5005/99/endg.
WP 18

Gruppe für den Schutz von Personen
bei der Verarbeitung personenbezogener Daten

Empfehlung 2/99
zur
Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs

Angenommen am 3. Mai 1999

Empfehlung 2/99 zur

Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN -

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und Artikel 30 Absätze 1 und 3 dieser Richtlinie[2],

gestützt auf ihre Geschäftsordnung, insbesondere die Artikel 12 und 14,

empfiehlt,

bei den auf europäischer Ebene zur Überwachung des Fernmeldeverkehrs beschlossenen Maßnahmen die Grundrechte und -freiheiten natürlicher Personen, insbesondere ihre Privatsphäre und das Brief- und Fernmeldegeheimnis, zu achten.

Der Anwendungsbereich dieser Empfehlung zielt auf die Überwachungen im weiteren Sinne ab, d.h. die Überwachung des Inhalts des Fernmeldeverkehrs, aber auch der mit dem Fernmeldeverkehr zusammenhängenden Daten, insbesondere durch vorbereitende Maßnahmen wie "Monitoring" und "Datamining" der Verkehrsdaten, die beabsichtigt sein könnten, um über die Zweckmäßigkeit einer Überwachung zu entscheiden[3].

A. Geltungsbereich der europäischen Bestimmungen zur Überwachung des Fernmeldeverkehrs

1. In der Entschließung des Rates vom 17. Januar 1995 über die rechtmäßige Überwachung des Fernmeldeverkehrs[4] werden die technischen Voraussetzungen für die Überwachung des Fernmeldeverkehrs genannt, ohne dabei auf die Bedingungen einzugehen, die bei

[1] Richtlinie vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl L 281 vom 23.11.1995, S. 31.

[2] Die drei Mitglieder, die die Registertilsynet (Dänemark), die Commission Nationale de l'Informatique et des Libertés (CNIL, Frankreich) bzw. den Data Protection Registrar (Vereinigtes Königreich) vertreten, haben über diese Empfehlung nicht mit abgestimmt, da das behandelte Thema ihres Erachtens nicht in den Zuständigkeitsbereich der Gruppe fällt. Sie unterstützen aber allgemein den Inhalt der Empfehlung.

[3] Dieses umfassendere Verständnis des Begriffs der Überwachung des Fernmeldeverkehrs entspricht dem Anwendungsbereich der später (Kapitel 1.1) zitierten Entschließung des Rates vom 17.1.1995 über rechtmäßige Überwachung des Fernmeldeverkehrs und dem allgemeinen Rahmen der geltenden einschlägigen Rechtsbestimmungen (s. unten, Kapitel B).
Die Empfehlung findet somit auf die Überwachung des nichtöffentlichen Fernmeldeverkehrs auf dem Internet Anwendung. Besondere Aufmerksamkeit widmet die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten im Rahmen der gleichzeitig durch die "task force Internet" der Gruppe erfolgenden Arbeiten der allgemeinen Problematik der Verarbeitung personenbezogener Daten im Zusammenhang mit der Entwicklung des Internets.

[4] ABl. C 329 vom 14.11.1996.

einer solchen Überwachung gegeben sein sollten. Nach dieser Entschließung sind Netzbetreiber und Diensteanbieter verpflichtet, den «gesetzlich ermächtigten Behörden» den überwachten Fernmeldeverkehr unverschlüsselt bereitzustellen.

Dies gilt für Telefonverbindungen über Fest- und Mobilfunknetze, elektronische Post, Fax, Telex und Datenverkehr im Internet und umfaßt sowohl den Inhalt des Fernmeldeverkehrs als auch die mit ihm zusammenhängenden Daten (diese beziehen sich insbesondere auf die Verkehrsdaten, aber auch auf alle von der überwachten Person erzeugten Signale - Ziffer 1.4.4 der Entschließung. Die Daten betreffen neben der überwachten Person auch die Teilnehmer, die diese Person kontaktieren oder von ihr kontaktiert werden[5].

Der Entschließung zufolge müssen die gesetzlich ermächtigten Behörden auch Zugang zu Daten haben, die bei Teilnehmern mobiler Dienste die Bestimmung des geographischen Standorts ermöglichen[6].

Diese Entschließung vom 17.1.1995 wird zur Zeit überarbeitet, insbesondere um sie an die neuen Kommunikationstechniken anzupassen. Der Textentwurf präzisiert u.a. die Anwendung der Überwachungsmaßnahmen auf den Fernmeldeverkehr über Satellit[7].

2. Ferner hat sich die Gruppe mit dem Anwendungsbereich der in der Ratsentschließung vom 17. Januar 1995 vorgesehenen Maßnahmen befaßt. Eine zu einem späteren Zeitpunkt erstellte, nicht veröffentlichte Fassung dieses Dokuments («Absichtserklärung» vom 25. Oktober 1995) sieht vor, daß die Unterzeichner in bezug auf die Spezifizierungen im Bereich der Fernmeldeverkehrsüberwachung mit dem Direktor des «Federal Bureau of Investigation» der Vereinigten Staaten Verbindung aufnehmen können. Vorbehaltlich des Einverständnisses der «Teilnehmer» sollen dieser Fassung zufolge auch andere Staaten am Informationsaustausch teilnehmen und an der Überarbeitung und Aktualisierung der Spezifizierungen mitwirken können.

   Die Gruppe weist zum einen darauf hin, daß die Rechtstellung dieses Texts unklar ist - insbesondere was die gültige Unterzeichnung durch die betroffenen Länder angeht - und er, da nirgendwo veröffentlicht, nach der unten zitierten Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte für den Bürger nicht zugänglich ist. Zum anderen kommt darin der Wille zum Ausdruck, die technischen Vorkehrungen zur Überwachung des Fernmeldeverkehrs in Absprache mit Staaten zu entwickeln, die weder

[5] Ziffer 1.4 des Anhangs der Ratsentschließung vom 17. Januar 1995.

[6] Ziffer 1.5 der oben genannten Entschließung.

[7] Dieser Text (Dokument 10951/1/98, Enfopol 98 Rev. 1) wird derzeit überarbeitet und kann unter "http://www.heise.de/bin/tp/deutsch/special/enfo/63321htm" abgerufen werden. Mit dieser Überarbeitung wird in erster Linie das Ziel verfolgt, die Überwachungsmöglichkeiten auf die neuen Kommunikationstechniken auszudehnen. Eine noch aktuellere Fassung scheint die Zustimmung der Arbeitsgruppe "Polizeiliche Zusammenarbeit" des Rates gefunden zu haben und zur Annahme oder Änderung an das Europäische Parlament weitergeleitet worden zu sein. Offensichtlich soll die neue Entschließung vom Rat am 27.-28. Mai 1999 verabschiedet werden (siehe "Datenschutz-Berater, 15.2.99, S. 5, in dem auf eine nicht veröffentlichte Fassung vom 20.1.99 Bezug genommen wird). Der EP-Ausschuß für Rechte und Bürgerrechte hat dem (federführenden) Ausschuß für Grundfreiheiten und innere Angelegenheiten empfohlen, den überarbeiteten Entwurf der Ratsempfehlung in der ENFOPOL 98 vorgeschlagenen Form u.a. aus Gründen des Schutzes der Privatsphäre und des imminenten Inkrafttretens des Vertrags von Amsterdam abzulehnen (s. Bericht von Herrn Florio). Der Ausschuß für Grundfreiheiten ist dieser Stellungnahme nicht gefolgt und wird somit in der Plenarsitzung vorschlagen, ENFOPOL 98 auf der Grundlage des Berichts von Herrn Schmid anzunehmen. Das Europäische Parlament dürfte Anfang Mai seinen Beschluß fassen.

der Europäischen Menschenrechtskonvention noch den Richtlinien 95/46/EG und 97/66/EG unterliegen.

3. Die Gruppe stellt fest, daß die Ratsentschließung die technischen Aspekte der Überwachung des Fernmeldeverkehrs regeln soll, ohne die nationalen Vorschriften, die das Abhören in juristischer Hinsicht regeln, anzutasten. Einige der in der Entschließung zur Ausweitung der Überwachungsmöglichkeiten vorgesehenen Maßnahmen widersprechen jedoch den nationalen Vorschriften bestimmter EU-Mitgliedstaaten, die ein höheres Maß an Schutz vorsehen (insbesondere Ziffer 1.4, Zugriff auf die verbindungsrelevanten Daten, einschließlich der Verbindungen von Teilnehmern mobiler Dienste, ohne die zur Zeit verfûgbaren vorausbezahlten anonymen Dienste zu berücksichtigen; Ziffer 1.5: Informationen über den geographischen Standort von Teilnehmern mobiler Dienste und Ziffer 5.1: Verbot für Netzbetreiber/Diensteanbieter, Informationen über durchgeführte Überwachungsmaßnahmen nachträglich weiterzugeben).

4. Zwar verfolgt die Ratsentschließung das Ziel des «Schutzes nationaler Interessen, insbesondere der staatlichen Sicherheit und der Aufklärung schwerer Verbrechen», die Gruppe möchte aber auf die Gefahr des Abgehens von diesen ursprünglichen Zielen aufmerksam machen, die durch eine Ausweitung der Überwachungs- und Entschlüsselungstechniken auf eine wachsende Zahl von Ländern - einige davon Drittländer - weiter verschärft würde.

   Das Europäische Parlament vertritt in seiner Entschließung vom 16. September 1998 zu den transatlantischen Beziehungen[8] die Auffassung, daß «die wachsende Bedeutung des Internet und der weltweiten Telekommunikation im allgemeinen und das ECHELON-System im besonderen sowie die Gefahren ihres Mißbrauchs Maßnahmen zum Schutz wirtschaftlicher Daten und eine wirksame Kodierung erfordern».

   Diese Überlegungen verdeutlichen, mit welchen Risiken eine über Fragen der nationalen Sicherheit im engeren Sinne - und sogar über den "dritten Pfeiler" der Europäischen Union - hinausgehende Überwachung des Fernmeldeverkehrs verbunden ist. Vor allem in Anbetracht der gemeinschaftsrechtlichen Bestimmungen zum Schutz der Grundrechte und -freiheiten natürlicher Personen, insbesondere ihrer Privatsphäre, stellt sich die Frage nach ihrer Legitimität.

5. Die Gruppe weist auch darauf hin, daß das Inkrafttreten des Vertrags von Amsterdam hinsichtlich der Maßnahmen zur Überwachung des Fernmeldeverkehrs einen Wechsel der Rechtsgrundlage nach sich ziehen wird. Zur derzeitigen Befugnis des Rates, den Entschließungstext aufgrund der Artikel K.1(9) und K.3(2) des Vertrags zur Zusammenarbeit von Polizei und Justiz auszuarbeiten, tritt ein Initiativrecht der Europäischen Kommission aufgrund des neuen Artikels K.6 § 2.

[8] Plenarsitzung, Sitzungsprotokoll Teil II, B4-0803, 0805, 0806 et 0809/98.

B. Allgemeiner rechtlicher Rahmen

6. Die Gruppe erinnert daran, daß jede Überwachung des Fernmeldeverkehrs, d.h. jede Kenntnisnahme von Inhalt von und/oder Daten im Zusammenhang mit privaten Telekommunikationsverbindungen zwischen zwei oder mehreren Teilnehmern durch einen Dritten, insbesondere der mit der Telekommunikationsnutzung verbundenen Verkehrsdaten, eine Verletzung des Rechts von Einzelpersonen auf Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstellt. Nach Artikel 8 § 2 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950[9] und seiner Auslegung durch den Europäischen Gerichtshof für Menschenrechte ist eine Überwachung nur zulässig, wenn sie drei Anforderungen genügt: eine Rechtsgrundlage ist vorhanden, die Maßnahme ist in einer demokratischen Gesellschaft erforderlich und trägt zu einem der in der Konvention genannten Ziele bei[10].

   Die Rechtsgrundlage muß klare und ausführliche Bestimmungen über Grenzen und Modalitäten dieses Eingriffs umfassen, was insbesondere angesichts der kontinuierlichen Weiterentwicklung der technischen Hilfsmittel erforderlich ist[11]. Die Rechtsvorschrift muß der Öffentlichkeit zugänglich sein, damit die Bürger die Folgen ihres Verhaltens absehen können[12].

   Eine großangelegte sondierende oder allgemeine Überwachung des Fernmeldeverkehrs muß darin untersagt sein[13].

---

[9] Es ist darauf hinzuweisen, daß die vom Europarat für den Bereich Fernmeldeverkehrüberwachung anerkannten Grundgarantien unabhängig von der auf Gemeinschaftsebene getroffenen Unterscheidung zwischen gemeinschaftlicher oder einzelstaatlicher Zuständigkeit für die Staaten Verpflichtungen mit sich bringen.

[10] Auch nach dem Übereinkommen Nr. 108 des Europarates ist eine Einmischung nur zulässig, wenn eine demokratische Gesellschaft sie zum Schutz der in Artikel 9 § 2 des Übereinkommens genannten nationalen Interessen benötigt und sie ausschließlich auf dieses Ziel beschränkt bleibt (doch ist darauf hinzuweisen, daß die im Übereinkommen Nr. 108 und die in der Konvention zum Schutz der Menschenrechte und Grundfreiheiten genannten nationalen Interessen nicht genau übereinstimmen).

[11] Siehe dazu die unten genannten Verpflichtungen des Artikels 4 der Empfehlung Nr. 4 des Europarates vom 7. Februar 1995 zum Schutz personenbezogener Daten in der Telekommunikation, insbesondere bei Telefondiensten.

[12] Urteile Huvig und Kruslin gegen Frankreich vom 25. April 1990, Reihe A Nr. 176 A und B, S. 15 ff.

[13] Siehe insbesondere Urteil Klass vom 6. September 1978, Reihe A Nr. 28, S. 23 ff., und Urteil Malone vom 2. August 1984, Reihe A Nr. 82, S. 30 und ff.

Wie im Urteil Leander vom 25. Februar 1987 weist der Gerichtshof auch im Urteil Klass nachdrücklich auf die Notwendigkeit ausreichender Garantien hin, die einen Mißbrauch ausschließen, da ein geheimes Überwachungssystem zum Schutz der nationalen Sicherheit das Risiko in sich berge, die Demokratie unter dem Vorwand, sie zu verteidigen, zu unterminieren, wenn nicht gar zunichte zu machen (Urteil Leander, Reihe A Nr. 116, S. 14 ff.).

Ob angemessene und ausreichende Garantien zum Auschluß von Mißbräuchen vorhanden sind, ist laut Urteil des Gerichtshofs in der Rechtssache Klass (Randnummern 50 ff.) unter Einbeziehung der genauen Umstände im Einzelfall zu beurteilen. Der Gerichtshof kommt in diesem Urteil zu dem Schluß, daß die einschlägigen deutschen Rechtsvorschriften keine sondierende oder allgemeine Überwachung zulassen und nicht gegen Artikel 8 der Europäischen Menschenrechtskonvention verstoßen. Die deutschen Rechtsvorschriften sehen folgende Garantien vor: eine Überwachung ist nur zulässig, wenn nach Indizienlage der Verdacht besteht, daß bestimmte schwere Straftaten vorbereitet oder begangen werden bzw. begangen worden sind; sie dürfen nur vorgeschrieben werden, wenn eine Feststellung der Tatsachen auf anderem Wege unmöglich oder nur unter erheblich erschwerten Bedingungen möglich ist; auch darf die Überwachung nur die verdächtige Person selbst sowie diejenigen betreffen, die verdächtigt werden, Kontakte zu dieser Person zu unterhalten.

7. Das in den Rechtssystemen der Mitgliedstaaten verankerte Recht auf Schutz der Privatsphäre ist auf Ebene der Europäischen Union in der Richtlinie 95/46/EG[14] festgeschrieben. Die Grundsätze der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten vom 4. November 1950 und des Übereinkommens des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten vom 28. Januar 1981 werden in dieser Richtlinie präzisiert. Die Richtlinie 97/66/EG[15] konkretisiert die Bestimmungen der oben genannten Richtlinie, indem sie die Mitgliedstaaten verpflichtet, die Vertraulichkeit der über öffentliche Telekommunikationsnetze oder öffentlich zugängliche Telekommunikationsdienste übermittelten Nachrichten sicherzustellen.

   Nach Artikel 13 Absatz 1 der Richtlinie 95/46/EG können die Mitgliedstaten Rechtsvorschriften erlassen, die bestimmte in der Richtlinie vorgesehene Pflichten (zum Beispiel im Hinblick auf die Datenerhebung) und Rechte (zum Beispiel das Recht, über eine Datenerhebung informiert zu werden) beschränken[16]. Diese Ausnahmen müssen jedoch auf die dort genannten Fälle beschränkt bleiben, d.h. die Maßnahme muß zum Schutz der unter a) bis g) dieses Artikels genannten öffentlichen Interessen erforderlich sein. Diese sind u.a. die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit und die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten.

   Auch nach Artikel 14 Absatz 1 der Richtlinie 97/66/EG dürfen die Mitgliedstaaten die Pflicht zur Wahrung der Vertraulichkeit von Nachrichten, die über öffentliche Netze übermittelt werden, nur beschränken, wenn dies für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit und die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten erforderlich ist.

C. Pflichten der Netzbetreiber und Diensteanbieter

8. Die Gruppe weist nachdrücklich darauf hin, daß die Pflichten, die die Richtlinien 95/46/EG (Artikel 17 Absätze 1 und 2) und 97/66/EG (Artikel 4, 5 und 6) Netzbetreibern und Diensteanbietern wie auch den Mitgliedstaaten in bezug auf Datensicherheit und -vertraulichkeit auferlegen, die Regel und nicht die Ausnahme sind.

   Sie erinnert daran, daß auch Artikel 7 des Übereinkommens des Europarates Nr. 108 vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und Artikel 4 der Empfehlung Nr. 4 des Europarates vom 7. Februar 1995 zum Schutz personenbezogener Daten in der Telekommunikation,

---

[14] Vom Anwendungsbereich der Richtlinie 95/46/EG ausgenommen sind nach Artikel 3 die Verarbeitung personenbezogener Daten, die für die Ausübung von Tätigkeiten erfolgt, die nicht in den Anwendungsbereich des Gemeinschaftsrechts fallen, sowie Verarbeitungen betreffend die öffentliche Sicherheit, die Landesverteidigung, die Sicherheit des Staates und die Tätigkeiten des Staates im strafrechtlichen Bereich. Die meisten zur Umsetzung dieser Richtlinie bislang erlassenen nationalen Rechtsvorschriften gelten jedoch auch für Bereiche, die nicht unter das Gemeinschaftsrecht fallen.

Das Gemeinschaftsrecht findet Anwendung, sobald richtliniengemäß verarbeitete Daten (z.B. Anrufe, die zur Fakturierung von einem Telekommunikationsanbieter in einer Liste zusammengestellt werden) im Rahmen einer Überwachung ein zweites Mal verarbeitet werden. Die Richtlinie 95/46/EG sieht für diese Überwachungen eine Reihe von Garantien vor, die nachstehend näher erläutert werden.

[15] Richtlinie vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. L 24 vom 30. Januar 1998, S.1.

[16] Diese Rechte und Pflichten sind festgelegt in Artikel 6 Absatz 1 "Grundsätze in bezug auf die Qualität der Daten", Artikel 10 und Artikel 11 Absatz 1 "Information der betroffenen Person" sowie Artikel 12 "Auskunftsrecht der betroffenen Person" und Artikel 21"Öffentlichkeit der Verarbeitungen".

insbesondere bei Telefondiensten, den Netzbetreibern entsprechende Pflichten auferlegen[17].

9. Diese Pflichten implizieren zum einen, daß Netzbetreiber und Diensteanbieter Verkehrsdaten und die Fakturierung betreffende Daten nur unter bestimmten Voraussetzungen verarbeiten dürfen: ausgehend von dem Grundsatz, daß Verkehrsdaten betreffend Teilnehmer und Nutzer gelöscht oder anonymisiert werden müssen, sobald die Verbindung beendet ist, sind die Zweckbestimmungen, für die die Daten verarbeitet werden können, die Dauer ihrer eventuellen Aufbewahrung und der Zugang zu den Daten strikt begrenzt[18].

10. Zum anderen müssen Netzbetreiber und Diensteanbieter demnach die notwendigen Maßnahmen ergreifen, um die Überwachung des Fernmeldeverkehrs für Stellen, die gesetzlich nicht dazu berechtigt sind, je nach Stand der Technik zu erschweren oder unmöglich zu machen.

    Die Gruppe unterstreicht in diesem Zusammenhang, daß der Einsatz effizienter modernster Techniken bei der legitimen Überwachung nicht zu einer generellen Absenkung des Niveaus der Vertraulichkeit und des Schutzes der Privatsphäre natürlicher Personen führen darf.

    Besondere Bedeutung gewinnen diese Verpflichtungen, wenn der Fernmeldeverkehr zwischen Teilnehmern in den Mitgliedstaaten über Drittländer geleitet wird oder geleitet werden kann, was insbesondere bei der Nutzung von Satelliten oder des Internet der Fall ist.

11. In den unter die Richtlinie 95/46/EG fallenden Bereichen könnte die Tatsache, daß der Fernmeldeverkehr über die Europäische Union hinausgehend zugänglich gemacht wird, einen Verstoß gegen Artikel 25 der Richtlinie darstellen, da die ausländischen Stellen, die diesen Verkehr überwachen, nicht zwangsläufig ein angemessenes Schutzniveau nachweisen können.

---

[17] 4.1. Die von Netzbetreibern oder Diensteanbietern erhobenen und verarbeiteten personenbezogenen Daten sollten nur weitergegeben werden, wenn der betroffende Teilnehmer nach vorheriger Aufklärung schriftlich sein ausdrückliches Einverständnis gegeben hat und die weitergegebene Information keinen Aufschluß über die angerufenen Teilnehmer zuläßt.
Der Teilnehmer kann sein Einverständnis jederzeit widerrufen, doch kann der Widerruf nicht rückwirkend sein.

4.2. Die von Netzbetreibern oder Diensteanbietern erhobenen und verarbeiteten personenbezogenen Daten können an staatliche Behörden weitergegeben werden, wenn diese Weitergabe gesetzlich vorgesehen ist und in einer demokratischen Gesellschaft erforderlich ist, um

a. die Sicherheit des Staates, die öffentliche Sicherheit oder die monetären Interessen des Staates zu schützen oder Straftaten zu verfolgen;
b. die betroffene Person sowie die Rechte und Freiheiten Dritter zu schützen.

4.3. Bei der Weitergabe personenbezogener Daten an staatliche Behörden sollten folgende Aspekte durch innerstaatliches Recht geregelt sein:

a. Ausübung des Rechts auf Zugang und Richtigstellung durch die betroffene Person;
b. Bedingungen, unter denen die zuständigen staatlichen Behörden berechtigt sind, der betroffenen Person die Auskunft zu verweigern oder die Erteilung der Auskunft hinauszuzögern;
c. Aufbewahrung oder Vernichtung dieser Daten."

[18] S. insbesondere die in Artikel 6 der Richtlinie 97/66/EG vorgesehenen Pflichten.
Diese Pflichten werfen Fragen hinsichtlich der Praktiken auf, die sich unter den Dienstleistungserbringern im Fernmeldewesen zur Zeit ausbreiten, d.h. eine allgemeine, vorherige Prüfung der Verkehrsdaten der Teilnehmer, um verdächtiges Verhalten bestimmter Teilnehmer aufzudecken - und gegebenenfalls die gezielte Überwachung des Inhalts bestimmter Verbindungen zu ermöglichen.

D. Wahrung der Grundfreiheiten bei der Überwachung durch staatliche Behörden

12. In den einzelstaatlichen Rechtsvorschriften muß unter Beachtung aller oben genannter Bestimmungen klar und umfassend sein,

- ✓ welche Dienststellen zur Anordnung der rechtmäßigen Überwachung des Fernmeldeverkehrs berechtigt sind und welche Stellen zur Durchführung der Überwachung befugt sind, sowie welche Rechtsgrundlage es dafür gibt,

- ✓ welche Zwecke mit einer solchen Überwachung verfolgt werden können, anhand deren beurteilt werden kann, ob die Maßnahme in einem angemessenen Verhältnis zu den zu schützenden nationalen Interessen steht,

- ✓ daß jede allgemeine oder sondierende Überwachung des Fernmeldeverkehrs im großen Maßstab verboten ist,

- ✓ welche genauen Umstände und Bedingungen bei der Überwachung gegeben sein müssen (z.B. Tatbestand, der die Maßnahme rechtfertigt, Dauer der Maßnahme), wobei nach dem Grundsatz zu verfahren ist, daß jedes Eindringen in die Privatsphäre eines anderen als Ausnahmefall anzusehen ist[19],

- ✓ daß die Achtung dieses Grundsatzes der Spezifizität als Folge des Verbots jeder allgemeinen oder sondierenden Überwachung insbesondere hinsichtlich der Verkehrsdaten impliziert, daß die staatlichen Behörden zu diesen Daten nur jeweils in Einzelfällen, nicht aber allgemein und proaktiv, Zugang haben.

- ✓ welche Sicherheitsvorkehrungen in bezug auf die Verarbeitung und die Speicherung der Daten getroffen wurden, sowie die Dauer ihrer Aufbewahrung,

- ✓ mit welchen besonderen Garantien personenbezogene Daten über Personen, die indirekt oder zufällig Gegenstand der Abhörung waren[20], verarbeitet werden können, insbesondere die Kriterien zur Rechtfertigung der Aufbewahrung der Daten und die Bedingungen für die Übermittlung dieser Daten an Dritte,

- ✓ wie die überwachte Person möglichst umgehend über die Überwachung zu unterrichten ist,[21]

---

[19] Siehe Fußnote 13.

[20] Die hier angesprochenen Daten beziehen sich auf Personen, die nicht Gegenstand von Überwachungsmaßnahmen sind, aber deren Korrespondent überwacht wird, wie z.B. die von der überwachten Person gewählte Nummer eines Verwandten oder die geographische Standortbestimmung von Personen, die über Mobilfunk Kontakt mit der überwachten Person hatten.

[21] Die überwachte Person sollte unterrichtet werden können, sobald die Information die Untersuchung nicht oder nicht mehr beeinträchtigt.

- ✓ welche Rechtsmittel der überwachten Person zur Verfügung stehen,[22]

- ✓ nach welchen Modalitäten diese Dienste durch eine unabhängige Aufsichtsbehörde kontrolliert werden[23],

- ✓ wie die tatsächlich praktizierte Politik der Überwachung des Fernmeldeverkehrs - bspw. in Form regelmäßiger statistischer Berichte - bekanntgegeben wird, [24]

- ✓ unter welchen konkreten Bedingungen die Daten im Rahmen bi- oder multilateraler Vereinbarungen an Dritte weitergegeben werden können.

Brüssel, den 3. Mai 1999

Für die Gruppe

Der Vorsitzende

Peter HUSTINX

[22] Das vorgenannte Urteil im Fall Leander weist darauf hin, daß die Instanz, bei der Rechtsmittel eingelegt werden können, nicht notwendigerweise eine richterliche Instanz stricto sensu zu sein hat, ihre Befugnisse und die Verfahrensgarantien jedoch zu berücksichtigen sind, um die Wirksamkeit der Rechtsmittel zu beurteilen. Unter diesen Rechtsmitteln sind im Hinblick auf die Beschränkungen, die jedem System geheimer Überwachung zum Schutz der Staatssicherheit innewohnen, möglichst effiziente Rechtsmittel zu verstehen - (§§ 83 und 84).

[23] Das Urteil im Fall Leander zielt auf die demokratische Kontrolle der Überwachungen ab, wenn es erläutert, daß das Parlament und unabhängige Einrichtungen [der Regierung] für das gute Funktionieren des Systems zu sorgen haben (§ 64).

[24] Diese Publizitätsanforderung sowie insbesondere die Notwendigkeit einer Kontrolle der Überwachungen durch eine unabhängige Behörde werden in der "Common position on public accountability in relation to interception of private communications" genannt, die die internationale Arbeitsgruppe über den Datenschutz im Telekommunikationsbereich am 15. April 1998 in Hong Kong angenommen hat.