5085/99/DE/ENDG
**WP 25**

**GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN**

# Empfehlung 3/99

**zur**

# Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke

Angenommen am 7. September 1999

**Empfehlung 3/99**

**zur**

**Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke**

## Einleitung

Die Bekämpfung der Computerkriminalität ist ein Thema, dem international immer größere Aufmerksamkeit zuteil wird[1]. Die G8-Länder[2] haben einen 10-Punkte-Aktionsplan verabschiedet[3], der gegenwärtig mit Unterstützung einer Fachgruppe für Hightech-Kriminalität umgesetzt wird, der Vertreter der Strafverfolgungsbehörden der G8-Staaten angehören. Eine der wichtigsten und brisantesten Fragen ist die Aufbewahrung von Verkehrsdaten (Daten über bereits abgeschlossene und gerade geschaltete Verbindungen) durch Internet-Dienstanbieter (Internet Service Provider) für Strafverfolgungszwecke und die Offenlegung dieser Daten gegenüber den Strafverfolgungsbehörden. Die G8-Arbeitsgruppe zur Hightech-Kriminalität beabsichtigt, Empfehlungen zur Aufbewahrung und Offenlegung von Verkehrsdaten abzugeben. Die G8-Justiz- und Innenminister werden diese Empfehlungen unter Umständen auf ihrem Treffen in Moskau am 19. und 20. Oktober 1999 erörtern.

Die Gruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten[4] ist sich der Tatsache bewußt, daß Verkehrsdaten eine wichtige Rolle bei der Ermittlung in Internet-Strafsachen spielen können, möchte die Regierungen der Mitgliedstaaten jedoch an die Grundsätze erinnern, wonach die Grundrechte und -freiheiten natürlicher Personen zu schützen sind, wobei in diesem Zusammenhang insbesondere die Achtung der Privatsphäre und das Brief-, Post- und Fernmeldegeheimnis zu berücksichtigen sind.

---

1 Siehe zum Beispiel „COMCRIME Study“ "Legal Aspects of computer-related Crime in the Information Society“ Januar 1997 - Erarbeitet im Rahmen des EU-Aktionsplans zur Bekämpfung der organisierten Kriminalität - Abrufbar auf der Website des Legal Advisory Board: http://www2.echo.lu/legal/en/comcrime/sieber.html. Der Europarat arbeitet gegenwärtig ein Übereinkommen über die Cyber-Kriminalität aus. Der Rat der Europäischen Union hat am 27. Mai 1999 seine Unterstützung für diese Arbeiten zugesichert. Computerkriminalität bezeichnet alle Straftaten, die über Netze verübt werden, wie z. B. mißbräuchliches Hacking, die Veröffentlichung illegalen Materials auf Websites und auch Delikte international aktiver krimineller Organisationen (z. B. Rauschgifthändler-, Kinderpornographieringe).

2 Die G8-Länder sind: Kanada, Frankreich, Deutschland, Italien, Japan, das Vereinigte Königreich, die Vereinigten Staaten von Amerika und Rußland.

3 „Meeting of Justice and Interior Ministers of the Eight December 9-10, 1997, Communiqué Washingtion D.C. December 10, Communiqué Annex: Priciples and Action Plan to Combat High-tech Crime“

4 Eingesetzt gemäß Artikel 29 der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates 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. Abrufbar unter: http://europa.eu.int/comm/dg15/de/media/dataprot/law/index.htm

Den Informationen der Gruppe zufolge sollen die G8-Justiz- und Innenminister aufgefordert werden, sich für eine ausgewogene Interpretation der beiden EU-Datenschutzrichtlinien[5] einzusetzen, die gegenwärtig umgesetzt werden, eine Auslegung, die Strafverfolgungsinteressen ebenso berücksichtigt wie den Grundsatz der Achtung der Privatsphäre.

Der Gruppe ist sich ferner der Belastung bewußt, die sich für Telekommunikationsbetreiber und -dienstanbieter ergeben kann.

Die vorliegende Empfehlung soll daher zu einer einheitlichen Anwendung der Richtlinien 95/46/EG und 97/66/EG beitragen, so daß klare und berechenbare Voraussetzungen für Telekommunikationsbetreiber, Internet-Dienstanbieter und Strafverfolgungsbehörden geschaffen werden und gleichzeitig die Achtung der Privatsphäre gewährleistet ist.

## Die Rechtslage

In der Europäischen Union werden durch die Richtlinie 95/46/EG die in den Rechtssystemen der Mitgliedstaaten verankerten Bestimmungen zum Schutz der Privatsphäre harmonisiert. Mit der Richtlinie werden die Grundsätze der Europäischen Konvention zum Schutz der Menschenrechte vom 4. November 1950 und das Übereinkommen des Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) vom 28. Januar 1981 konkretisiert und erweitert. Richtlinie 97/66/EG enthält analoge Vorschriften für den Bereich der Telekommunikation. Beide Richtlinien gelten für die Verarbeitung personenbezogener Daten, einschließlich Verkehrsdaten von Abonnenten und Nutzern, im Internet.[6]

Die Rechtmäßigkeit einer solchen Datenverarbeitung durch Telekommunikationsbetreiber und -dienstanbieter wird insbesondere in Artikel 6, 7, 13 sowie 17 Absätze 1 und 2 von Richtlinie 95/46/EG sowie Artikel 4, 5, 6 und 14 der Richtlinie 97/66/EG behandelt.

Diese Vorschriften erlauben es Telekombetreibern und -dienstanbietern, unter bestimmten, sehr eng gefaßten Voraussetzungen Daten über den Telekommunikationsverkehr zu verarbeiten.

Nach Artikel 6 Absatz 1 Buchstabe b) dürfen personenbezogene Daten nur für festgelegte eindeutige und rechtmäßige Zwecke erhoben und nicht in einer mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Artikel 6 Absatz 1 Buchstabe e) besagt, daß personenbezogene Daten nicht länger aufbewahrt werden dürfen, als es für die Realisierung der Zwecke, für die sie erhoben oder weiter verarbeitet werden, erforderlich ist. Artikel 13 räumt den Mitgliedstaaten die Möglichkeit ein, unter anderem die Pflichten und Rechte gemäß Artikel 6

[5] Richtlinie 95/46/EG, siehe Fußnote 3, und Richtlinie 97/66/EG des Europäischen Parlaments und des Rates 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. Abrufbar unter: siehe Fußnote 4.

[6] Siehe "Arbeitsunterlage: Die Verarbeitung personenbezogener Daten im Internet", angenommen am 23. Februar 1999, abrufbar unter: siehe Fußnote 1.

Absatz 1 einzuschränken, sofern eine solche Beschränkung für die Sicherheit des Staates, die öffentlichen Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig ist.

Die Anwendung dieser Grundsätze ist in Richtlinie 97/66/EG Artikel 5 und Artikel 6 Absätze 2 bis 5 näher ausgeführt. In Artikel 5 wird die **Vertraulichkeit der Kommunikation** sichergestellt, die über öffentliche Telekommunikationsnetze und öffentlich zugängliche Telekommunikationsdienste erfolgt. Die Mitgliedstaaten müssen das Mithören, Abhören und Speichern sowie die anderen Arten des Abfangens oder Überwachens von Kommunikationen durch andere Personen als die Benutzer untersagen, wenn keine Einwilligung der betroffenen Benutzer vorliegt, es sei denn, diese Personen sind gemäß Artikel 14 Absatz 1 gesetzlich dazu ermächtigt.

Generell müssen **Verkehrsdaten** unmittelbar nach Beendigung der Verbindung gelöscht oder anonymisiert werden (Artikel 6 Absatz 1 der Richtlinie 97/66/EG). Diese Vorschrift ist durch die Sensibilität von Verkehrsdaten begründet, die individuelle Kommunikationsprofile offenlegen, einschließlich Informationsquellen und Aufenthaltsort der Benutzer von Festnetz- oder Mobiltelefonen, sowie durch die potentielle Bedrohung der Privatsphäre durch das Sammeln, die Offenlegung oder die Weiterverwendung solcher Daten. Eine Ausnahme zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen sieht Artikel 6 Absatz 2 vor. Diese Verarbeitung ist jedoch nur bis zum Ablauf der Frist zulässig, innerhalb deren die Rechnung rechtlich angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann.

In Artikel 14 Absatz 1 wird den Mitgliedstaaten das Recht eingeräumt, die Pflichten und Rechte gemäß Artikel 6 zu beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die Sicherheit des Staates oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten notwendig ist.

Aus diesen Vorschriften ergibt sich, daß Telekommunikationsbetreiber und Internet-Dienstanbieter Verkehrsdaten nicht allein für Strafverfolgungszwecke sammeln und speichern dürfen, es sei denn, sie sind aus den oben aufgeführten Gründen und unter den oben aufgeführten Bedingungen gesetzlich dazu verpflichtet. Dies entspricht einer langen Tradition in der Mehrzahl der Mitgliedstaaten, in denen die nationalen Datenschutzgrundsätze es nicht zulassen, daß Privatunternehmen, personenbezogene Daten allein im Hinblick auf einen etwaigen künftigen Bedarf von Polizei und Sicherheitskräften speichern.

In diesem Zusammenhang sei angemerkt, daß die meisten Mitgliedstaaten über Rechtsvorschriften gemäß Artikel 13 der Richtlinie 95/46/EG und Artikel 14 der Richtlinie 97/66/EG verfügen, in denen genau festgelegt ist, unter welchen Voraussetzungen Polizei und Sicherheitskräfte zum Zwecke der Strafverfolgung auf Daten *zugreifen* dürfen, die private Telekommunikationsbetreiber und Internet-Dienstanbieter für ihre eigenen zivilen Zwecke gespeichert haben.

Wie die Gruppe bereits in ihrer Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs vom 3. Mai 1999[7] dargelegt hat, wird die Kenntnisnahme Dritter von Verkehrsdaten über die Nutzung von Telekommunikationsdiensten generell als Überwachung des Fernmeldeverkehrs betrachtet und stellt daher eine Verletzung des Rechtes des Einzelnen auf Achtung der

[7] Abrufbar unter: siehe Fußnote 1.

Privatsphäre und der Vertraulichkeit der Kommunikation gemäß Artikel 5 der Richtlinie 97/66/EG[8] dar. Darüber hinaus ist eine solche Offenlegung von Verkehrsdaten nicht mit Artikel 6 dieser Richtlinie vereinbar.

Verletzungen dieser Rechte und Pflichten können nicht hingenommen werden, es sei denn, es sind drei grundlegende Kriterien im Einklang mit Artikel 8 Absatz 2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten vom 4. November 1950 erfüllt, und zwar gemäß der Auslegung des Europäischen Gerichtshofs für Menschenrechte: 1. das Vorhandensein einer Rechtsgrundlage, 2. die Notwendigkeit der Maßnahme in einer demokratischen Gesellschaft und 3. die Übereinstimmung mit einem der in der Konvention aufgeführten legitimen Ziele. In der Rechtsgrundlage müssen die Grenzen und Mittel für die Maßnahme exakt festgelegt sein, d. h. es muß genau definiert sein, für welche Zwecke die Daten verarbeitet werden dürfen und über welchen Zeitraum sie (wenn überhaupt) aufbewahrt werden dürfen ; darüber hinaus muß der Zugriff auf die Daten streng begrenzt werden. Eine breit angelegte erkundende oder auch allgemeine Überwachung muß verboten sein[9]. Daraus folgt, daß Behörden nur nach Einzelfallprüfung Zugang zu Verkehrsdaten erhalten können und niemals generell oder vorbeugend.

Diese Kriterien stehen mit den obengenannten Bestimmungen von Artikel 13 der Richtlinie 95/46/EG und Artikel 14 der Richtlinie 97/66/EG in Einklang.

## Unterschiedliche einzelstaatliche Regelungen[10]

---

[8] Strafverfolgungsbehörden fordern ferner Zugang zu Echtzeit-Verbindungsinformationen, Daten über aktive Verbindungen (sogenannte „future traffic data“).

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

Im Klass-Urteil wird, ebenso wie im Leander-Urteil vom 25. Februar 1987, besonders hervorgehoben, daß angemessene und wirksame Garantien gegen Mißbrauch vorhanden sein müssen angesichts der Gefahr, daß ein System geheimer Überwachung zum Schutz der Sicherheit des Staates die Demokratie, die es schützen soll, aushöhlt oder sogar zerstört. (Leander-Urteil, Serie A Nr.. 116, S. 14ff).

Im Klass-Urteil (Absatz 50ff.) stellt der Gerichtshof fest, daß bei der Frage, ob angemessene und wirksame Garantien gegen Mißbrauch vorhanden sind, alle Umstände des Falles zu berücksichtigen sind. Im Fall Klass war der Gerichtshof der Auffassung, daß die gesetzliche Regelung in Deutschland, die Überwachungsmaßnahmen erlaubt, keine erkundende oder allgemeine Überwachung gestattet und nicht gegen Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte verstößt. Die deutsche Rechtsvorschrift sieht folgende Garantien vor: Die Überwachung ist auf Fälle begrenzt, in denen tatsächliche Anhaltspunkte für den Verdacht bestehen, daß jemand schwerwiegende Straftaten plant, begeht oder begangen hat; die Maßnahmen dürfen nur angeordnet werden, wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos oder wesentlich erschwert wäre. Selbst dann darf die Überwachung sich nur gegen den Verdächtigen selbst oder gegen seine mutmaßlichen Kontaktpersonen richten.

[10] Die Kommission prüft gegenwärtig die Vorschriften derjenigen Mitgliedstaaten, die Maßnahmen zur Umsetzung von Richtlinie 97/66/EG und Richtlinie 95/46/EG mitgeteilt haben. Siehe Umsetzungsübersicht zu Richtlinie 95/46/EG, abrufbar unter: siehe Fußnote 4.

Was den zulässigen Aufbewahrungszeitraum für Verkehrsdaten angeht, so erlaubt die Richtlinie 97/66/EG nur die Aufbewahrung für Abrechnungszwecke[11] und das nur bis zum Ablauf der Frist, innerhalb deren die Rechnung rechtlich angefochten werden kann. Dieser Zeitraum unterscheidet sich jedoch beträchtlich von Mitgliedstaat zu Mitgliedstaat. In Deutschland zum Beispiel dürfen Telekommunikationsbetreiber und -dienstanbieter die für die Gebührenabrechnung erforderlichen Daten bis zu 80 Tage speichern, um eine korrekte Abrechnung nachweisen zu können[12]. In Frankreich hängt der Zeitraum vom Status des Betreibers ab: Der „traditionelle" Telekommunikationsbetreiber darf Verkehrsdaten bis zu einem Jahr aufbewahren; dabei stützt man sich auf die gesetzliche Frist für die Anfechtung von Gebührenrechnungen. Für die anderen Betreiber ist diese Frist auf 10 Jahre festgesetzt. Das österreichische Telekommunikationsgesetz sieht keine festen Fristen für die Speicherung von Verkehrsdaten für Abrechnungszwecke vor, begrenzt diesen Aufbewahrungszeitraum jedoch auf die Frist, innerhalb deren die Rechnung angefochten oder der Anspruch auf Zahlung geltend gemacht werden kann. Im Vereinigten Königreich kann die Rechnung laut Gesetz 6 Jahre lang angefochten werden, Betreiber und Dienstanbieter speichern die entsprechenden Daten jedoch lediglich etwa 18 Monate. In Belgien ist eine solche Frist nicht gesetzlich festgeschrieben, der größte Telekommunikationsdienstanbieter hat die Frist in seinen allgemeinen Geschäftsbedingungen jedoch auf 3 Monate festgesetzt. In Portugal ist eine andere Vorgehensweise zu beobachten, hier ist die Frist nicht gesetzlich fixiert, sondern wird von der nationalen Datenschutzbehörde von Fall zu Fall festgesetzt. Erwähnenswert ist ferner, daß die Frist in Norwegen 14 Tage beträgt.

Auch die gegenwärtige Praxis der Internet-Dienstanbieter ist uneinheitlich: Kleine Dienstanbieter bewahren wegen mangelnder Speicherkapazität Verkehrsdaten offenbar nur für sehr kurze Zeiträume (wenige Stunden) auf. Größere Internet-Provider, die sich eine entsprechende Speicherkapazität leisten können, bewahren Verkehrsdaten unter Umständen mehrere Monate auf (dies kann jedoch von ihrem Abrechnungssystem - Berechnung de tatsächlichen Anschlußzeit oder Pauschale für eine bestimmte Anschlußdauer - abhängen).

Für Zwecke der Strafverfolgung verpflichtet das niederländische Telekommunikationsgesetz Telekommunikationsbetreiber und -dienstanbieter, Verkehrsdaten zu erheben und drei Monate aufzubewahren.

## Schranken für einen funktionierenden Binnenmarkt

Diese Unterschiede können die länderübergreifende Erbringung von Telekommunikations- und Internet-Diensten im Binnenmarkt behindern; ferner können so unterschiedliche Fristen die Wirksamkeit der Strafverfolgung beeinträchtigen. Man könnte geltend machen, daß ein in einem Mitgliedstaat

[11] Und soweit erforderlich für die Bezahlung von Zusammenschaltungen zwischen Telekommunikationsbetreibern, siehe Artikel 6 Absatz 2 der Richtlinie 97/66/EG.

[12] Wird die Rechnung innerhalb dieses Zeitraums angefochten, dürfen die entsprechenden Daten selbstverständlich aufbewahrt werden, bis der Streit beigelegt ist.

ansässiger Internet-Dienstanbieter Verkehrsdaten nur so lange speichern darf, wie es in dem Mitgliedstaat zulässig ist, in dem der Kunde lebt und den Dienst in Anspruch nimmt. Ferner ist es denkbar, daß ein Internet-Dienstanbieter dazu gedrängt wird, Verkehrsdaten länger aufzubewahren, als es in seinem eigenen Mitgliedstaat zulässig ist, weil die Länder, in denen die Nutzer ansässig sind, dies so verlangen. Bei der Gebührenabrechnung für das Roaming in der Mobiltelefonie rechnet nicht der ausländische Betreiber ab, sondern der Betreiber des Landes, in dem der Teilnehmer sein Abonnement hat. Unterschiedliche Aufbewahrungsfristen für die Daten, die für die Gebührenabrechnung benötigt werden, können mithin zu den gleichen Problemen führen wie bei den Internet-Dienstanbietern. Die in Artikel 4 der Richtlinie 95/46/EG festgeschriebene Anwendung des einzelstaatlichen Rechts löst dieses Problem nur dann, wenn der Internet-Dienstanbieter für die Verarbeitung verantwortlich ist und nur in einem Mitgliedstaat einen Sitz hat, nicht jedoch in den Fällen, in denen er in mehreren Mitgliedstaaten, für die jeweils unterschiedliche Fristen gelten, einen Sitz hat oder wenn er die Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet.

## Empfehlung

Aufgrund der dargelegten Sachverhalte ist die Gruppe der Auffassung, daß, will man eine unannehmbare Bedrohung der Privatsphäre vermeiden und gleichzeitig den Erfordernissen einer effizienten Strafverfolgung Rechnung tragen, das wirksamste Vorgehen darin besteht, grundsätzlich nicht zuzulassen, daß Verkehrsdaten allein für Strafverfolgungszwecke aufbewahrt werden; ferner sollten die einzelstaatlichen Rechtsvorschriften Telekommunikationsbetreiber, Telekommunikationsdienstanbieter und Internet-Dienstanbieter nicht dazu verpflichten, Verkehrsdaten länger aufzubewahren, als sie sie für die Gebührenabrechnung benötigen.

Die Gruppe empfiehlt der Europäischen Kommission, Maßnahmen für eine weitere Harmonisierung der Fristen vorzuschlagen, innerhalb deren Telekommunikationsbetreiber, Telekommunikationsdienstanbieter und Internet-Dienstanbieter Verkehrsdaten zum Zwecke der Gebührenabrechnung und der Bezahlung von Zusammenschaltungen aufbewahren dürfen[13]. Die Gruppe ist der Auffassung, daß diese Frist so lang sein sollte, wie es nötig ist, damit der Verbraucher die Rechnung anfechten kann, jedoch gleichzeitig so kurz wie möglich, damit Betreiber und Dienstanbieter nicht über Gebühr belastet und Verhältnismäßigkeit und Zweckgebundenheit als Teil des Rechts auf Achtung der Privatsphäre gewährleistet sind. Die Frist sollte am höchsten Schutzniveau ausgerichtet werden, das in der Union zu finden ist. Die Gruppe weist darauf hin, daß in einer Reihe von Mitgliedstaaten Fristen von maximal 3 Monaten erfolgreich angewandt worden sind.

Die Gruppe empfiehlt ferner den Regierungen der Mitgliedstaaten, diese Erwägungen zu berücksichtigen.

---

[13] Angesichts dieser Zweckbestimmung ist eine Unterscheidung zwischen privaten und öffentlichen Betreibern nicht gerechtfertigt.

Geschehen zu Brüssel am
7. September 1999

Für die Gruppe

*Der Vorsitzende*

Peter HUSTINX