5225/J XX.GP

DRINGLICHE ANFRAGE

der Abgeordneten Van der Bellen, Freundinnen und Freunde

an den Bundesminister für Inneres

betreffend Überwachungsbefugnisse der Sicherheitsbehörden

“Die wahre staatsrechtliche Struktur eines Gemeinwesens enthüllt sich in der Handhabung der Sicherheitspolizei. Hier wird deutlich, wie es mit den heute in nahezu allen Verfassungen anzutreffenden wohltönenden Deklarationen von Freiheit des Einzelnen und Menschenwürde bestellt ist. Hier finden sich die letzten Schlupfwinkel jener Staatsauffassung, die man mit dem Namen “Polizeistaat” dem immer weiter an Boden gewinnenden rechtsstaatlichen Denken gegenübergestellt hat” (Ludwig Adamovich, 1970).

I.

Wie in den letzten Jahren immer wieder von Politikern, insbesondere den jeweiligen Innenministern, betont wird, ist in Österreich die Gesamtkriminalität gegenüber dem Vorjahr zurückgegangen. So auch im Jahre 1997 gegenüber 1996. Trotzdem wurden in den letzten Jahren die sicherheitsbehördlichen Befugnisse zur Überwachung der in Österreich lebenden Bürgerinnen ständig ausgeweitet. Rechtsstaatliche Grundsätze werden durch polizeistaatliches Denken zurückgedrängt. So ist neben den kleineren Novellierungen des Sicherheitspolizeigesetzes (z.B. Schaffung einer Gefährdungskartei) insbesondere die Einführung des Lauschangriffes und der Rasterfahndung zu erwähnen.

Auch wenn nicht nachvollziehbar ist, warum angesichts zunehmender Aufklärungsquote neue Ermittlungsmethoden wie Lauschangriff und Rasterfahndung eingeführt werden mussten, so sind alle diese Befugnisse doch mit den grundlegenden Aufgaben der Sicherheitsbehörden in Einklang zu bringen. Die zuletzt vom Innenministerium vorgeschlagenen Befugnisse für die Sicherheitsbehörden, nämlich die allgemeine Gefahrenerforschung, die Sicherheitsüberprüfung und die Regierungsinformation sind mit den sicherheitsbehördlichen Aufgaben zum Schutz der Öffentlichen Ruhe, Ordnung und Sicherheit nicht mehr zu vereinbaren. Der Schutz der Öffentlichen Ruhe und Sicherheit verpflichtet die Sicherheitsbehörden zur Verhütung allgemeiner Gefahren.

Die Gefahrendefinition knüpft nach Lehre und Rechtsprechung an gerichtlich strafbare Handlungen an. Demnach liegt eine sicherheitspolizeilich relevante Gefahr dann vor, wenn die Verwirklichung bestimmter Delikte des StGB unmittelbar bevorsteht oder schon begonnen hat. Den Begriff der öffentlichen Ordnung definiert der VwGH als “die Gesamtheit jener ungeschriebenen Regeln für das Verhalten des Einzelnen in der Öffentlichkeit, deren Befolgung als unentbehrliche Voraussetzung für ein gedeihliches Miteinander der Menschen angesehen wird”. Außerdem gehört zu den Aufgaben der Polizei laut BVG die erste allgemeine Hilfeleistungspflicht. In einem modernen demokratischen Staat ist das Monopol legitimer physischer Gewalt mit dem Versprechen verbunden, für die Sicherheit aller seiner Bürgerinnen zu sorgen. Das heißt, die Sicherheitsbehörden haben im Interesse und zum Schutz der einzelnen BürgerInnen unserer Gesellschaft tätig zu werden und nicht zur Aufrechterhaltung einer abstrakten Ruhe und Ordnung.

Einen wesentlichen Teil der Befugnisse betrifft die Ermittlung, Verarbeitung und Weitergabe personenbezogener Daten. Es handelt sich hiebei um einen der schwerwiegendsten Eingriffe in das Privat - und Familienleben durch die Sicherheitsbehörden. Laut Auskunft des Innenministers haben ca 27.000 Sicherheitsbeamte Zugang zu den verschiedenen Dateninformationssystemen des Innenministeriums. Pro Tag erfolgen ca 93.000 Zugriffe zu den verschiedensten Dateninformationsnetzen. Ob von den Sicherheitsbehörden personenbezogene Daten ermittelt werden oder nicht und in welchem Umfang personenbezogene Daten verarbeitet werden, darüber gibt es für die betroffenen Personen keine Informationen und auch keine Kontrollmöglichkeit. Wenn die Daten nicht gelöscht werden, können die betroffenen BürgerInnen auch nichts machen. So kann eine genaue Verkehrs - oder Grenzkontrolle Zufall sein oder Folge einer Datenermittlung durch die Sicherheitsbehörden aufgrund irgendeines Vorfalles. Der/die Betroffene weiß es nicht. Es gibt nach den gesetzlichen Bestimmungen keine Informationspflicht für die Behörden. Selbst bei widerrechtlich ermittelten Daten werden die betroffenen Personen nicht verständigt, wie zuletzt vom Innenminister in einer Anfrage erklärt wurde. Das in der EU - Datenschutzrichtlinie verankerte Widerrufsrecht setzt aber eine ausführliche Information in jeder Beziehung voraus.

Es ist bekannt, dass jahrelang von zwei Beamten des Innenministeriums Daten missbräuchlich an Privatdetekteien weitergegeben wurden. Daten wurden und werden aber auch auf andere Art und Weise widerrechtlich ermittelt, verarbeitet und übermittelt.

1. Es gibt zahlreiche Fälle, in denen personenbezogene Daten, die aufgrund einer Anzeige ermittelt wurden, trotz der Einstellung des Strafverfahrens oder Zurücklegung der Anzeige durch die Staatsanwaltschaft, an andere Behörden übermittelt und von diesen verwendet werden.

   Es sind uns mehrere Fälle bekannt, in denen von den Sicherheitsbehörden derartige Akten offensichtlich an die Staatsbürgerschaftsbehörden übermittelt wurden. So ist in einem Erkenntnis des VwGH zu lesen; Im Zeitraum vom Juli 1992 bis Anfang Oktober 1992 sei Herr N.N. wegen Verdachtes der gewerbsmäßigen Schleppertätigkeit beamtshandelt worden. Die Behörde hat sich den Akt zur Einsicht kommen lassen, widmete in der Folge den Erhebungen und Mitteilungen der Anzeige an die Staatsanwaltschaft breiten Raum und kam “bei eigener Betrachtung und Bewertung” zum Schluss, dass der strafrechtliche Verdacht zu Recht bestanden habe.

2. Bekannt ist auch, dass von den Sicherheitsbehörden im Zeitraum von 1993 bis 1997 Tausende Personen wegen Verstoss gegen § 16 Suchtgiftgesetz in rechtswidriger Weise erkennungsdienstlich behandelt hat und die Daten verarbeitet wurden. Dies wurde von der Datenschutzkommission in einzelnen Fällen festgestellt. Die zuständige BH hat sich in ihrem Vorgehen auf eine Weisung des Innenministeriums berufen.

   In der Anfragebeantwortung vom 1. September 1998 zu 4835/J erklärte der Innenminister, dass eine Verständigung der Betroffenen gesetzlich nicht vorgesehen sei, da das Gesetz davon ausgehe, dass der Betroffene durch die persönliche Anwesenheit von dieser Maßnahme Kenntnis habe. Wenn nicht einmal die Behörde über die gesetzlichen Bestimmungen Bescheid wusste, wie kann dann von den betroffenen Jugendlichen dies verlangt werden? Da aber Jugendliche nicht auf die Rechtswidrigkeit aufmerksam gemacht werden, konnten sie davon auch nicht Kenntnis haben.

   Gemäß § 63 SPG sind unrichtige oder entgegen den Bestimmungen dieses Gesetzes ermittelte Daten unverzüglich richtig zu stellen oder zu löschen. Der Innenminister handelt neuerlich rechtswidrig, wenn er eine Löschung nur vornehmen will, wenn die Ermittlung nicht im Einklang mit der neuen Rechtslage nach Inkrafttreten des Suchtmittelgesetzes steht. Im übrigen ist es unverantwortbar, die Löschung rechtswidrig ermittelte Daten nicht unverzüglich zu veranlassen, sondern diese Daten vorerst zu überprüfen, ob sie nicht doch aus anderen Gründen in Evidenz gehalten werden können. Rechtswidrig ermittelte Daten sind zu löschen, und zwar ohne wenn und aber.

3. Zuletzt sind uns wiederum von der Gemeinde Pressbaum in Niederösterreich Fälle von Jugendlichen bekannt geworden, die aufgrund des Verdachtes, in einer Runde mit anderen Personen Haschisch mitgeraucht zu haben, erkennungsdienstlich behandelt und entsprechend unter Druck gesetzt wurden. In diesen Fällen des “Mitrauchens” handelt es sich um einen sogenannten “Eigengebrauch”, was eine Ermittlung erkennungsdienstlicher Daten unzulässig macht.

4. Grundsätzlich sind personenbezogene Daten nach Erfüllung der Aufgaben wieder zu löschen (§ 63 Abs. 1 SPG). Im Zuge einer ausgeschriebenen Fahndung (Abgängigkeitsanzeige), dies kann Minderjährige oder psychisch Behinderte betreffen, werden die Daten aber für fünf Jahre gespeichert und erst nach sieben Jahren gelöscht, obwohl in den meisten Fällen bereits nach kurzer Zeit der Grund der Ermittlung weggefallen ist. Die Auskunft für eine psychisch kranke Person, die vom Krankenhaus davongelaufen war und zur Fahndung ausgeschrieben wurde, lautet folgendermaßen:

   “Speicherungsgrund: Festnehmen und Vorführen: Entwichener Geisteskranker”
   “Löschungsdatum: (...)2005” (sieben Jahre nach Ausschreibung)

   In einem anderen Fall wird ebenfalls von einem entwichenen “Geisteskranken” gesprochen und festgehalten, dass die Vormerkung erst im Jahre 2038 außer Kraft tritt.

Abgesehen davon, dass nach der letzten Novelle zum Sicherheitspolizeigesetz (mit der Novellierung des Waffengesetzes) der Hinweis auf die psychische Krankheit (“Geisteskranker”> nicht nur geschmacklos, sondern auch

rechtswidrig ist, widerspricht auch die Dauer der Speicherung der Daten den Notwendigkeiten und den gesetzlichen Bestimmungen.

5. Als Herr S. L. von seiner Möglichkeit, in den Stapo - Akt Einsicht zu nehmen, Gebrauch machte, musste er feststellen, dass sich auch das Heeresabwehramt offensichtlich mit ihm beschäftigt hatte. Aus einem Aktenvermerk ging hervor, dass sich das HAA bei seinem damaligen Dienstgeber nach den privaten und beruflichen Aktivitäten erkundigte und sich dabei als “Staatspolizei” ausgab. Da dies offensichtlich die Staatspolizei störte, wurde ein Aktenvermerk angebracht, der wörtlich lautet: “Schon wieder missbräuchliche Verwendung "Staatspolizei" durch HAA.” Dabei handelt es sich offensichtlich um keinen Einzelfall.

6. Der Innenminister plante mit der Novelle zum SPG die Aufgabenbereiche der Sicherheitsbehörden um die “Gefahrenerforschung” auszuweiten. Damit könnten - wie derzeit von den Heeresnachrichtendiensten - unter dem Titel der Gefahrenerforschung sämtliche kritische Personen und Gruppierungen überwacht werden, so wie derzeit der Verteidigungsminister die Tätigkeit des Heeresabwehramtes mit der Überwachung von Personen, die sich kritisch über die Einrichtung des Bundesheeres oder deren Anschaffungen äußern, rechtfertigt. Der Sicherheitsapparat wird damit zu einem Metternichschen Machtinstrumentarium missbraucht, das bei Bedarf gegen kritische politische Gegner verwendet werden kann. Allenfalls werden dann die Akten sogar mit nach Hause genommen oder in Parteiinstitutionen gelagert, wie wir zuletzt feststellen mussten. Diese Praxis entspricht polizeistaatlichen Methoden, die mit unseren demokratischen Grundsätzen nicht vereinbar sind. Es gibt keinen ersichtlichen Grund, über gewählte Vertreter/innen des Volkes oder Mitglieder von Regierungen Akten anzulegen, auch wenn sie sich kritisch zu Einrichtungen wie den Sicherheitsbehörden oder der Landesverteidigung äußern. Die kritische Beurteilung von Handlungen und Institutionen unseres Staates ist die tagtägliche Aufgabe unserer Politiker/innen und wesentlicher Bestandteil eines demokratischen Systems.

   Die Veröffentlichung kriminalpolizeilicher Ermittlungen in der Zeitschrift “Top” (Nr. 7/9 vom September 1997) mit Namen und Anschrift mehrerer Tatverdächtiger belegt die Bedenken, dass nach Wunsch Daten gegen Personen weitergegeben und politisch verwendet werden.

7. Unter diesen Gesichtspunkten kann einer Ausweitung der Befugnis der Sicherheitsbehörden, personenbezogene Daten zu ermitteln, nur abgelehnt werden. Dies vor allem auch deshalb, da damit Bereiche erfasst werden, die mit der Aufgabenerfüllung der Sicherheitsbehörden nichts zu tun haben. So kann es nicht Aufgabe der Sicherheitsbehörden sein, für private Unternehmen Sicherheitsüberprüfungen von zukünftigen Angestellten privater Firmen vorzunehmen. Denn selbst wenn die JobbewerberInnen einer derartigen Überprüfung zustimmen (wer einen Job will, wird in der Regel keine Alternative dazu haben), so widerspricht diese Praxis den arbeitsverfassungsrechtlichen Grundsätzen, dass ArbeitnehmerInnen nicht verpflichtet sind, Angaben ihren Privatbereich betreffend den ArbeitgeberInnen bekanntzugeben. So sind laut Judikatur des Obersten Gerichtshofes Frauen nicht verpflichtet, den ArbeitgeberInnen über ihre Schwangerschaft Auskunft zu erteilen. Mit nichts zu rechtfertigen ist die Sicherheitsüberprüfung von Personen, die im gemeinsamen Haushalt des Betroffenen leben und volljährig sind, da in diesen Fällen nicht einmal die Zustimmung dieser Personen einzuholen ist. Mit der möglichen

Überprüfung des Vorlebens der betroffenen Personen ist zu befürchten, dass entgegen der Datenschutzrichtlinie der EU Daten betreffend politischer Meinung, religiöser oder philosophischer Überzeugungen oder die Gewerkschaftszugehörigkeit sowie Daten über Gesundheit und Sexualleben ermittelt werden.

8. Auch die Ermittlung personenbezogener Daten über Personen zur Warnung der Bundesregierungsmitglieder und Landeshauptleute steht im krassen Widerspruch zu den gesetzlich verankerten Aufgaben der Sicherheitsbehörden und ist daher aus datenschutzrechtlichen Grundsätzen abzulehnen. Es kann nicht angehen, dass z.B. bei einer Ausstellungseröffnung, an der auch ein Regierungsmitglied teilnimmt, über sämtliche Gäste sowie die VeranstalterInnen Datenermittlungen durchgeführt werden, um das Regierungsmitglied oder den Landeshauptmann vor zukünftigen Vorwürfen einer bestimmten Oppositionspartei zu warnen.

Der zuletzt bekanntgewordene Datenmissbrauch durch Beamte des Innenministeriums hat einerseits gezeigt, dass auch in Hinkunft derartige Missbräuche nicht ausgeschlossen werden können und dass es nur möglich ist, nach dem Zufallsprinzip strengere Kontrollen durchzuführen. Auch wenn es bisher bereits Kontrollen gab, so konnten diese Beamten doch jahrelang Daten an Privatdetekteien verkaufen. Dieses Beispiel zeigt deutlich, dass ein Schutz vor Missbrauch personenbezogener Daten nur dann besteht, wenn die Daten überhaupt nicht ermittelt werden. Außerdem ist die Kontrolle durch die betroffenen Personen auszubauen. Dies setzt allerdings voraus, dass diese über die von ihnen ermittelten Daten informiert werden, da sie ansonsten von dem in der EU - Richtlinie verankerten Recht auf Widerruf gegen Daten nicht Gebrauch machen können.

II.

Im Europäischen Parlament wurde im September eine Studie betreffend die Bewertung der Technologien für eine politische Kontrolle diskutiert. Die aktualisierte Zusammenfassung wurde der Einfachheit halber direkt übernommen, da diesen Ausführungen nichts hinzuzufügen ist und sich eine Menge Fragen ergeben, zumal der IM derzeit in der EU - Ratspräsidentschaft nur durch das “Strategiepapier” negativ aufgefallen ist, zum Ausbau und Schutz der Rechte der Bürgerinnen - insbesondere gegen Überwachungsmaßnahmen - aber noch keinen Beitrag geleistet hat.

EINE BEWERTUNG DER TECHNOLOGIE FÜR EINE POLITISCHE KONTROLLE

Zusammenfassung, September 1998
Aktualisierte Zusammenfassung als Unterlage für die September - Tagung 1998

INHALTSVERZEICHNIS

1. EINLEITUNG

Das vorliegende Dokument ist eine Zusammenfassung der Zwischenstudie “Eine Bewertung der Technologien für eine politische Kontrolle” (PE 166.499), nachstehend "Zwischenstudie” genannt, die von der Omega Foundation in Manchester erstellt und am 18. Dezember 1997 dem STOA - Gremium und am 27. Januar 1998 dem Ausschuß für Grundfreiheiten und innere Angelegenheiten vorgelegt wurde.

Als bekannt wurde, daß die elektronische Überwachung auf der Tagesordnung der September - Tagung 1998 des Europäischen Parlaments stehen würde, wurde die Omega Foundation aufgefordert, eine aktualisierte Zusammenfassung der Zwischenstudie als Unterlage für diese Sitzung zu erarbeiten. Die aktualisierte Zusammenfassung deckt verschiedene Bereiche der in der Zwischenstudie abgehandelten Technologien für eine politische Kontrolle ab. Das Dokument befaßt sich in seiner gegenwärtigen Form jedoch nur mit der spezifischen Frage der elektronischen Überwachung. Nur die vollständige Fassung enthält auch die Fußnoten und die Bibliographie.

Die Zwischenstudie wurde mit großem Interesse aufgenommen, und die ausführlichen Pressekommentare in - und außerhalb der Europäischen Union beweisen, wie sehr die Öffentlichkeit über viele der in der Studie beschriebenen Neuerungen beunruhigt ist. Diese aktualisierte Zusammenfassung orientiert sich an den gleichen grundlegenden Zielsetzungen wie die Zwischenstudie, wobei es darum geht,

(i) den Mitgliedern des Europäischen Parlaments ein knappes Nachschlagewerk über die jüngsten Fortschritte im Bereich der Technologie für eine politische Kontrolle zur Verfügung zu stellen;

(ii)den gegenwärtigen Stand der Technik im Bereich der herausragendsten Entwicklungen zu klären und zu beschreiben und die Teile der Zwischenstudie, die in der Öffentlichkeit größte Besorgnis hervorgerufen haben, weiter zu klären und zu aktualisieren;

(iii)den Mitgliedern des Europäischen Parlaments eine Darstellung der gegenwärtigen Trends sowohl in Europa als auch weltweit zu geben;

(iv)politische Optionen für Strategien zur Regelung der künftigen demokratischen Kontrolle und Verwaltung dieser Technologie vorzuschlagen;

(v)weiteres kurzgefaßtes Informationsmaterial zu liefern, um die Antwort des Parlaments auf die vorgeschlagene Erklärung der Kommission über elektronische

Abhöreinrichtungen zu untermauern, die auf die Tagesordnung der Sitzung des Europäischen Parlaments am Mittwoch, dem 16. September 1998, gesetzt wurde.

2. ENTWICKLUNGEN IN DER ÜBERWACHUNGSTECHNOLOGIE

Unter Überwachungstechnologie versteht man Vorrichtungen oder Systeme, die die Bewegungen von Personen, ihres Eigentums oder anderer Vermögenswerte überwachen, verfolgen und bewerten können. Diese Technologie wird zu einem großen Teil dazu eingesetzt, die Tätigkeiten von Dissidenten Menschenrechtsaktivisten, Journalisten, Studentenführern, Minderheiten, Gewerkschaftsführern und politischen Gegnern zu verfolgen. Eine ganze Reihe von Überwachungsgeräten wurde entwickelt, wie beispielsweise Nachtsichtgeräte, Parabolmikrophone zum Abhören von Gesprächen in über 1 km Entfernung, Lasermikrophone, die jedes Gespräch von einem geschlossenen Fenster in Sichtweite aus verfolgen können, die “Danish Jai” - Stroboskopkamera, die in wenigen Sekunden Hunderte von Aufnahmen machen und alle Teilnehmer an einer Demonstration oder an einem Marsch einzeln photographieren kann, und das automatische Fahrzeugerkennungssystem, das mit Hilfe eines geographischen Informationssystems von Karten Autos in einer Stadt verfolgen kann.

Die ursprünglich für die Verteidigung und die Geheimdienste entwickelten neuen Technologien haben sich nach dem Kalten Krieg schnell für die Strafverfolgung und im privaten Sektor durchgesetzt. Dabei handelt sich um einen jener Bereiche des technologischen Fortschritts, in dem überholte Vorschriften nicht mit der immer weiter verbreiteten mißbräuchlichen Verwendung Schritt halten konnten. Bis zu den 60er Jahren waren die meisten Überwachungsgeräte technologisch einfach und teuer, da sie voraussetzten, daß man den Verdächtigen auf Schritt und Tritt folgte, wozu bis zu 6 Personen in Zweierteams, die in drei Achtstunden - Schichten arbeiteten, nötig waren. Alle Informationen und erzielten Kontakte wurden schriftlich festgehalten und abgelegt, wobei wenig Aussicht auf eine schnelle Überprüfung bestand. Auch die elektronische Überwachung war sehr arbeitsintensiv. Beispielsweise beschäftigte die ostdeutsche Polizei 500.000 geheime Informanten, wovon 10.000 ausschließlich dazu eingesetzt wurden, die Telefongespräche der Bürger abzuhören und niederzuschreiben.

In den 80er Jahren entstanden neue Formen der elektronischen Überwachung, von denen viele auf die Automatisierung des “Lauschangriffs” abzielten. Dieser Trend wurde in den USA in den 90er Jahren durch erhöhte Regierungsausgaben am Ende des Kalten Krieges angekurbelt, wobei das Verteidigungsministerium und der Geheimdienst zur Rechtfertigung ihrer Budgets neue Aufgaben zugeteilt bekamen und ihre technologische Ausstattung auf bestimmte Bereiche der Strafverfolgung wie die Bekämpfung von Drogenhandel und Terrorismus übertragen wurde. 1993 unterzeichneten das US - Verteidigungsministerium und das US - Justizministerium Vereinbarungen über “andere Einsätze als Krieg und Strafverfolgung”, um eine gemeinsame Weiterentwicklung und Nutzung der Technologie zu ermöglichen. David Banisar von Privacy International stellt dazu folgendes fest: “Computer - und Elektronikunternehmen expandieren als Reaktion auf die in den 80er Jahren einsetzenden Kürzungen bei den Verträgen im Rüstungssektor auf neue Märkte - im In - und Ausland -, und zwar mit ursprünglich für militärische Zwecke entwickelten Geräten. Unternehmen wie E Systems, Electronic Data Systems und Texas Instruments verkaufen fortschrittliche Computersysteme und Überwachungsgeräte

an Staats - und Lokalregierungen. die sie für die Strafverfolgung, für Grenzkontrollen und die Verwaltung im Sozialwesen einsetzen. Wovon die ostdeutsche Geheimpolizei nur träumen konnte, wird in der freien Welt schnell zu einer Realität."

2.1 Fernsehüberwachungsnetze (CCTV)
Die Technik der Fernsehüberwachung hat sich in den letzten Jahren rasch weiterentwickelt. Natürlich photographieren Polizei und Agenten immer noch Demonstrationen und Personen von Interesse, aber solche Bilder können zunehmend gespeichert und abgerufen werden. Dank der gegenwärtigen Entwicklung zur Ultraminiaturisierung sind solche Geräte jetzt tatsächlich unauffindbar und können sowohl von Einzelpersonen als auch Unternehmen und offiziellen Behörden mißbräuchlich eingesetzt werden.

Die Mitgliedstaaten der Europäischen Union vertreten ganz unterschiedliche Positionen im Zusammenhang mit CCTV - Kameranetzen, wobei in Dänemark derartige Kameras gesetzlich verboten sind, während es im Vereinigten Königreich bereits Hunderte von CCTV - Netzen gibt. Trotzdem sollte man sich auf einen auf dem Grundsatz des Datenschutzes basierenden, allgemein gültigen gemeinsamen Standpunkt zur Stellung der bestehenden Systeme einigen. Eine besondere Überlegung betrifft den rechtlichen Status der Zulässigkeit von digitalem Material, wie es von fortschrittlicheren CCTV - Systemen geliefert wird, als Beweismittel. Ein großer Teil dieser Materialien wird unter die Datenschutzgesetze fallen, wenn das gesammelte Material beispielsweise über ein Autokennzeichen oder über eine Uhrzeit abgerufen werden kann. Da das von solchen Systemen gelieferte Material unbemerkt editiert werden kann, muß die europäische Datenschutzrichtlinie in Primärrecht umgesetzt werden; so kann geklärt werden, welches Recht für CCTV gilt, um Verwirrung sowohl unter den Inhabern von CCTV - Datenbanken als auch unter den Bürgern als erfaßte Personen zu vermeiden. Das Primärrecht wird es ermöglichen, die Auswirkungen der Richtlinie auf Tätigkeitsfelder auszudehnen, die nicht unter das Gemeinschaftsrecht fallen.
Artikel 3 und 13 der Richtlinie sollten verhindern, daß der Einsatz von CCTV im Inland unter allen Umständen gerechtfertigt ist.

Die eigenen Verhaltenskodizes, wie beispielsweise jener der Local Govemment Information Unit (LGIU, 1996) im Vereinigten Königreich, sollten die besten Erfahrungen aller EU - Mitgliedstaaten berücksichtigen, um den Einsatz aller CCTV - Überwachungssysteme in der Öffentlichkeit und insbesondere in Wohngebieten abzudecken. Als erster Schritt sollte der Ausschuß für Grundfreiheiten offiziell in Erwägung ziehen, die Praxis und Kontrolle von CCTV - Systemen in den Mitgliedstaaten zu prüfen, um festzustellen, welche Aspekte der verschiedenen Verhaltenskodizes in einen einheitlichen Kodex und einen durchsetzbaren Rechtsrahmen für die Strafverfolgung und den Schutz der Grundfreiheiten sowie die Wiedergutmachung übernommen werden könnten.

2.2 Algorithmische Überwachungssysteme

Die nächste Generation der Kontrolltechnologie wird die städtische Überwachung revolutionieren, weil eine zuverlässige Wiedererkennung von Gesichtern möglich wird. Derartige Systeme werden zunächst stationär eingesetzt werden, beispielsweise an Drehtüren, Zollübergängen, Sicherheitsübergängen usw., wo eine

vollständige Standardgesichtserkennung stattfinden kann. Der Zwischenstudie zufolge wird Anfang des 21. Jahrhunderts die Gesichtserkennung über CCTV eine Realität sein, und die Länder mit CCTV - Infrastrukturen werden solche Technologien als natürliche Weiterentwicklung betrachten. Tatsächlich hat die amerikanische Firma Software and Systems in London ein System getestet, das Menschenmengen scannen und die Gesichter mit den in die Datenbank eines entfernten Computers eingespeicherten Bildern vergleichen kann. Wir stehen am Beginn einer Revolution der “Algorithmischen Überwachung” - also Datenanalyse mittels komplexer Algorithmen, die eine automatisierte Erkennung und Verfolgung ermöglicht. Eine derartige Automatisierung erweitert nicht nur das Überwachungsnetz, es verringert auch die Maschenweite (siehe Norris, C. , et. al, 1998).

Analog dazu wurden auch Fahrzeugerkennungssysteme entwickelt, die ein Kennzeichen erkennen und dann das Fahrzeug mittels eines computerisierten geographischen Informationssystems durch eine Stadt verfolgen können. Solche Systeme sind bereits im Handel, beispielsweise das 1994 von der britischen Firma Racal zu einem Preis von £ 2000 eingeführte System Talon. Das System ist so ausgelegt, daß es bei Tag wie bei Nacht Kennzeichen auf der Grundlage eines neuronalen Netzwerks erkennen kann, das von Cambridge Neurodynamics entwickelt wurde. Ursprünglich wurde es für die Verkehrsüberwachung eingesetzt, aber seine Funktionen wurden in den letzten Jahren so weiterentwickelt, daß es nunmehr auch für
Sicherheitsüberwachungen einsetzbar ist und in den “Ring of Steel” um London integriert wurde. Das System kann alle Fahrzeuge aufzeichnen, die an einem bestimmten Tag in den Überwachungsraum einfahren oder ihn verlassen.

Es ist wichtig, daß klare Richtlinien und Verhaltenskodizes für solche technologische Innovationen festgesetzt werden, und zwar lange bevor die digitale Revolution neue und unvorhersehbare Möglichkeiten schafft, solche visuellen Bilder zu vergleichen, zu analysieren, zu erkennen und zu speichern. Schon jetzt ermöglichen multifunktionelle Verkehrsmanagementsysteme wie “Traffic Master” (das die Fahrzeugerkennungssysteme zur kartierung und Quantifizierung von Staus verwendet) ein nationales Überwachungssystem. Diese Vorschriften müssen auf eindeutigen Datenschutzgrundsätzen basieren und Artikel 15 der Europäischen Richtlinie von 1995 über den Schutz von natürlichen Personen und die Verarbeitung von personenbezogenen Daten berücksichtigen. Dieser Artikel lautet im wesentlichen wie folgt: “Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden, die ausschließlich aufgrund einer automatisierten Verarbeitung von Daten [...] ergeht. (1) Es spricht vieles dafür, daß das Europäische Parlament den in einem jüngst erschienenen Bericht des britischen House of Lords enthaltenen Ratschlag befolgt (Bericht des Fachausschusses über digitale Bilder als Beweismittel, 1998). Dieser Rat lautet: (i) daß das Europäische Parlament ... “sowohl für den öffentlichen als auch den privaten Sektor Leitlinien für den Einsatz des Datenvergleichs und insbesondere für die Verbindung von Überwachungssystemen mit anderen Datenbanken vorgibt; (ii) daß der für den Datenschutz zuständige Beamte ermächtigt wird, den Betrieb von Datenvergleichssystemen zu überprüfen”.

Derartige Überwachungssysteme werfen erhebliche Probleme im Zusammenhang mit der Verantwortlichkeit auf, insbesondere wenn sie autoritären Regimes zur Verfügung gestellt werden. Die am Platz des Himmlischen Friedens eingesetzten Kameras wurden von Siemens Plessey als fortschrittliches Verkehrskontrollsystem

vertrieben. Nach den Studentenmassakern im Jahr 1989 kam es jedoch zu einer Hexenjagd, als die Behörden bei dem Versuch, die Rebellen aufzuspüren, Tausende folterten und verhörten. Das mit Pelco - Kameras aus den USA arbeitende Überwachungssystem Scoot wurde eingesetzt, um die Proteste genau aufzuzeichnen. Die Bilder wurden im chinesischen Fernsehen wiederholt ausgestrahlt,
wobei eine Belohnung für Informationen ausgesetzt wurde, mit dem Ergebnis, daß fast alle Regimegegner identifiziert wurden. Die demokratische Verantwortlichkeit ist also das einzige Kriterium, das moderne Verkehrsüberwachungssysteme von fortschrittlichen Technologien zum Aufspüren von Dissidenten unterscheidet. Ausländische Firmen exportieren Verkehrskontrollsysteme nach Lhasa in Tibet, obwohl Lhasa bis jetzt noch keine Verkehrsüberwachungsprobleme hat. Das Problem dabei könnte ein sträflicher Mangel an Vorstellungskraft sein.

2.3 Wanzen und Abhörgeräte

Eine große Zahl von Wanzen und Abhörgeräten wurde entwickelt, um Gespräche aufzunehmen und Telefonverbindungen abzuhören. In den letzten Jahren war der weitverbreitete illegale und legale “Lauschangriff” sowie das Setzen von “Wanzen” ein Thema in vielen europäischen Staaten. Illegale Wanzen sind jedoch eine Technologie von gestern. Moderne Schnüffler können mit Hilfe von speziell ausgestatteten Laptop - Computern alle Mobiltelefone abhören, die in ihrem Erfassungsbereich aktiv sind, indem sie die entsprechende Nummer anklicken. Das Gerät kann sogar “interessante” Nummern anpeilen, um zu überprüfen, ob gerade ein Gespräch geführt wird. Diesen Wanzen und Abhörvorrichtungen kommt jedoch angesichts der nationalen und internationalen Abhörvorrichtungen, die von den Regierungen unterhalten werden, keinerlei Bedeutung mehr zu.

2.4 Nationale und internationale Netze zum Anzapfen von Femmeldeverbindungen

In der Zwischenstudie wird das globale Überwachungssystem im Detail beschrieben, das die Massenüberwachung von allen Telekommunikationsverbindungen einschließlich von Telefon, E - Mail und Faxübertragungen von privaten Bürgern, Politikern, Gewerkschaften und Unter nehmen ermöglicht. In den letzten Jahren war eine politische Verlagerung hinsichtlich der
Zielgruppe zu verzeichnen. Anstatt ein Verbrechen zu untersuchen (was eine Reaktion darstellen würde), verfolgen die Stratverfolgungsbehörden zunehmend bestimmte soziale Klassen und Rassen, die in gefährdeten Gebieten leben, bevor ein Verbrechen begangen wird - eine Form der Datenüberwachung für eine präventive Polizeiarbeit, die auf militärischen Modellen zur Sammlung von enormen Mengen einfacher Daten basiert.

Ohne Verschlüsselung sind die modernen Kommunikationssysteme transparent für fortschrittliche Abhörvorrichtungen, die zum Mithören eingesetzt werden können. In der Zwischenstudie wird auch erklärt, welche inhärenten Überwachungs - und Abhörmöglichkeiten Mobiltelefone bieten, die von der Polizei und Geheimdiensten genutzt werden können. Beispielsweise impliziert die digitale Technologie, die dazu benötigt wird, die Telefonbenutzer für ankommende Verbindungen aufzuspüren, daß alle Benutzer von Mobiltelefonen in einem Land aufgespürt werden können, wenn das Telefon empfangsbereit ist, wo immer sie sich aufhalten, und ihr jeweiliger Aufenthaltsort im Computer der Gesellschaft gespeichert werden kann. Die

Schweizer Polizei hat beispielsweise insgeheim den Aufenthaltsort von Mobiltelefonbenutzern vom Computer des Anbieters Swisscom aus verfolgt, der der Sonntags Zeitung zufolge die Bewegungen von mehr als einer Million Abonnenten in einer Genauigkeit von wenigen hundert Metern und für mindestens ein halbes Jahr gespeichert hat.

Von allen in der Zwischenstudie behandelten Entwicklungen erregte jedoch jenes Kapitel am meisten Besorgnis, das sich mit den verfassungsmäßigen und rechtlichen Fragen im Zusammenhang mit dem Zugang der amerikanischen nationalen Sicherheitsbehörde zu allen europäischen Fernmeldeverbindungen mit der Möglichkeit, diese anzuzapfen beschäftigt. Es bestreitet zwar niemand die Rolle solcher Netze bei der Bekämpfung des Terrorismus, des Drogenhandels, der Geldwäsche und des illegalen Waffenhandels, das Ausmaß des in der Studie dargestellten Netzes zum Abhören von Auslandsgesprächen sowie die Frage, ob die bestehenden Rechtsvorschriften, der Datenschutz und der Schutz der Privatsphäre in den Mitgliedstaaten ausreichend sind, um die Vertraulichkeit von Verbindungen zwischen EU - Bürgern und Unternehmen mit jenen in Drittländern zu gewährleisten, gaben jedoch Anlaß zu großer Sorge.

Da durch Presseberichte anschließend einige Verwirrung gestiftet wurde, sollen an dieser Stelle etliche der Fragen im Zusammenhang mit der transatlantischen elektronischen Überwachung geklärt und ein kurzer Überblick über die früheren und die jüngsten Entwicklungen seit Veröffentlichung der Zwischenstudie im Januar 1998 gegeben werden Es gibt im wesentlichen zwei unterschiedliche Systeme, nämlich:

(i) Das System VK/USA, das die Tätigkeiten der militärischen Nachrichtendienste wie NSA - CIA in den USA umfaßt und an das GCHQ und M16 im Vereinigten königreich angeschlossen sind, die das als ECHELON bekannte System betreiben.

(ii)Das System EU - FBI, das verschiedene Strafverfolgungsbehörden untereinander verbindet, wie beispielsweise FBI, Polizei, Zoll, Einwanderungsbehörden und Behörden der inneren Sicherheit.

Da der Titel von Punkt 44 der Tagesordnung für die Sitzung des Europäischen Parlaments am 16. September 1998(2) immer noch Verwirrung stiften könnte - vom Standpunkt des Nachrichtendienstes aus gesehen handelt es sich dabei um zwei unterschiedliche “Gemeinschaften” -, sei hier noch kurz auf die Aktivitäten beider Systeme eingegangen: auf die Bereiche Echelon, Verschlüsselung, Überwachung EU - FBI und neue Schnittstellen, die beispielsweise Zugang zu Internetanbietern und Datenbanken anderer Behörden bieten.

2.4.1 ANZAPFUNG ALLER FERNMELDEVERBINDUNGEN IN DER EU DURCH DIE NSA

Der Zwischenstudie zufolge werden in Europa alle E - Mail -, Telefon - und Faxverbindungen routinemäßig von der Nationalen Sicherheitsagentur der Vereinigten Staaten angezapft, und alle Zielinformationen werden vom Europäischen Festland über das strategische Zentrum in London und über das wichtige Zentrum in Menwith Hill in den North York Moors des Vereinigten Königreiches über Satellit nach Fort Meade in Maryland weitergeleitet.

Dieses System wurde erstmals in den 70er Jahren von einer Gruppe von Forschern im Vereinigten Königreich entdeckt (Campbell, 1981). Ein vor kurzem erschienenes Buch von Nicky Hager, “Secret Power” (Hager, 1996), liefert umfassende Details über ein als ECHELON bekanntes Projekt. Hager interviewte mehr als 50 Personen, die mit dem Nachrichtendienst zu tun haben, um zu belegen, daß dieses globale Überwachungssystem die ganze Welt umfaßt und ein Zielsystem auf allen wichtigen Intelsatelliten bildet, die dazu verwendet werden, die meisten Verbindungen über Satellitentelefon, Internet, E - Mail, Fax und Telex weiterzuleiten. Diese Stationen befinden sich in Sugar Grove und Yakima in den Vereinigten Staaten, in Waihopai in Neuseeland, in Geraldton in Australien, in Hongkong und in Morwenstow im Vereinigten Königreich.

Das ECHELON - System gehört zum UKUSA - System, aber im Gegensatz zu vielen elektronischen Spionagesystemen, die während des Kalten Krieges entwickelt wurden, wurde ECHELON hauptsächlich für nichtmilitärische Zielgruppen entworfen: Regierungen, Organisationen und Unternehmen in praktisch allen Ländern, Das ECHELON - System zapft wahllos sehr große Mengen von Verbindungen an und wertet dann durch künstliche Intelligenz wie Memex zum Auffinden von Schlüsselwörtern die wertvollen Informationen aus. Fünf Staaten können die Ergebnisse nutzen, wobei gemäß dem UK/USA - Abkommen von 1948 die USA der Hauptpartner sind und Großbritannien, Kanada, Neuseeland und Australien eine untergeordnete Position einnehmen.

Alle fünf Zentren stellen den anderen vier Partnern “Wörterbücher” der Schlüsselworte, Sätze, Personen und anzuzapfende Anschlüsse zur Verfügung, und die angezapfte Verbindung wird sofort an das Land weitergeleitet, daß den entsprechenden Antrag gestellt hat. Einerseits werden so zwar viele Informationen über potentielle Terroristen gesammelt, es gibt aber andererseits auch viele wirtschaftliche Einsätze, insbesondere für die intensive Überwachung all jener Länder, die an den GATT - Verhandlungen teilnehmen. Aber Hager stellte fest, daß die weitaus wichtigsten Prioritäten dieses Systems weiterhin im Bereich der militärischen und politischen Geheimdienste liegen, die die so gewonnenen Nachrichten für ihre Interessen nutzen können.

Hager zitiert “ hochrangige Geheimagenten”, die mit dem Observer in London gesprochen haben. “Wir glauben, daß wir in Anbetracht dessen, was wir für groben Mißbrauch und Fahrlässigkeit in unserem Arbeitsumfeld halten, nicht länger Stillschweigen bewahren können.” Als Beispiel nannten sie die Anzapfung von drei karitativen Organisationen, einschließlich Amnesty International und Christian Aid, durch GCHQ. "GCHQ kann deren Verbindungen jederzeit für Routinezielerhebungen abhören”, sagten die GCHQ - Informanten. Das Verfahren für das Abhören von Telefonverbindungen ist als Mantis bekannt, bei Telexen wird es Mayfly genannt. Durch die Eingabe eines Codes für Hilfe für die Dritte Welt konnte die Quelle beweisen, daß die Telexe aller drei Organisationen überprüft werden können. Ohne jede Regelung der Verantwortlichkeit ist es schwierig festzustellen, welche Kriterien ausschlaggebend dafür sind, ob eine Person oder Organisation zum Ziel erklärt wird oder nicht.

Seit Erscheinen der Zwischenstudie haben Journalisten tatsächlich behauptet, daß ECHELON amerikanischen Firmen, die im Waffenhandel tätig sind, zugute gekommen ist und die Stellung Washingtons in ausschlaggebenden Gesprächen mit Europa im Rahmen der Welthandelsorganisation während einer Auseinandersetzung im Jahre 1995 mit Japan bezüglich der Ausfuhr von Fahrzeugteilen gestärkt hat. Der

Financial Mail On Sunday zufolge “umfassen die von US - Experten identifizierten Schlüsselwörter die Namen von zwischenstaatlichen Handelsorganisationen und Unternehmenskonsortien, die gegen US - Firmen bieten. Das Wort “Block” steht auf der Liste, um Verbindungen ausmachen zu können, die Off - shore - Ölvorkommen in Gebieten betreffen, wo der Meeresgrund noch in Explorationsblöcke eingeteilt werden muß”... Es wurde auch angedeutet, daß sich die USA 1990 in geheime Verhandlungen eingemischt und Indonesien dazu gebracht haben, den amerikanischen Riesenkonzern AT&T an einem Telecom - Vertrag in Höhe von mehreren Milliarden Dollar zu beteiligen, als es an einem gewissen Punkt so aussah, als ob der Vertrag ausschließlich an die japanische NEC gehen würde.

Die Sunday limes (11. Mai 1998) berichtete, daß die Radome von Menwith Hill (NSA Station F83) in North Yorkshire, Vereinigtes Königreich, schon bald die Aufgabe erhielten, die Verbindungen von international tätigen Transportunternehmen (ILC) abzuhören - im wesentlichen handelt es sich dabei um gewöhnliche Geschäftsverbindungen. Das Personal stieg von 400 Mitarbeitern in den 80er Jahren auf derzeit über 1.400 an; zusätzlich sind 370 Bedienstete des Verteidigungsministeriums dort tätig. Die Sunday Times berichtete auch von Behauptungen, daß Gespräche zwischen der deutschen Firma Volkswagen und General Motors abgehört wurden und daß sich die Franzosen beschwert haben, daß Thompson - CSF, die französische Elektronikfirma, einen Vertrag in Höhe von 1,4 Milliarden Dollar über die Lieferung eines Radarsystems an Brasilien verloren hätte, weil die Amerikaner die Details der Verhandlungen abgehört und an die US - Firma Raytheon weitergeleitet haben, die anschließend den Auftrag erhielt. Ferner wird behauptet, daß Airbus Industry ein Vertrag in Höhe von 1 Milliarde Dollar an Boeing und McDonnel Douglas verlorenging, weil entsprechende Informationen vom amerikanischen Geheimdienst abgehört wurden. Andere Zeitungen, wie Liberation (21. April 1998) und Il Mondo (20. März 1998), definierten das Netz aufgrund der Achse UK - USA als angelsächsisches Spionagenetz. Privacy International geht noch weiter. Sie räumt zwar ein, daß “streng genommen weder die Kommission noch das Europäische Parlament das Recht haben, Sicherheitsfragen durch Vorschriften zu regeln bzw. in Sicherheitsfragen einzugreifen .., sie tragen jedoch die Verantwortung dafür, daß dieser Bereich in der ganzen Union harmonisiert wird”.

Privacy International zufolge dürfte das Vereinigte Königreich feststellen, daß seine Verbindungen im Rahmen der “besonderen Beziehungen” gegen seine Verpflichtungen aus dem Vertrag von Maastricht verstoßen, da es in Titel V des Vertrags von Maastricht heißt: “Zu jeder außen - und sicherheitspolitischen Frage von allgemeiner Bedeutung findet im Rat eine gegenseitige Unterrichtung und Abstimmung zwischen den Mitgliedstaaten statt, damit gewährleistet ist, daß ihr vereinter Einfluß durch konvergierendes Handeln möglichst wirksam zum Tragen kommt.” Im Bereich der besonderen Beziehungen kann Großbritannien jedoch keine offenen Anhörungen mit seinen anderen europäischen Partnern durchführen. Die Situation wird weiter dadurch kompliziert, daß in der französischen Zeitschrift Le Point die Gegenbehauptung aufgestellt wird, daß die Franzosen über den Helios 1A - Spionagesatelliten systematisch die Telefon - und Kabelverbindungen der Vereinigten Staaten und der anderen alliierten Länder überwachen (limes, 17. Juni, 1998).

Selbst wenn nur die Hälfte all dieser Behauptungen zutrifft, muß das Europäische Parlament Maßnahmen ergreifen, um zu gewährleisten, daß so mächtige Überwachungssysteme jetzt, da der Kalte Krieg zu Ende ist, auf Grundlage eines demokratischeren Konsens funktionieren. Natürlich entspricht die Politik der

Mitgliedstaaten der Europäischen Union in Übersee nicht immer jener der USA, und im wirtschaftlichen Bereich ist Spionage nach wie vor Spionage. Keine Behörde der USA würde es einem ähnlichen Spionagenetz der EU ermöglichen, von amerikanischem Boden aus zu agieren, ohne diesem, falls es überhaupt geduldet würde, strikte Beschränkungen aufzuerlegen. Nach einer umfassenden Erörterung der Auswirkungen des Betriebs derartiger Netze sollte das Europäische Parlament geeignete Verfahren für die unabhängige Überprüfung und Überwachung schaffen; alle Bemühungen um ein Verbot der Verschlüsselung durch EU - Bürger sollten, falls ihnen überhaupt stattgegeben wird, solange zurückgestellt werden, bis demokratische und verantwortliche Systeme geschaffen wurden.

2.4.2 GLOBALES TELEKOMMUNIKATIONSÜBERWACHUNGSSYSTEM EU-FBI

Ein großer Teil der Nachforschungen und Untersuchungen, die notwendig waren, um die Geschichte, Struktur, Rolle und Funktion des Abkommens EU - FBI zur Legitimisierung globaler elektronischer Überwachung bekanntzumachen, ist Statewatch zu verdanken, der hoch angesehenen britischen Organisation für Kontrolle und Forschung im Bereich der Grundfreiheiten.

Statewatch hat die Unterzeichnung des Transatlantischen Abkommens in Madrid beim Gipfeltreffen EU - USA vom 3. Dezember 1995 ausführlich beschrieben - einen Teil davon bildet der “gemeinsame Aktionsplan EU - USA”. In der Folge hat Statewatch festgestellt, daß diese Bemühungen einen Versuch darstellen, die Atlantische Allianz in der Ära nach dem Kalten Krieg neu zu definieren, wobei man mit Hilfe dieser Haltung mehr und mehr die Anstrengungen interner Sicherheitsbehörden zu rechtfertigen sucht, die in Europa zunehmend Polizeiarbeit übernehmen. Statewatch merkt an, daß der erste gemeinsame Aktionsplan zur Überwachung nicht im Rat für Justiz und Inneres erörtert wurde, sondern ausgerechnet im Rat für Fischereifragen vom 20. Dezember 1996 als A - Punkt (ohne Aussprache) nebenbei angenommen wurde.

Im Februar 1997 berichtete Statewatch, daß die EU die geheime Vereinbarung getroffen hat, ein internationales Netz zum Abhören von Telefongesprächen einzurichten, und zwar über ein geheimes Netz von Ausschüssen, die im Rahmen des “dritten Pfeilers” des Vertrags von Maastricht für die Zusammenarbeit im Bereich der öffentlichen Ordnung gebildet werden. Die Hauptpunkte des Plans sind in einer Vereinbarung festgelegt, die 1995 von den EU - Staaten unterzeichnet wurde (ENFOPOL 112 10037/95 25.10.95) und die immer noch unter Verschluß gehalten wird. Dem Guardian zufolge (25.2.97) spiegelt er die Sorge der europäischen Nachrichtendienste wider, daß die moderne Technologie sie daran hindern wird, private Verbindungen abzuhören. Dem Bericht zufolge sollten die EU - Länder sich auf “internationale Abhörstandards einigen, die eine Kodierung gewährleisten würden; andernfalls könnten verschlüsselte Wörter von Regierungsbehörden entschlüsselt werden”. Offiziellen Berichten zufolge einigten sich die Regierungen der EU-Staaten darauf, eng mit dem FBI in Washington zusammenzuarbeiten. Frühere Protokolle dieser Sitzungen legen jedoch die Vermutung nahe, daß die ursprüngliche Initiative von Washington ausging. Statewatch zufolge müssen Anbieter von Netzen und den entsprechenden Diensten in der EU “abhörbare” Systeme installieren und jede Person oder Gruppe überwachen, wenn sie einen Abhörbefehl erhalten.

Diese Pläne wurden weder den europäischen Regierungen noch dem Ausschuß für Grundfreiheiten des Europäischen Parlaments zur Prüfung vorgelegt, obwohl die Frage der Grundfreiheiten durch solche unverantwortliche Systeme eindeutig aufgeworfen wird. Die Entscheidung, diese Entwicklung voranzutreiben, wurde nur im geheimen im Rahmen eines “schriftlichen Verfahrens” durch den Austausch von Telexen zwischen den 15 Regierungen der EU - Staaten getroffen. Statewatch teilt mit, daß der globale Überwachungsplan EU - FBI nun “außerhalb des dritten Pfeilers” weiterentwickelt wird. In der Praxis bedeutet dies, daß der Plan von einer Gruppe von 20 Ländern - den 15 EU - Mitgliedstaaten plus USA, Australien, Kanada, Norwegen und Neuseeland - weiterentwickelt wird. Diese Gruppe von 20 Ländern hat weder dem Rat (Justiz und Inneres) noch dem Europäischen Parlament noch den einzelstaatlichen Parlamenten Rechenschaft abzulegen. Die Finanzierung dieses Systems wird nicht erwähnt, aber in einem Bericht der deutschen Bundesregierung wird angegeben, daß allein der Teil des Pakets, der die Mobiltelefone betrifft, schätzungsweise 4 Milliarden DM kosten wird.

Statewatch zieht die Schlußfolgerung, daß “die Schnittstelle zwischen dem ECHELON - System und seiner potentiellen Weiterentwicklung im Bereich der Telefonverbindungen, gemeinsam mit der Standardisierung der von der EU und den USA finanzierten Zentren und Ausrüstungen für “abhörbare Verbindungen”, eine wirklich globale Bedrohung darstellt, die keinerlei rechtlichen oder demokratischen Kontrollen unterliegt” (Pressemitteilung vom 25.2.97). In vielerlei Hinsicht handelt es sich dabei um Treffen von Agenten eines neuen globalen Staats des militärischen Geheimdienstes. Es ist für alle sehr schwierig, sich ein vollständiges Bild davon zu machen, was in den hochrangig besetzten Treffen zur Festlegung dieser “transatlantischen Agenda” beschlossen wird. Statewatch erzielte zwar einen Entscheid des Bürgerbeauftragten, der ihm Einsicht in die Vereinbarung gewährt, weil der Ministerrat “den Zugangscode falsch angewandt hat”; bislang wurde jedoch noch niemandem Einblick in die Akten gewährt. Und ohne solche Einsicht in die Unterlagen müssen wir uns damit abfinden, daß die Entscheidungen hinter verschlossenen Türen getroffen werden. Die Erklärung der Kommission zu ECHELON und den transatlantischen Beziehungen, die einen noch nie dagewesenen Vorgang darstellt und die für den 16 September angesetzt ist. wird vermutlich durch das, was sie verschweigt, ebensoviel Aussagekraft haben wie durch das, was sie der Öffentlichkeit preisgibt. Die Mitglieder des Europäischen Parlaments könnten die folgenden politischen Optionen in Erwägung ziehen:

2.5 POLITISCHE OPTIONEN

(i) Eine Reihe von detaillierteren Untersuchungen zu den sozialen, politischen, kommerziellen und verfassungsmäßigen Auswirkungen des in der Studie beschriebenen globalen elektronischen Überwachungsnetzes sollte im Hinblick auf die Abhaltung einer Reihe von Anhörungen von Experten als Grundlage für die künftige Politik der EU im Bereich der Grundfreiheiten in Auftrag gegeben werden. Diese Untersuchungen könnten folgende Bereiche abdecken;

(a) die verfassungsmäßigen Fragen, die sich im Zusammenhang mit der Möglichkeit der nationalen Sicherheitsagentur (NSA) der Vereinigten Staaten, alle europäischen Fernmeldeverbindungen anzuzapfen, ergeben, und insbesondere die rechtlichen Verpflichtungen der Mitgliedstaaten im Zusammenhang mit dem Vertrag

von Maastricht sowie die gesamte Problematik des Einsatzes dieses Netzes für die automatisierte politische und wirtschaftliche Spionage;

(b) die sozialen und politischen Auswirkungen des globalen Überwachungssystems FBI - EU, der dadurch mögliche wachsende Zugriff auf die neuen Kommunikationsmedien einschließlich E - Mail und die weitere Expansion in neue Länder, gemeinsam mit allen damit zusammenhängenden finanziellen und verfassungsrechtlichen Fragen;

(c) die Struktur, Rolle und Aufgabe eines EU - weiten Überwachungsgremiums, das unabhängig vom Europäischen Parlament eingesetzt werden könnte, um die Tätigkeiten aller Organisationen zu überprüfen und überwachen, die sich mit dem Anzapfen von Telekommunikationsverbindungen in Europa beschäftigen.

(ii) Das Europäische Parlament hat die Möglichkeit, darauf zu drängen, die Vorschläge der Vereinigten Staaten abzulehnen, private Nachrichten über das globale Kommunikationsnetz (Internet) für die amerikanischen Nachrichtenbehörden zugänglich zu machen. Ferner sollte das Parlament den neuen kostspieligen Verschlüsselungskontrollen nicht zustimmen, bevor innerhalb der EU eine umfassende Debatte über die Auswirkungen derartiger Maßnahmen stattgefunden hat. Diese Auswirkungen betreffen die Grund - und Menschenrechte der europäischen Bürger und die kommerziellen Rechte der Unternehmen, sich ohne ungerechtfertigte Überwachung durch Nachrichtenbehörden, die mit multinationalen Konkurrenten zusammenarbeiten, im Rahmen des Gesetzes zu betätigen.

(iii) Das Europäische Parlament sollte eine Reihe von Anhörungen von Experten einberufen, welche all die technischen, politischen und kommerziellen Tätigkeiten der Organisationen zum Thema haben, die sich mit der elektronischen Überwachung beschäftigen. Ferner sollte es mögliche Strategien ausarbeiten, um diese Tätigkeiten so zu gestalten, daß sie den Grundsätzen der demokratischen Verantwortlichkeit und Transparenz entsprechen. Bei diesen Anhörungen könnte man sich auch mit der Frage von eigenen Verhaltenskodizes befassen, um im Fall von Unregelmäßigkeiten und mißbräuchlicher Verwendung eine Wiedergutmachung zu gewährleisten. Man sollte in Kriterien ausdrücklich festlegen, wer überwacht werden darf und wer nicht, wie diese Daten gespeichert, verarbeitet und weitergeleitet werden dürfen und ob solche Kriterien und die entsprechenden Verhaltenskodizes öffentlich zugänglich gemacht werden sollten.

(iv) Das Mandat des Ausschusses für Grundfreiheiten und innere Angelegenheiten sollte dahingehend erweitert werden, daß es die Befugnisse und Zuständigkeiten für alle Fragen im Zusammenhang mit den Grundfreiheiten umfaßt, die durch elektronische Überwachungsgeräte und Netze aufgeworfen werden; im Rahmen seines nächsten Arbeitsprogrammes sollte er eine Reihe von Berichten fordern, in denen folgenden Fragen nachgegangen wird.

(a) Wie könnten rechtlich verbindliche Verhaltenskodizes gewährleisten, daß neue Überwachungstechnologien den Datenschutzgesetzen entsprechen?

(b) Die Vorgabe von Leitlinien hinsichtlich der Praxis des Datenvergleichs und insbesondere der Verbindung von Überwachungssystemen mit anderen Datenbanken sowohl für den öffentlichen als auch für den privaten Sektor; dabei sollte auf die Frage eingegangen werden, wie man den Datenschutzbeauftragten der

Mitgliedstaaten entsprechende Befugnisse zur Überprüfung des Betriebs von Datenvergleichssystemen erteilen könnte.

(c) Welche weiteren Rechtsvorschriften sollten erlassen werden, um den Verkauf von elektronischen Abhörgeräten und Wanzen an Privatpersonen und Unternehmen zu regeln, so daß ihr Verkauf durch die gesetzliche Erlaubnis und nicht durch eine Selbstregulierung bestimmt wird?

(d) Wie kann gewährleistet werden, daß das Abhören von Telefongesprächen durch die Mitgliedstaaten auf einem Verfahren der öffentlichen Verantwortung, wie in a) oben erwähnt, beruht (z.B. wäre es denkbar, daß man für das Abhören von Telefonen eine Genehmigung beantragen muß, die vom jeweiligen Parlament in einem bestimmten Verfahren erteilt wird; in den meisten Fällen können die Strafverfolgungsbehörden nur unter höchst außergewöhnlichen Umständen, die der Genehmigungsbehörde so rasch wie möglich mitgeteilt werden müssen, Telefongespräche eigenmächtig abhören).

(e)Wie ist es möglich, die Technologien, mit deren Hilfe automatisch Kundenprofile und Anrufmuster für Freundschafts - und Kontaktnetze erstellt werden können, durch die gleichen Rechtsvorschriften zu regeln wie das Abhören von Telefongesprächen, und wie können sie dem Parlament des jeweiligen Mitgliedstaates gemeldet werden?

(f) Eine Untersuchung sollte in Auftrag gegeben werden, um festzustellen, welcher Art in den Mitgliedstaaten die besten Erfahrungen bei der Überprüfung von CCTV sind, um zu ermitteln, welche Aspekte der verschiedenen Verhaltenskodizes in einen einheitlichen kodex und ein rechtliches Rahmenwerk übernommen werden könnten, das die Strafverfolgung, den Schutz der Grundfreiheiten sowie die Wiedergutmachung abdeckt.

(v) Schaffung von Verfahrensmechanismen durch die zuständigen Ausschüsse des Europäischen Parlaments, die Vorschläge für Technologien prüfen, die Auswirkungen auf die Grundfreiheiten im Zusammenhang mit der Überwachung haben (beispielsweise der Ausschuß für Telekommunikationen); diese Ausschüsse sollten verpflichtet werden, alle einschlägigen Vorschläge und Berichte an den Ausschuß für Grundfreiheiten weiterzuleiten, damit dieser sich dazu äußern kann, bevor irgendwelche politischen oder finanziellen Entscheidungen über deren Nutzung getroffen werden.

(vi) Abkommen zwischen den Mitgliedstaaten über die Übermittlung der jährlichen Statistiken über das Abhören von Verbindungen in einer standardisierten und einheitlichen Form an die Parlamente der einzelnen Mitgliedstaaten. Diese Statistiken sollten umfassende Angaben zur tatsächlichen Zahl der angezapften Verbindungen enthalten, und die Daten sollten nicht aggregiert sein (um zu vermeiden, daß die Statistiken nur die Zahl der erteilten Genehmigungen ausweisen, während die überwachten Organisationen Hunderte von Mitgliedern haben können, deren Telefone angezapft werden).

(1) Gemeinsamer Standpunkt (EG) Nr. 1/95, vom Rat festgelegt am 20. Februar 1995 im Hinblick auf den Erlaß der Richtlinie 95/../EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

(2) Erklärung der Kommission - Transatlantische Beziehungen/Echelon - System. Transatlantische Beziehungen nach dem Gipfeltreffen EU - USA vom 18. Mai und der Einsatz von Überwachungstechniken im Bereich der Kommunikation.

Die unterfertigten Abgeordneten stellen daher folgende

ANFRAGE:

I. Fragen betreffend Überwachungsmaßnahmen in Österreich:

1. Wieviele Personen sind vom Datenmissbrauch der beiden Beamten des Innenministeriums betroffen?

2. Wurden diese Personen davon informiert?

3. Laut APA - Aussendung wurden angeblich Daten unter anderem auch an "seriöse Firmen" weitergegeben. In Zukunft soll dies mit der Sicherheitsüberprüfung legalisiert werden. Wie rechtfertigen Sie die Sicherheitsüberprüfung für private Unternehmen, aber auch für Beamte mit den Aufgaben der Sicherheitsbehörden?

4. Warum werden von Ihnen die zahlreichen Jugendlichen, die in rechtswidriger Weise in den Jahren 1993 bis 1997 erkennungsdienstlich behandelt wurden, nicht verständigt?

5. Bis wann können diese betroffenen Jugendlichen damit rechnen, dass die ermittelten Daten gelöscht werden?

6. Warum werden nach wie vor Jugendliche - wie zuletzt in Pressbaum -, die Haschisch nur in einer Runde mitrauchen (zum Eigengebrauch besitzen), erkennungsdienstlich behandelt?

7. Werden Sie dafür sorgen, dass in allen Fällen, in denen die Daten rechtswidrig ermittelt wurden und von Amts wegen zu löschen sind, die betroffenen Personen davon verständigt werden?

8. In zahlreichen Fällen wurden personenbezogene Daten, auch nachdem die Staatsanwaltschaft keine Anzeige erstattet hatte, an andere Behörden, insbesondere Staatsbürgerschaftsbehörden, weitergeleitet und diesen Personen ein erheblicher Schaden zugefügt. Wie rechtfertigen Sie dieses rechtswidrige Vorgehen?

9. Der Antrag auf Widerruf ermittelter Daten kann nur eingebracht werden, wenn auch bekannt ist, dass von den Behörden Daten ermittelt wurden. Werden Sie daher dafür sorgen, dass grundsätzlich alle betroffenen Personen, über die personenbezogene Daten ermittelt werden, davon informiert werden?

10. Wie vereinbaren Sie die Sicherheitsüberprüfung insbesondere für private Firmen mit den Aufgaben der Sicherheitsbehörden?

11. Wie rechtfertigen Sie die im Entwurf zur Novelle des Sicherheitspolizeigesetzes verankerte Regierungsinformation mit den Aufgaben der Sicherheitsbehörden?

12. Warum scheint bei der Ermittlung von personenbezogenen Daten psychisch Behinderter oder Kranker nach wie vor der Hinweis auf diesen Umstand (“Geisteskranker”) auf?

13. Wie rechtfertigen Sie die Tatsache, dass in den Fällen der nach § 57 Abs. 1 Z 7, 8 und 9 SPG ermittelten personenbezogenen Daten, diese nach Widerruf der Fahndung (Erfüllung der Aufgabe) offensichtlich nicht gesperrt werden?

14. Haben Sie Untersuchungen angestellt, ob von weiteren ehemaligen Innenministern bzw. Beamten der” Stapo” Kopien von “Stapo - Akten” angefertigt und mitgenommen wurden?

15. Ist es richtig, dass, wie vom ehemaligen Innenminister Soronics der Presse mitgeteilt wurde, in der politischen Akademie der ÖVP mehrere Stapo - Akten bzw. Kopien gelagert sind?

16. Wie der Fall des Herrn J.L. zeigt, gaben sich in vielen Fällen Beamte der Heeresnachrichtendienste als Staatspolizisten aus. Wie häufig hat es derartige Vorfälle gegeben und was wurde dagegen unternommen? Wurde von Ihrem Ministerium Anzeige erstattet?

17. Werden von Ihrem Ministerium Daten auch an die Heeresnachrichtendienste übermittelt?

18. Wenn ja, in welchen Fällen und aufgrund welcher gesetzlicher Grundlagen?

19. Durch den Akt von Doris Kammerlander - Pollet ist bekannt geworden, dass das Heeresabwehramt auch die Kraftfahrzeugnummern und - daten notierten. Haben die Beamten der Heeresnachrichtendienste Zugriff auf die KFZ - Dateien?

20. Wie beurteilen Sie die Ermittlung personenbezogener Daten durch die heeresnachrichtlichen Dienste, wie sie im Entwurf für ein Militärbefugnisgesetz festgeschrieben sind?
Fragen betreffend Überwachungsmaßnahmen auf EU - Ebene:

21. Wissen Sie von der Existenz eines multilateralen Telekommunikationsüberwachungssystems namens “Echelon”, wie es vom Zwischenbericht des wissenschaftlichen Dienstes des Europäischen Parlaments beschrieben wird?

22. Kennen Sie das “Transatlantische Abkommen” von Madrid vom 3.12.1995 und eine dabei getroffene geheime Vereinbarung zwischen der EU und den USA, ein internationales Netz zum Abhören von Telefongesprächen einzurichten, und zwar über ein geheimes Netz von Ausschüssen, die im Rahmen des III. Pfeilers des Vertrages von Maastricht für die Zusammenarbeit im Bereich der öffentlichen Ordnung gebildet werden?

23. Wenn ja, war Österreich an Vorbereitungen und/oder dem Abschluss der Vereinbarung in irgendeiner Weise beteiligt?

24. Wenn ja, ist Österreich an dieses Abkommen gebunden?

25. Hat die österreichische Bundesregierung Kenntnis davon, dass bei der Überwachung der österreichischen Telekommunikation eine technische Einrichtung der NSA in Bad Albung eingesetzt wird?

26. Kennen Sie zu diesem Abkommen einen gemeinsamen Action - Plan zur Überwachung des Telefonverkehrs?

27. Was ist der Inhalt des EU - Dokumentes ENFOPOL 112 10037/95?

28. Können Sie den Bürgern und Bürgerinnen Österreichs garantieren, dass Telefongespräche oder der Telekommunikationsverkehr in, von und nach Österreich von einer Behörde eines Drittstaates niemals systematisch abgehört werden?

29. Ist ein Joint Action “out of area” - Überwachungsplan als sogenannter A - Punkt im Rat für Fischereifragen beschlossen worden, und wenn ja, wann?

30. Hat Österreich diesem Plan zugestimmt?

31. Entspricht es den Tatsachen, dass unter österreichischer Ratspräsidentschaft eine Entschließung zur “Überwachung des Telekommunikationsverkehrs in Bezug auf neue Technologien” erarbeitet wird?

32. Entspricht es den Tatsachen, dass sich darin die Mitgliedsländer verpflichten, allen Telekommunikationsbetreibern auf ihrem Staatsgebiet alle technischen Vorkehrungen aufzuerlegen, die eine umfassende Überwachung aller Telefongespräche, Emails, Internetaktivitäten, TeilnehmerInnendaten, Standortbestimmung von Handy - TeilnehmerInnen und des Kommunikations - inhaltes ermöglichen sollen?

33. Entspricht es den Tatsachen, dass unter österreichischem EU - Vorsitz ein Rechtshilfeübereinkommen vorbereitet wird, das die grenzüberschreitende Überwachung des gesamten Telekommunikationsverkehrs erleichtern soll?

34. Ist es richtig, dass im Zusammenhang mit der im Amsterdamer Vertrag vorgesehenen Erweiterung der operativen Kompetenzen von Europol eine Situation eintreten könnte, in der Europol eine zur Überwachung des Telekommunikationsverkehrs legitimierte Behörde wird, ohne der Kontrolle des EuGH und ohne der Kontrolle des Europäischen Parlaments zu unterliegen?

35. Ist es richtig, dass durch die Ausweitung der operativen Befugnisse von Europol eine Aushöhlung nationaler Grundrechte und Rechtsschutzgarantien kommen könnte?

36. Ist es richtig, dass aufgrund einer pauschalen Ermächtigung des Rates im Amsterdamer Vertrag die Ausweitung der operativen Befugnisse von Europol keiner Legitimation durch die nationalen Parlamente mehr bedarf?

37. Sehen Sie, Herr Bundesminister, in den angeführten Entwicklungen im Bereich der inneren Sicherheit eine Gefahr für die Grund - und Bürgerrechte in Europa?

38. Was haben Sie unternommen, um sicherzustellen, dass es in der Europäischen Union durch den Ausbau der inneren Sicherheit zu keiner Schwächung, Aushöhlung und Gefährdung von Grundrechten und rechtsstaatlichen Prinzipien kommen kann?

39. Können Sie garantieren, dass es zu keinerlei operativen Kompetenzen kommt, ohne dass die Immunität der Europol - Bediensteten vor Strafverfolgung aufgehoben wird?

40. Teilen Sie die Auffassung, dass im Falle einer Destabilisierung der Demokratie oder einer Regierungsübernahme durch eine extrem rechte Partei diese Überwachungsmaßnahmen ohne Gesetzesänderung eine komplette Bespitzelung jedes/jeder beliebigen Bürgers/Bürgerin ermöglicht?

In formeller Hinsicht wird die dringliche Behandlung dieser Anfrage gemäß § 93 Abs. 2 GOG verlangt.