11885/04/DE
WP 99

Stellungnahme 9/2004 zum Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus [Vorschlag Frankreichs, Irlands, Schwedens und Großbritanniens (Ratsdokument 8958/04 v. 28.4.2004)]

angenommen am 9. November 2004

DIE GRUPPE FÜR DEN SCHUTZ NATÜRLICHER 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 sowie auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie, ferner auf Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.Juli 2002,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14 -

hat folgende Stellungnahme angenommen:

In den letzten Jahren hat die Datenschutzgruppe sich wiederholt zur Speicherung von Telekommunikationsverkehrsdaten[2] geäußert, und die Konferenz der europäischen Datenschutzbeauftragten hat mehrere gemeinsame Erklärungen zu diesem Thema abgegeben[3]. Der Vorschlag für einen Rahmenbeschluss über die Vorratsspeicherung solcher Verkehrsdaten, den vier Mitgliedstaaten dem Rat der Europäischen Union vorgelegt haben, erfordert erneut eine Stellungnahme der Datenschutzgruppe. Da sich die Erörterungen in der zuständigen Arbeitsgruppe des Rates noch im Anfangsstadium befinden, hat diese Stellungnahme vorläufigen Charakter. Die Datenschutzgruppe hat die Absicht, die Frage zu einem späteren Zeitpunkt auf der Grundlage eines überarbeiteten Entwurfes erneut zu prüfen.

Die Datenschutzgruppe hat den Entwurf auf seine Vereinbarkeit mit Artikel 8 der Europäischen Menschenrechtskonvention hin geprüft.

In diesem Zusammenhang muss berücksichtigt werden, dass die Bürger für alltägliche Tätigkeiten zunehmend elektronische Kommunikationsnetze und –dienste nutzen. Die bei dieser Form der Kommunikation generierten Daten, die so genannten „Verkehrsdaten“, können Informationen über Ort, Zeitpunkt und Gesprächspartner von Mobil- oder Festnetztelefongesprächen, Telefaxkommunikation, E-Mails, SMS und anderen Formen der Internetkommunikation enthalten und daher in zunehmendem Maße die Lebensführung der Nutzer widerspiegeln.

---

1 Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/law/index.htm

2 Siehe: Empfehlung 3/97 über Anonymität im Internet; Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs; Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke; Stellungnahme 7/2000 zum Vorschlag der Europäischen Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation vom 12. Juli 2000, KOM(2000) 385; Stellungnahme 4/2001 zum Entwurf einer Konvention des Europarates über Cyberkriminalität; Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus; Stellungnahme 5/2002 zur Erklärung der europäischen Datenschutzbeauftragten auf der Internationalen Konferenz in Cardiff (9.-11. September 2002) zur obligatorischen systematischen Aufbewahrung von Verkehrsdaten im Bereich der Telekommunikation; Stellungnahme1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung. Der Anhang dieser Stellungnahme enthält eine Zusammenfassung dieser Papiere. Außerdem sind alle Unterlagen abrufbar unter http://europa.eu.int/comm/internal_market/privacy.

3 Siehe in Stockholm (April 2000) und Cardiff (2002) angenommene Erklärungen.

In ihrer *Empfehlung 2/99 vom 3. Mai 1999 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs* definierte die Datenschutzgruppe die Überwachung des Fernmeldeverkehrs als die 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. In diesem Zusammenhang stellte die Datenschutzgruppe seinerzeit auch fest, dass jede Überwachung des Fernmeldeverkehrs (einschließlich der Überwachung und des Data Mining von Verkehrsdaten) eine Verletzung des Rechts von Einzelpersonen auf Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstelle. Daraus folgt, dass Überwachungen abzulehnen sind, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention durch den Europäischen Gerichtshof für Menschenrechte ergeben: Sie müssen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen.

Nach Auffassung der Datenschutzgruppe gelten dieselben grundlegenden Erfordernisse für die Speicherung von Verkehrsdaten, soweit sie über das für die Erbringung der Kommunikationsdienstleistungen und andere legitime Geschäftszwecke Notwendige hinausgehen, sowie für jeden anschließenden Zugriff auf diese Daten für Strafverfolgungszwecke[4].

Die Datenschutzgruppe bezweifelt ernsthaft, dass der Beschlussentwurf diese Grundanforderungen erfüllt. Was das erste Erfordernis (gesetzliche Grundlage) betrifft, so hält sie es nicht für sinnvoll, zum jetzigen Zeitpunkt darauf einzugehen, da sich die Diskussionen im Rat noch in einem sehr frühen Stadium befinden. Mit Blick auf das dritte Erfordernis (notwendig zum Schutz legitimer, in der Konvention aufgeführter Interessen) stellt die Datenschutzgruppe das eigentliche Ziel des Entwurfs in Frage. Soll er wirklich nur wie angegeben (Erwägungsgrund 7) der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten dienen, und sind andere Ziele des Artikels 8 ausgeschlossen? Das Ziel muss zuallererst klar sein.

---

[4] Diese Sichtweise wird von der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte gestützt. Dieser hat beispielsweise in seinem Amann-Urteil (S. 30 ff.) festgestellt, dass bereits die Speicherung von Informationen einen Grundrechtseingriff darstelle, unabhängig davon, ob diese Daten gegen die betroffene Person verwendet werden oder nicht. Auch im Rotaru-Urteil hat er die Speicherung historischer Daten durch den Geheimdienst als Eingriff in die Grundrechte eingestuft. Im Urteil PG gegen UK (S. 42 ff.) hat der Gerichtshof die Auffassung vertreten, die Erfassung des Fernmeldeverkehrs verstoße nicht per se gegen Artikel 8, beispielsweise dann nicht, wenn sie durch die Telefongesellschaft für Abrechnungszwecke vorgenommen werde. Hingegen stelle der Zugriff der Polizei auf Informationen des Providers über angerufene Nummern einen Eingriff in die Privatsphäre oder das Fernmeldegeheimnis dar. Im Fall Malone (S. 84 ff.) vertrat der Gerichtshof ebenfalls die Auffassung, dass die Weitergabe solcher Daten von der Telefongesellschaft an die Polizei einen Eingriff in das Recht auf Schutz der „Korrespondenz“ nach Artikel 8 darstelle. Aus diesen Fällen könnte man ableiten, dass die Verpflichtung der Telekom-Gesellschaften zur Speicherung von Verkehrsdaten als solche nicht gegen Artikel 8 verstößt, die Weiterverarbeitung dieser Daten oder ihre Weitergabe an die Behörden indessen sehr wohl im Widerspruch dazu steht. Diese Schlussfolgerung wäre falsch. In der Sache MM. gegen Niederlande stellte der Gerichtshof fest, dass die Behörden die Haftbarkeit nicht umgehen können, indem sie Privatpersonen einsetzen, wenn sie einen wesentlichen Beitrag zur Ausführung der Überwachung leisten. Dies würde mithin bedeuten, dass beispielsweise Datenspeicherung und Data Mining für die Zwecke der öffentlichen Ordnung durch die Telekom-Gesellschaften in ihren eigenen Systemen ebenfalls einen Eingriff in die Grundrechte darstellen.

Zum zweiten Kriterium (in einer demokratischen Gesellschaft notwendig) ist zu sagen, dass die Speicherung gemäß der Auslegung des EGMR einem zwingenden gesellschaftlichen Bedarf („pressing social need“) entspringen muss (siehe unter anderem Urteil in der Sache Klass gegen Bundesrepublik Deutschland vom 18 November 1977, Europäischer Gerichtshof für Menschenrechte, Reihe A, Nr. 28). Der Gerichtshof für Menschenrechte hat zwar die Befugnis der Vertragsstaaten anerkannt, in Ausnahmefällen und unter besonderen Umständen die Korrespondenz und Telekommunikation von Personen auch heimlich zu überwachen. Er hat aber hinzugefügt:

„… dies bedeutet nicht, dass die Vertragsstaaten ein unbeschränktes Ermessen haben, Personen in ihrem Hoheitsgebiet einer heimlichen Überwachung zu unterwerfen. Angesichts der Tatsache, dass entsprechende Befugnisse mit der Begründung, die Demokratie verteidigen zu wollen, diese gerade zu unterminieren oder zu zerstören drohen, betont der Gerichtshof, dass die Vertragsstaaten zur Bekämpfung der Spionage oder des Terrorismus nicht jede Maßnahme beschließen dürfen, die sie für angemessen halten“ (Klass, S. 3).

Die im Beschlussvorschlag vorgesehene Verpflichtung zur routinemäßigen, flächendeckenden Vorratsspeicherung sämtlicher Verkehrs-, Nutzer- und Teilnehmerdaten würde die ausnahmsweise zulässige Überwachung zur evident unverhältnismäßigen Regel machen. Der vorgeschlagene Beschluss wäre nicht nur auf einzelne Personen anwendbar, die auf Grund besonderer Gesetze überwacht würden, sondern auf alle Personen, die die elektronische Kommunikation nutzen. Ferner würden alle versandten oder empfangenen Mitteilungen erfasst. Nicht alles, was sich für die Strafverfolgung als nützlich erweisen könnte, ist wünschenswert oder kann als in einer demokratischen Gesellschaft notwendig angesehen werden, zumal wenn es zu einer systematischen Registrierung der gesamten elektronischen Kommunikation führt. Dass eine so umfängliche Speicherung von Verkehrsdaten der einzig gangbare Weg zur Bekämpfung der Kriminalität oder zur Wahrung der nationalen Sicherheit ist, dafür liefert der Rahmenbeschluss keinerlei überzeugenden Argumente. Mit der Verpflichtung der Provider zur Speicherung von Verkehrsdaten, die sie nicht für eigene Zwecke benötigen, würde der Grundsatz der Zweckbindung in beispielloser Weise durchbrochen.

Untersuchungen europäischer Telefongesellschaften haben gezeigt, dass das Gros der von Strafverfolgungsbehörden abgerufenen Daten nicht älter als sechs Monate war. Das belegt, dass längere Aufbewahrungsfristen eindeutig unverhältnismäßig sind.

Es soll darauf hingewiesen werden, dass die Vertreter der Strafverfolgungsbehörden bisher jeglichen Nachweis für die Notwendigkeit so weit reichender Maßnahmen schuldig geblieben sind. Es fällt auf, dass sie bei den in jüngster Zeit veranstalteten Workshops, bei denen Hintergrund und Folgen des Beschlussentwurfes beleuchtet werden sollten, ausnahmslos durch Abwesenheit geglänzt haben.

Die Konvention zur Bekämpfung der Datennetzkriminalität (Cybercrime-Konvention) sieht nur eine einzelfallbezogene Sicherungsspeicherung nach dem Modell des „fast freeze – quick thaw“ vor, das entgegen der Auffassung der vier Regierungen, die den Rahmenbeschluss vorschlagen, durchaus geeignet ist, Straftaten zu verhüten oder sie zu verfolgen. Es ist bezeichnend für die gegenwärtige rechtspolitische Diskussion, dass der jetzt gemachte Vorschlag ernsthaft erörtert wird, noch bevor die Cybercrime-Konvention in den meisten Unterzeichnerstaaten in Kraft getreten ist und in ihren praktischen Auswirkungen bewertet werden kann. Die Artikel-29-Gruppe hat bereits in ihrer

Stellungnahme 5/2002 festgestellt, dass bei der Aufbewahrung von Verkehrsdaten für Zwecke der Strafverfolgung die Bedingungen des Artikels 15 Absatz 1 der Richtlinie 2002/58/EG strikt einzuhalten sind, d.h. in jedem Einzelfall ist die Aufbewahrung nur während einer begrenzten Zeit und nur wenn dies in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist, zulässig. Auch die europäischen Datenschutzbeauftragten haben sich auf ihrer Internationalen Konferenz in Cardiff (9.-11. September 2002) zur zwangsweisen systematischen Speicherung von Verkehrsdaten der Telekommunikation geäußert. Sie erklärten, dass die systematische Speicherung aller Verkehrsdaten für die Dauer von einem Jahr oder länger eindeutig unverhältnismäßig und deshalb abzulehnen wäre.

Der Entwurf des Rahmenbeschlusses wird diesen Anforderungen nicht nur nicht gerecht, es wird damit versucht, sie explizit außer Kraft zu setzen, indem kein konkreter Tatverdacht und keine hinreichend sichere Tatsachenbasis im Einzelfall gefordert werden, sondern die Vorratsspeicherung pauschal und präventiv für eine mögliche zukünftige Strafverfolgung zulasten aller, die elektronische Kommunikationsnetze nutzen, angeordnet werden soll.

Die Datenschutzgruppe hält die Pflichtspeicherung aller Arten von Verkehrsdaten der Telekommunikation für Zwecke der öffentlichen Ordnung unter den im Beschlussentwurf vorgesehenen Bedingungen für eindeutig unverhältnismäßig und deshalb für unzulässig nach Artikel 8 der Menschenrechtskonvention.

Geschehen zu Brüssel am 9. November 2004

Für die Datenschutzgruppe

Der Vorsitzende

Peter Schaar

ANHANG

Zusammenfassung der Erklärungen der Artikel-29-Datenschutzgruppe zur Speicherung von Telekommunikationsverkehrsdaten

EMPFEHLUNG 3/97 ZUR ANONYMITÄT IM INTERNET

In Empfehlung 3/97 über Anonymität im Internet hat die Artikel-29-Datenschutzgruppe erklärt, dass, auch wenn Verkehrsdaten in einigen Rechtsordnungen in gewissem Umfang durch das Brief- und Fernmeldegeheimnis geschützt sind, die massive Zunahme solcher Daten Anlass zu berechtigter Sorge gibt. In dem Maße wie Onlinedienste leistungsfähiger und beliebter werden, wird sich auch das Problem der Transaktionsdaten ausweiten. Wenn immer mehr Alltagstätigkeiten online abgewickelt werden, wird immer mehr von dem, was wir tun, erfasst.

Allein durch ihr Vorhandensein schaffen identifizierbare Transaktionsdaten ein Instrument, mit dem das Verhalten des Einzelnen mit beispielloser Intensität überwacht und kontrolliert werden kann. Nach Auffassung der Datenschutzgruppe sollten Regierungen und Behörden im Internet nicht mehr Möglichkeiten zur Einschränkung der Rechte des Einzelnen und zur Überwachung potenziell rechtswidrigen Verhaltens haben als in der Offline-Welt.

EMPFEHLUNG 2/99 ZUR ACHTUNG DER PRIVATSPHÄRE BEI DER ÜBERWACHUNG DES FERNMELDEVERKEHRS, ANGENOMMEN AM 3. MAI 1999

In ihrer Empfehlung 2/99 zur Achtung der Privatsphäre bei der Überwachung des Fernmeldeverkehrs (einschließlich Monitoring und Data Mining von Verkehrsdaten) vom 3. Mai 1999 hat die Datenschutzgruppe sich mit dem Verhältnis von Fernmeldeüberwachung und Grundrechten auseinandergesetzt. Dabei hat sie die Überwachung des Fernmeldeverkehrs definiert als die 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. Sie hat betont, dass jede Überwachung des Fernmeldeverkehrs eine Verletzung des Rechts von Einzelpersonen auf Schutz der Privatsphäre und eine Verletzung des Brief- und Fernmeldegeheimnisses darstellt. Aus diesem Grund sind Überwachungen abzulehnen, sofern sie nicht drei grundlegende Kriterien erfüllen, die sich aus der Auslegung von Artikel 8 Absatz 2 der Europäischen Menschenrechtskonvention durch den Europäischen Gerichtshof für Menschenrechte ergeben: Sie müssen gesetzlich vorgesehen und in einer demokratischen Gesellschaft notwendig sein und einem der in der Konvention aufgeführten legitimen Ziele dienen.

In diesem rechtlichen Kontext müssen breit angelegte erkundende oder allgemeine Überwachungen verboten sein. Die Datenschutzgruppe verweist insbesondere auf die Fälle Leander und Klass, in denen der Gerichtshof festgestellt hatte, dass ausreichende Garantien benötigt würden, 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. Im Urteil Klass kam der Gerichtshof zu dem Schluss, dass die einschlägigen deutschen Rechtsvorschriften nicht gegen Artikel 8 der Europäischen

Menschenrechtskonvention verstießen, da sie nur eine Überwachung bestimmter verdächtiger Personen oder deren mutmaßlicher Kontaktpersonen zuließen. Die Datenschutzgruppe führt in dieser Empfehlung (Ziff. 9) die Anforderungen auf, die einzelstaatliche Rechtsvorschriften über Telefonüberwachungen erfüllen müssen.

EMPFEHLUNG 3/99 ZUR AUFBEWAHRUNG VON VERKEHRSDATEN DURCH INTERNET-DIENSTANBIETER FÜR STRAFVERFOLGUNGSZWECKE, ANGENOMMEN AM 7. SEPTEMBER 1999

Die Pflicht zur Löschung oder Anonymisierung von Verkehrsdaten ist durch die Sensibilität dieser Daten begründet, die individuelle Kommunikationsprofile offen legen, einschließlich Informationsquellen und Aufenthaltsorten der Benutzer von Festnetz- oder Mobiltelefonen, sowie durch die potenzielle Bedrohung der Privatsphäre durch das Sammeln, die Offenlegung oder die Weiterverwendung solcher Daten.

Die Datenschutzgruppe merkt an, dass die gesetzlich zulässigen Speicherzeiträume von Mitgliedstaat zu Mitgliedstaat sehr unterschiedlich sind. Sie empfiehlt, nicht zuzulassen, dass Verkehrsdaten allein für Strafverfolgungszwecke aufgehoben werden, und die Dienstanbieter nicht zu verpflichten, die Daten länger aufzubewahren, als es für Abrechnungszwecke notwendig ist, und spricht sich für eine weitere Harmonisierung des Aufbewahrungszeitraums in der EU aus.

STELLUNGNAHME 7/2000 ZUM VORSCHLAG DER EUROPÄISCHEN KOMMISSION FÜR EINE RICHTLINIE DES EUROPÄISCHEN PARLAMENTS UND DES RATES ÜBER DIE VERARBEITUNG PERSONENBEZOGENER DATEN UND DEN SCHUTZ DER PRIVATSPHÄRE IN DER ELEKTRONISCHEN KOMMUNIKATION VOM 12. JULI 2000 - KOM (2000) 385, ANGENOMMEN AM 2. NOVEMBER 2000

Verkehrsdaten wie zum Beispiel URLs können Aufschluss über persönliche Interessen geben (unter anderem durch Hinweise auf religiöse Überzeugung, politische Meinung, Gesundheit oder Sexualleben). Diese Daten sollten mit der für die Kommunikation geltenden Vertraulichkeit behandelt werden.

Ein weiterer, noch zu erörternder Aspekt, der von der Datenschutzgruppe angesprochen wird, ist, dass einige dieser Daten auch als sensible Daten im Sinne des Artikels 8 der allgemeinen Datenschutzrichtlinie 95/46/EG angesehen werden könnten, die prinzipiell nicht verarbeitet werden dürfen.

Angesichts der weitgefassten Definition der Verkehrsdaten vertritt die Gruppe die Auffassung, dass es nicht unbedingt akzeptabel ist, wenn alle Verkehrsdaten auf die gleiche Weise behandelt werden. Einige Arten von Verkehrsdaten benötigen unter Umständen mehr Schutz als andere.

STELLUNGNAHME 4/2001 ZUM ENTWURF EINER KONVENTION DES EUROPARATES ÜBER CYBERKRIMINALITÄT, ANGENOMMEN AM 22. MÄRZ 2001

Wenn das Verfahrensrecht harmonisiert wird, muss auch die Angleichung der Garantien und Voraussetzungen für die darauf gestützten Maßnahmen in Betracht gezogen werden. Auch in diesem Zusammenhang hat die Datenschutzgruppe betont, dass eine allgemeine Überwachungspflicht in Form der routinemäßigen Speicherung von Verkehrsdaten, wie sie ursprünglich in der Cybercrime-Konvention (Version 25) vorgeschlagen worden war, einen unzulässigen Eingriff in die in Artikel 8 der Europäischen Menschenrechtskonvention garantierten Grundrechte darstellen würde.

Außerdem wäre denkbar, dass die Wirtschaft mehr Rechtssicherheit benötigt wenn es darum geht, wem wann Zugang zu vertraulichen Informationen und vertraulicher Kommunikation zu gewähren ist.

STELLUNGNAHME 10/2001 ZUR NOTWENDIGKEIT EINES AUSGEWOGENEN VORGEHENS IM KAMPF GEGEN DEN TERRORISMUS

In *der am 14. Dezember 2001 angenommenen Stellungnahme 10/2001 zur Notwendigkeit eines ausgewogenen Vorgehens im Kampf gegen den Terrorismus* erklärt die Datenschutzgruppe, die Bekämpfung des Terrorismus sei ein notwendiges und gültiges Anliegen einer demokratischen Gesellschaft. Aber bei diesem Kampf müssten bestimmte Bedingungen beachtet werden, die ebenfalls elementarer Bestandteil unserer demokratischen Gemeinwesen sind. Die Datenschutzgruppe ist sich der Ernsthaftigkeit des Terrorismusproblems durchaus bewusst - eines Phänomens, mit dem Europa schon geraume Zeit konfrontiert ist. Sie hält indessen langfristige Überlegungen für erforderlich über Maßnahmen, die lediglich nur „nützlich“ oder „wünschenswert“ sind, wie beispielsweise die flächendeckende anlassunabhängige Vorratsspeicherung von Telekommunikationsdaten. Die Maßnahmen dürfen Grundrechte und Grundfreiheiten nicht einschränken. Ein wichtiges Element des Kampfes gegen den Terrorismus ist, dass wir die grundlegenden Werte bewahren, auf denen unsere Demokratien basieren, denn genau diese Werte wollen diejenigen zerstören, die den Einsatz von Gewalt propagieren.

STELLUNGNAHME 5/2002 ZUR ERKLÄRUNG DER EUROPÄISCHEN DATENSCHUTZBEAUFTRAGTEN AUF DER INTERNATIONALEN KONFERENZ IN CARDIFF (9.-11. SEPTEMBER 2002) ZUR OBLIGATORISCHEN SYSTEMATISCHEN AUFBEWAHRUNG VON VERKEHRSDATEN IM BEREICH DER TELEKOMMUNIKATION, ANGENOMMEN AM 11. OKTOBER 2002

Die Datenschutzgruppe hat die Berechtigung und die Rechtmäßigkeit der zwangsweisen systematischen Speicherung von Verkehrsdaten, um einen möglichen Zugang durch Strafverfolgungs- und Sicherheitsorgane zu gestatten, ernsthaft in Zweifel gezogen.

Eine lange und harte Auseinandersetzung über die Regelung dieser Frage in Richtlinie 2002/58/EG führte zur Festlegung strenger Voraussetzungen für die Speicherung von Verkehrsdaten für Strafverfolgungszwecke in Artikel 15 Absatz 1 der Richtlinie; danach sollte die Speicherung in jedem Fall nur befristet erfolgen dürfen und nur, wenn es in einer demokratischen Gesellschaft angemessen und verhältnismäßig ist. Die Datenschutzgruppe stellt fest, dass die systematische Speicherung aller Verkehrsdaten für die Dauer von einem Jahr oder länger eindeutig unverhältnismäßig und deshalb abzulehnen wäre.

Außerdem erklärte sie, sie erwarte vor der Verabschiedung von Maßnahmen, die sich in Bereichen ergeben könnten, die unter die dritte Säule fallen, gehört zu werden.

STELLUNGNAHME 1/2003 ZUR SPEICHERUNG VON VERKEHRSDATEN ZU ZWECKEN DER GEBÜHRENABRECHNUNG, ANGENOMMEN AM 29. JANUAR 2003

In *der am 20. Januar 2003 angenommenen Stellungnahme 1/2003 zur Speicherung von Verkehrsdaten zu Zwecken der Gebührenabrechnung* gibt die Datenschutzgruppe Orientierungshilfe für die Harmonisierung des Zeitraums, in dem die Verwendung von Verkehrsdaten für Abrechnungszwecke gesetzlich zulässig ist. Für Abrechnungszwecke sollten die Daten normalerweise nicht länger als drei bis sechs Monate gespeichert

werden. Verarbeitet werden dürfen nur solche Verkehrsdaten, die dem Zweck angemessen und dafür relevant sind und nicht über das Notwendige hinausgehen. Andere Verkehrsdaten müssen gelöscht oder anonymisiert werden.

Vorgehensweisen, die nicht mit diesen Grundsätzen übereinstimmen, und Praktiken, die nicht eindeutig gemäß Artikel 15 der Richtlinie 2002/58/EG gesetzlich zugelassen sind, sind prima facie mit den Anforderungen der Datenschutzrichtlinie unvereinbar.