten können dann ihre Informationen austauschen. Im Unterschied zur Rasterfahndung geht es hier um interne Datenbestände. Der Datenabgleich wird dabei weitestgehend nicht personenbezogen durchgeführt, sondern bezieht sich auf den Abgleich von näheren Umständen des Tatorts, des Deliktstyps, der Tatwerkzeuge und Tatbegehung. Soweit das Durchrastern **nicht personenbezogen** erfolgt, ist es datenschutzrechtlich unproblematisch.

Ein Datenschutzproblem ergibt sich dann, wenn etwa (wie vom deutschen Bundeskriminalamt praktiziert) die Geburtsorte von Tätern abgeglichen werden (unter der Annahme, daß sich der Dieb aus Palermo und der Räuber aus Palermo wohl kennen werden). Solche Formen des Datenabgleichs erfordern aus der Sicht des Datenschutzes eine besondere Rechtfertigung. Vor allem dürfen sie nur durchgeführt werden, wenn sie erfolgversprechend sind. Bevor dafür eine gesetzliche Grundlage geschaffen wird, sollte eine detailliertere Diskussion geführt werden. In Deutschland werden derartige Formen des Datenabgleichs unter der Aufsicht der Datenschutzbeauftragten durchgeführt.

- Der Zugriff der Polizei auf **externe Datenbestände** oder auf Datenbestände, die nicht zum Bereich der Kriminalpolizei gehören, ist datenschutzrechtlich prinzipiell problematisch. Auch scheinbar harmlose Zugriffsberechtigungen (etwa auf die Kraftfahrzeugevidenz) können (z. B. für private Zwecke) mißbraucht werden.

Bei manchen Dateien (Melderegister, Kraftfahrzeugevidenz, Paßvidenz, waffenrechtliche Evidenzen etc.) kann es

jedoch durchaus sinnvoll sein, der Polizei Zugriffsmöglichkeiten zu eröffnen. Dabei sollte keine abstrakte gesetzliche Ermächtigung formuliert werden, sondern bei jeder einzelnen Datei eine angemessene Regelung gefunden werden:

- Der Zugriff im Einzelfall ist der Eröffnung genereller Abfragemöglichkeiten vorzuziehen.
 - Der Zugriff durch eine beschränkte Anzahl von Personen ist weniger problematisch als der Zugriff durch jeden beliebigen Beamten.
 - Die Protokollierung der Zugriffe kann Mißbräuchen entgegenwirken. Ebenso die Bestellung von Datenschutzbeauftragten oder die Durchführung von Systemprüfungen durch die Datenschutzkommission.
 - Eine **Verknüpfung** externer Datenbestände mit polizeilichen Daten ist am problematischsten und sollte nur bei ganz wenigen Dateien erlaubt sein.
- Datenschutzrechtlich **äußerst problematisch** und daher tabu sollten die folgenden Datenbestände sein:
- Daten über die Gesinnung, politische Überzeugung, Religions- oder Gewerkschaftszugehörigkeit. Ebenso Daten über die Mitgliedschaft bei Vereinen, die Teilnahme an Veranstaltungen oder das Abonnieren von Zeitungen.
 - Daten über die Gesundheit oder das Sexualleben.
 - Daten, deren Überwachung die Menschen in der freien Ausübung der Bewegungsfreiheit einschränken würden. Der Aufenthaltsort eines Menschen soll nicht durch Auswertung von Bankomatbehebungen, Kreditkarten- oder Chipkarteneinsatz oder durch Daten des Road-Pricing ermittelt werden dürfen.
 - Unzulässig soll auch die systematische Auswertung fremdenpolizeilicher Evidenzen sein. Dabei ist die Gefahr zu groß, Vorurteilen und Feindbildern zu folgen: Viele Heroindealer sind Nigerianer. Also überprüft man in einem konkreten Fall alle in Österreich gemeldeten Nigerianer. Macht man das immer, dann findet man natürlich nur nigerianische Dealer.