



**5042/00/DE/ENDGÜLTIG
WP36**

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

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

Die Gruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist das unabhängige Beratungsgremium der EU in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt. Die Sekretariatsgeschäfte werden wahrgenommen von:

Europäische Kommission, GD Binnenmarkt, Referat Freier Verkehr von Informationen, Datenschutz,
Rue de la Loi 200, B-1049 Brüssel/Wetstraat 200, B-1049 Brüssel - Belgien - Büro: C100-2/133
Internetadresse: www.europa.eu.int/comm/internal_market/de/media/dataprot/index.htm

**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 1995¹,

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a und Absatz 3 der Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12, 13 und 14,

hat folgende Stellungnahme 7/2000 angenommen:

1. Einführung

Im Rahmen der 1999 durchgeführten Überprüfung der Rechtsvorschriften der Gemeinschaft zur Telekommunikation² hat die Kommission am 12. Juli 2000 Entwürfe zu neuen Richtlinien über die elektronische Kommunikation angenommen, die die bestehenden Rechtsvorschriften ersetzen sollen. Einer der fünf Entwürfe betrifft die Neufassung der 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.

Anknüpfend an ihre Stellungnahme 2/2000 zu der allgemeinen Überprüfung der Rechtsvorschriften im Bereich Telekommunikation³ möchte sich die Gruppe⁴ nunmehr an den Diskussionen über den Richtlinienentwurf im europäischen Parlament und im Rat beteiligen.

2. Analyse des Richtlinienentwurfs

Die Hauptanliegen der Gruppe sind die Verarbeitung personenbezogener Daten über und durch das Internet, die genauer untersucht werden muss, sowie Fragen, die sich aus dem liberalisierten Telekommunikationsmarkt ergeben.

¹ Amtsblatt L 281 vom 23.11.1995, S. 31, verfügbar unter der Adresse:
<http://europa.eu.int/comm/dg15/en/media/dataprot/index.htm>

² Die Überprüfung von 1999 wurde im November 1999 durch eine Mitteilung der Kommission eingeleitet, an die sich eine breite öffentliche Konsultation anschloss. Die Ergebnisse dieser Konsultation wurden in einer zweiten Mitteilung zusammengefasst, die die Kommission am 26. April annahm. Alle Dokumente zu der Überprüfung und die Richtlinienentwürfe liegen unter folgender Adresse vor:
<http://www.ispo.cec.be/infosoc/telecompolicy/review99/Welcome.html>.

³ Alle von der Gruppe angenommenen Dokumente sind unter folgender Adresse abrufbar:
http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

⁴ Eingesetzt durch 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. L281, 23. November 1995, S. 31, abrufbar unter:
<http://europa.eu.int/comm/dg15/en/media/dataprot/law/index.htm>

Artikel 1 - Geltungsbereich und Zielsetzung und Artikel 3 - Betroffene Dienste

Die Gruppe entnimmt den Unterlagen, dass die Artikel "Geltungsbereich" und "Betroffene Dienste" unverändert bleiben. Die spezifischen Bestimmungen der neuen Richtlinie würden demnach auf die Erbringung *öffentlich* zugänglicher elektronischer Kommunikationsdienste in *öffentlichen* Kommunikationsnetzen in der Gemeinschaft angewandt. Die Verarbeitung personenbezogener Daten für die Zwecke geschlossener/privater Netze würde somit ausschließlich unter die allgemeine Richtlinie 95/46/EG fallen. Dies ist bedauerlich, weil private Netze im Alltag und für die Kommunikation der Bürger zunehmend an Bedeutung gewinnen, beispielsweise im Rahmen ihrer Berufstätigkeit, und weil die Risiken, die diese Netze im Hinblick auf die Privatsphäre mit sich bringen, dementsprechend zunehmen und konkreter werden (z. B. Überwachung des Verhaltens von Arbeitnehmern mit Hilfe von Verkehrsdaten, mangelnde Vertraulichkeit der Kommunikation).

Die Verarbeitung personenbezogener Daten im Zusammenhang mit der Erbringung von *Dienstleistungen* über öffentliche Kommunikationsdienste und -netze⁵, beispielsweise die Inhalte von Rundfunk-/Fernsehübertragungen und von Dienstleistungen der Informationsgesellschaft, wird in dem neuen Richtlinienentwurf ebenfalls nicht berücksichtigt. Damit fällt die Verarbeitung von Daten in letzterem Fall lediglich unter die Richtlinie 95/46/EG, wie alles, was nicht von der spezifischen Richtlinie über den Schutz der Privatsphäre erfasst wird (siehe Erwägungsgrund 9, der mit dem entsprechenden Erwägungsgrund der zur Zeit gültigen Richtlinie 97/66/EG identisch ist).

Interaktive Fernsehübertragungsdienste würden jedoch unter die Richtlinie fallen.⁶

Diese Punkte könnten sinnvollerweise in den einschlägigen Artikeln der einzelnen Richtlinien oder in den Erwägungsgründen geklärt werden.

Artikel 2 - Begriffsbestimmungen

Die Gruppe begrüßt die Bemühungen um Klärung der Terminologie. Sie nimmt zur Kenntnis, dass die vorgeschlagene Richtlinie mit der Auffassung übereinstimmt, die sie in ihrem Arbeitspapier "Die Verarbeitung personenbezogener Daten im Internet"⁷ vertreten hat, wonach beide Datenschutzrichtlinien voll auf die Verarbeitung von Daten im Internet⁸ anwendbar sind.

Verkehrsdaten werden definiert als *alle Daten, die im Verlauf oder für die Übertragung einer Nachricht über ein elektronisches Kommunikationsnetz verarbeitet werden*. Diese

⁵Dies ergibt sich aus Artikel 3 dieses Richtlinienentwurfs und Artikel 2 des Entwurfs der Richtlinie über den allgemeinen Rahmen. Die Gruppe stellt fest, dass der Begriff "öffentlich zugänglicher Kommunikationsdienst" in keinem der beiden Texte definiert wird und die Definition des "elektronischen Kommunikationsdienstes" im Richtlinienentwurf über den Schutz der Privatsphäre im Vergleich zu der im Rahmentext enthaltenen Definition nicht vollständig ist.

⁶ Wissenswert wäre auch, ob Textmitteilungen auf Mobiltelefonen abgedeckt werden.

⁷ Alle Dokumente, die von der Arbeitsgruppe angenommen werden, können unter folgender Adresse abgerufen werden: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm

⁸ Siehe Artikel 2 -Begriffsbestimmungen, Entwurf des Erwägungsgrundes (5), Artikel 3 - Betroffene Dienste, sowie die Definition des Begriffs "elektronische Kommunikationsnetze" im Rahmentext, wo die angeführten Beispiele um "IP-Netze" ergänzt werden könnten.

Definition enthält keine "Notwendigkeitsklausel". Die Gruppe begrüßt diesen Ansatz, der dazu führt, dass alle Verkehrsdaten, die während einer Verbindung erzeugt werden, ob sie für die Herstellung der Verbindung notwendig sind oder nicht, nach Beendigung der Verbindung gelöscht werden müssen (siehe Artikel 6 Absatz 1). Die Definition bezieht Standortdaten ein, die während der Verbindung erzeugt werden, sowie "Navigationsdaten" (wie zum Beispiel URLs/Unique Resource Locator), die Aufschluss über die persönlichen Interessen des Betroffenen geben könnten (unter anderem über die besuchten Websites, die wiederum Hinweise auf religiöse Überzeugung, politische Meinung, Gesundheit oder Sexualeben geben). Da sie genau angeben, welche Seiten einer Website besucht wurden, zeigen sie nämlich den Inhalt, den die betreffende Person abgerufen hat.

Da Verkehrsdaten solche personenbezogenen Informationen über die betreffende Person enthalten könnten, sollten sie darüber hinaus mit der Vertraulichkeit behandelt werden, die für Kommunikation gilt (siehe Artikel 5 und unten)⁹.

Die Gruppe geht davon aus, dass die vorgeschlagene Definition von "Anruf" Sprachtelefondienste über das Internet nicht umfasst, sondern lediglich traditionelle leitungsvermittelte Sprachtelefondienste.

Die Gruppe begrüßt zwar die im Richtlinienentwurf enthaltene Definition von „Anruf“, weist jedoch darauf hin, dass sie nach wie vor die Auffassung vertritt, dass „Anruf“ im Sinne der bestehenden Richtlinie 97/66/EG auch die Nutzung des Internets umfasst. Der Begründung des Richtlinienentwurfs zufolge scheint die Europäische Kommission diese Ansicht zu teilen.

Die Gruppe stellt fest, dass der Begriff „Teilnehmer“ nicht mehr definiert wird, obwohl er im Richtlinienentwurf durchgängig benutzt wird. Statt dessen wird der Begriff „Benutzer“ definiert, der jedoch juristische Personen ausschließt. Die Gruppe möchte die Gründe für diese Änderungen wissen.

Im Richtlinienentwurf ist nicht mehr von „Telekommunikationsdiensten“ die Rede, sondern von „elektronischen Kommunikationsdiensten“. In der Begründung des Entwurfs wird erwähnt, dass diese Änderung erforderlich war, um eine terminologische Übereinstimmung mit dem Vorschlag für eine Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste zu erzielen¹⁰.

Der Begriff „elektronische Kommunikationsdienste“ wird im Entwurf der Richtlinie über den Schutz der Privatsphäre nicht definiert, wohl aber in Artikel 2(b) der vorgeschlagenen Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und -dienste.

Der neuen Definition zufolge sind *Elektronische Kommunikationsdienste gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung und Leitweglenkung von Signalen über elektronische Kommunikationsnetze bestehen, einschließlich Telekommunikations- und Übertragungsdienste in Rundfunknetzen, nicht aber Dienste, die Inhalte über elektronische Kommunikationsnetze und -dienste anbieten oder eine redaktionelle Kontrolle über sie ausüben.*

⁹ Ein weiterer, noch zu erörternder Aspekt ist, dass einige dieser Daten auch als sensible Daten im Sinne der allgemeinen Datenschutzrichtlinie 95/46/EG angesehen werden könnten, deren Verarbeitung im Prinzip verboten ist.

¹⁰ KOM(2000) 393.

Die neue Definition basiert eigentlich auf dem gleichen Kerngedanken wie die frühere Definition (die Übertragung und Leitweglenkung von Signalen über elektronische Kommunikationsnetze); die Aufführung einiger Beispiele für Dienste, die in die Definition einbezogen oder davon ausgeschlossen sind, ist jedoch sehr nützlich, weil dadurch Licht auf die in vorausgegangenen Abschnitten erwähnten Diskussionen geworfen wird.

Aus der in der neuen Definition enthaltenen Liste kann gefolgert werden, dass Dienste, die Inhalte über elektronische Kommunikationsnetze und –dienste anbieten nicht in den Anwendungsbereich der vorgeschlagenen Richtlinie über den Schutz der Privatsphäre fallen werden. Dies wird auch in Erwägungsgrund 7 der Präambel der vorgeschlagenen Richtlinie über einen gemeinsamen Rechtsrahmen für elektronische Kommunikationsnetze und –dienste bekräftigt, der lautet: *Es ist notwendig, die Regulierung der Übertragung von der Regulierung von Inhalten zu trennen.* Es wird jedoch betont, dass bei dieser Trennung die Verbindungen zwischen beiden zu berücksichtigen sind.

Die wichtigste Folge dieser Trennung ist, dass zusätzliche Dienste wie z.B. DoubleClick oder Dienste, die Inhalte an ein Portal oder eine Website liefern (jedoch nicht als Host dafür dienen) nicht durch diese Richtlinie abgedeckt werden, sondern lediglich durch die allgemeine Datenschutzrichtlinie. Darüber hinaus bedeutet dies, dass *Internet Service Provider* dann unter die spezifische Richtlinie fallen, wenn sie als Zugangsanbieter tätig sind und die Verbindung zum Internet bereitstellen; wenn sie Inhalte bereitstellen, werden sie lediglich von der allgemeinen Richtlinie abgedeckt.

Der Vorteil einer eindeutigen Trennung der Regulierung der Inhalte von der Regulierung der Übertragung liegt in der dadurch entstehenden Klarheit. In der Praxis wird es jedoch schwieriger sein, mit einer solchen Trennung zu arbeiten (z.B. im Falle eines *Internet Service Providers*, der auch Inhalte anbietet, indem er als Host für seine eigene Portal-Site fungiert). Dieser ISP muss dann die Bestimmungen der allgemeinen Richtlinie auf alle seine Tätigkeiten anwenden und die Bestimmungen der spezifischen Richtlinie (die spezifische Pflichten enthält) auf seine Tätigkeiten als Zugangsanbieter.

Ein weiterer interessanter Aspekt der neuen Definition von „elektronischen Kommunikationsdiensten“ ist die Erwähnung der Tatsache, dass diese Dienste gegen Entgelt zur Verfügung gestellt werden sollten. Weder die Präambel noch die Begründung erwähnen diesen Begriff und enthalten keine Anhaltspunkte zu seiner Auslegung. Dies könnte dahingehend interpretiert werden, dass die Anbieter eines kostenlosen Zugangs nicht in den Anwendungsbereich der überarbeiteten Richtlinie über den Schutz der Privatsphäre fallen würden, da sie von den Internetbenutzern kein Entgelt (zumindest keine finanzielle Vergütung) erhalten.

Diese Interpretation ist jedoch nicht korrekt, da der Gerichtshof der Europäischen Gemeinschaften in seiner Rechtsprechung über Dienstleistungen im Sinne von Artikel 50 (ex-Artikel 60) EG-Vertrag¹¹ deutlich zum Ausdruck gebracht hat, dass das Entgelt nicht unbedingt durch den Empfänger der Dienstleistung gezahlt werden muss. Es kann z.B. auch durch Werbung erbracht werden.

¹¹ Urteil C-109/92 Wirth [1993], Slg. I-6447, 15

Die Anbieter eines kostenlosen Zugangs erhalten ihr Entgelt nämlich von denjenigen, die Werbung oder Banner auf den Internetseiten unterbringen. Damit ist klar, dass diese Dienste unter die Definition der elektronischen Kommunikationsdienste fallen und somit in den Anwendungsbereich der Richtlinie.

Es wäre jedoch wünschenswert, wenn dies im Richtlinienentwurf klargestellt würde, da nicht jeder Leser der Richtlinie mit der Auslegung dieses Begriffs durch den Gerichtshof der Europäischen Gemeinschaften vertraut ist.¹²

Artikel 4 - Sicherheit

Die Gruppe begrüßt die im Erwägungsgrund 13 enthaltene Erklärung über Sicherheitsmaßnahmen, wie zum Beispiel die Verschlüsselung. Sie schlägt vor, die Notwendigkeit konkreterer Verpflichtungen für Netzbetreiber und Diensteanbieter auf der Grundlage einer Analyse nationaler Gesetze zur Umsetzung von Sicherheitsanforderungen in Betracht zu ziehen, um freien Datenverkehr und freien Austausch von Ausstattung (Software und Hardware) zu erleichtern. Es wäre außerdem von Nutzen, konkreter auf die auf dem Spiel stehenden Risiken hinzuweisen, und zwar nicht nur in bezug auf das Internet, sondern auch auf sonstige Kommunikationsumgebungen, da die Sicherheitsverpflichtungen allen Netz- und Diensteanbietern auferlegt werden.

Artikel 5 - Vertraulichkeit der Kommunikation

Die Gruppe erinnert an die allgemein geteilte Auffassung, wonach Vertraulichkeit der Kommunikation zu den wichtigsten Bestandteilen des Schutzes des Grundrechts auf Privatsphäre, Datenschutz und Kommunikationsgeheimnis zählt. Jegliche Ausnahme von diesem Recht und dieser Verpflichtung sollte auf das in einer demokratischen Gesellschaft unbedingt Notwendige beschränkt und in Übereinstimmung mit den Bestimmungen von Artikel 15 und Artikel 13 der Richtlinie 95/46/EG gesetzlich eindeutig definiert werden.

Da der Wortlaut des vorgeschlagenen Artikels 5 Absatz 2 zu vage ist und somit Ausnahmen von dem Grundsatz der Vertraulichkeit ohne Berücksichtigung der grundlegenden Bedingungen zulässt, sollte dieser Absatz gestrichen werden.

In diesem Zusammenhang erinnert die Gruppe an ihre Empfehlung 2/99, in der sie betont, dass Netzbetreiber und Telekommunikationsdienste die erforderlichen Maßnahmen ergreifen müssten, um das Abfangen von Telekommunikation durch Unbefugte unmöglich zu machen oder technisch so zu erschweren, wie es der gegenwärtige Stand der Technik erlaubt. Die Gruppe betont in diesem Zusammenhang, dass die Umsetzung wirksamer Möglichkeiten des Abfangens von Kommunikation, unter Anwendung gerade der fortgeschrittensten Techniken, nicht zu einer Herabsetzung des Grades der Vertraulichkeit der Kommunikation und des Schutzes der Privatsphäre von Personen führen darf.

Diese Verpflichtungen gewinnen besondere Bedeutung, wenn Telekommunikationsverbindungen zwischen Personen, die sich auf dem Gebiet der Mitgliedstaaten befinden, über das europäische Hoheitsgebiet hinausgehen oder

¹² Beispielsweise durch Aufnahme des Wortlauts „normalerweise gegen Entgelt“ in die Definition und Erklärung der Bedeutung der Begriffe im Sinne der oben genannten Rechtsprechung im einschlägigen Erwägungsgrund.

hinausgehen könnten, insbesondere wenn hierbei Satelliten oder das Internet zum Einsatz kommen.

Die Vertraulichkeit der Kommunikation (auch im Internet) muss die Regel, nicht die Ausnahme sein.

Artikel 6 - Verkehrsdaten und Daten für die Gebührenabrechnung

Die Gruppe ist der Meinung, dass die Gelegenheit genutzt werden sollte, die Bestimmungen zu Verkehrsdaten eingehender zu überprüfen. In Anbetracht der weit gefassten Definition von Verkehrsdaten sollte klargestellt werden, dass es nicht unbedingt akzeptabel ist, wenn alle Verkehrsdaten auf die gleiche Weise behandelt werden. Es sollte klar sein, für welche Zwecke und in welchem Umfang bestimmte Verkehrsdaten (im Sinne der neuen, weiter gefassten Definition) überhaupt erzeugt, gesammelt und gespeichert werden dürfen und für welche Zwecke sie weiterverwendet werden könnten. Die Gruppe möchte betonen, dass die Benutzer nicht ein für allemal auf das Recht auf Privatsphäre und Datenschutz verzichten, wenn sie der Verarbeitung der Daten für einen bestimmten Zweck zustimmen. Die Gruppe erinnert auch daran, dass das in der derzeit gültigen Richtlinie 97/66/EG vorgesehene Schutzniveau in jedem Fall aufrechterhalten, wenn nicht sogar verstärkt werden sollte.

Zu Artikel 6 (2): Hinsichtlich des gegenwärtigen Textvorschlags, der die Verarbeitung von Verkehrsdaten zulässt, die für die Gebührenabrechnung erforderlich sind, stellt die Gruppe fest, dass der Richtlinienentwurf keine Harmonisierung des Zeitraums vorsieht, in dem die Rechnung gesetzlich angefochten werden kann. Die Gruppe möchte wissen, wie die Kommission beabsichtigt, die Empfehlung 3/99 der Gruppe weiterzuverfolgen, nämlich diesen Zeitraum zu harmonisieren, um die Speicherung von Verkehrsdaten für diesen konkreten Zweck der Gebührenabrechnung zu begrenzen und damit das Grundrecht der Bürger auf den Schutz der Privatsphäre zu stärken. Die Gruppe fordert das Europäische Parlament und den Rat auf, eine klare Frist zu setzen, die so kurz wie möglich sein sollte.

Jegliche Verarbeitung von Verkehrsdaten für zusätzliche Zwecke bedeutet eine neue Gefährdung des Grundrechts auf Schutz der Privatsphäre und kann nur unter der Voraussetzung erwogen werden, dass geeignete Schutzvorkehrungen vorhanden sind. Die Gruppe empfiehlt deshalb, in Artikel 6 Absatz 3 einen "Notwendigkeitstest" aufzunehmen im Hinblick auf die Möglichkeit, Verkehrsdaten für die Zwecke des eigenen Marketings des Anbieters zu verarbeiten.

Was den Vorschlag anbelangt, die Verarbeitung von Verkehrsdaten für die Erbringung von "Mehrwertdiensten" zuzulassen, ist die Gruppe der Ansicht, dass dieser Ausdruck im Hinblick auf eine Garantie der Einschränkung des Zwecks nicht klar genug ist. Der Erwägungsgrund enthält weder eine Definition noch Hinweise auf die vollständige Bandbreite derartiger Dienste. Da der Zusammenhang ein anderer ist als bei der Vermarktung der eigenen Dienste des Anbieters, könnten andere Garantien erforderlich sein.

Die Gruppe unterstützt die neue Bestimmung in Artikel 6 Absatz 4 bezüglich der Informationen, die der betroffenen Person gegeben werden sollen. Sie schlägt vor, in den entsprechenden Erwägungsgrund ebenfalls aufzunehmen, dass die betroffene Person auch

über ihr Recht unterrichtet werden muss, gegen die Verarbeitung Widerspruch einlegen zu können (Artikel 14 der Richtlinie 95/46/EG).

Artikel 7 - Einzelgebührenachweis

Die Gruppe begrüßt den ausdrücklichen Hinweis im betreffenden Artikel auf alternative Modalitäten für Einzelgebührenachweise, die die Privatsphäre besser schützen. Gleichzeitig bedauert sie, dass eine dieser Modalitäten (Unkenntlichmachung der Ziffern, Erwägungsgrund 18 der Richtlinie 97/66/EG) in dem Entwurf des Erwägungsgrunds nicht mehr erwähnt wird. Die Gruppe wünscht eine Bestätigung in dem Sinne, dass diese Modalität auch weiterhin ein gesetzliches Mittel bleibt und empfiehlt ihre Aufnahme in den Erwägungsgrund.

Artikel 9 - Standortdaten

Da mehr Klarheit über Mehrwertdienste erforderlich ist (siehe oben), sollte die Nutzung von Standortdaten (Verkehrsdaten) für derartige Zwecke in Anbetracht der weiter oben vorgeschlagenen gründlichen Überprüfung der Bestimmungen über Verkehrsdaten untersucht werden. Grundsätzlich sollten Standortdaten nicht für die Erbringung von Mehrwertdiensten verarbeitet werden. Sie können ausnahmsweise für klar umrissene Zwecke verarbeitet werden, bei denen die Nutzung von Standortdaten technisch erforderlich ist und vorausgesetzt, dass angemessene Vorkehrungen zur Sicherung der Privatsphäre getroffen sind.

Ohne die endgültige Haltung der Gruppe zu dem inhaltlichen Aspekt des Problems der Verarbeitung von Standortdaten für Mehrwertdienste¹³ vorwegzunehmen, ist die Gruppe der Meinung, dass die in Artikel 9 (2) vorgeschlagene technische Möglichkeit, die Verarbeitung von Standortdaten zu verhindern, keine zufriedenstellende Lösung ist. Angesichts der Sensibilität von Standortdaten in bezug auf die Freizügigkeit und der Tatsache, dass die hier erfassten Standortdaten für die Herstellung der Verbindung nicht notwendig sind, muss der Benutzer/Teilnehmer vollständige Kontrolle über ihre Verarbeitung haben. Somit sollte das Gegenteil die Regel sein: Der Teilnehmer muss die Möglichkeit haben, die Verarbeitung von Standortdaten bei jeder Erbringung eines Mehrwertdienstes (wozu erforderlichenfalls die Verbindung zum Netz, die Übertragung oder eine Kommunikation gehören) auf einfache Weise und kostenfrei zu gestatten. Die technische Umsetzung dieses Rechts muss innerhalb der Ausstattung des Benutzers/Teilnehmers und nicht im Netz verankert sein (im Gegensatz zur Rufnummernanzeige).

Artikel 10 - Ausnahmen

Die Gruppe ist der Ansicht, dass in diesem Artikel zusätzliche Sicherungen erforderlich sein könnten, um die Umgehung der strikteren Regeln in Artikel 15 und Artikel 13 der Richtlinie 95/46/EG zu verhindern. Da der "alte" Begriff "Anruf" hier beibehalten wird, geht die Gruppe davon aus, dass in diesem Artikel nur Sprachtelefondienst über Fest-

¹³ Oder allgemeiner die Bekanntgabe von Standortdaten an Benutzer des Netzes

und Mobilnetze abgedeckt wird, nicht jedoch Sprachtelefondienst über das Internet, IP-Adressen und E-Mails.

(a) Was die vorgeschlagene Möglichkeit anbelangt, sich über die Entscheidung des Teilnehmers, seine Nummer auf seinen Antrag hin nicht anzuzeigen¹⁴, hinwegzusetzen, damit böswillige oder belästigende Anrufe zurückverfolgt werden können, sollten Sicherungen vorgesehen werden, die dafür Sorge tragen, dass geprüft wird, ob ein Anruf tatsächlich böswillig oder belästigend war.

(b) Das Außerkraftsetzen der Unterdrückung der Rufnummernanzeige und die Nutzung von Standortdaten gegen den Willen des Teilnehmers/Benutzers oder ohne sein Wissen sind nicht deutlich genug: Erstens sollte geklärt werden, welche Standortdaten (Verkehrsdaten) hier gemeint sind. Zweitens sollten die Strafverfolgungsbehörden, die berechtigt sind, Notfalleinrufe entgegenzunehmen, genauer benannt werden, um eine Umgehung von Artikel 15 auszuschließen. Außerdem sollte festgelegt werden, dass die Daten nach erfolgter Hilfeleistung gelöscht werden müssen.

In diesem Zusammenhang stellt die Gruppe fest, dass die Mitgliedstaaten nach *Artikel 22 (3) des Entwurfs der Richtlinie über den allgemeinen Dienst und die Rechte des Nutzers*¹⁵ sicherstellen müssen, dass die Netzbetreiber Rettungsdiensten die Adresse des Anrufers mitteilen, und zwar soweit technisch machbar bei allen '112'-Anrufen. Obwohl es unbestritten ist, dass die für die Rettung von Personen in Notsituationen bereitstehenden Dienste über alle Informationen verfügen sollten, die für die Erkennung des Anrufers erforderlich sind, weist die Gruppe die Kommission auf die Notwendigkeit hin, die Übereinstimmung mit den Grundsätzen des Datenschutzes zu gewährleisten. Beiden Texten sollte das gleiche Verständnis und die gleiche Definition von "Rettungsdiensten" zugrunde liegen. Und die Verpflichtung zur Bekanntgabe von Standortdaten gegenüber diesen Stellen sollte auf die Angaben beschränkt sein, die für die Identifizierung des Hilfsbedürftigen erforderlich sind. In Anbetracht der Sensibilität der Standortdaten (siehe Anmerkungen zu den Artikel 2 und 9) wäre es in gewisser Hinsicht vielleicht erwägenswert, den Notfallruf '112' als Dienst einzustufen, was zur Folge hätte, dass nur die erforderlichen Standortdaten von Anrufern, die der Erbringung dieser Dienstleistung zugestimmt haben, an die "112"-Notrufdienste weitergegeben werden.

Artikel 12 - Teilnehmerverzeichnisse

Die Gruppe unterstützt den Vorschlag, den Teilnehmern die Entscheidung darüber zu überlassen, ob sie in elektronischen oder gedruckten Verzeichnissen aufgeführt werden wollen. Darüber hinaus sollten die Teilnehmer angesichts der Bedeutung elektronischer Verzeichnisse, insbesondere in der heutigen Informationsgesellschaft, über die Nutzungsmöglichkeiten der Verzeichnisse unterrichtet werden, und die Daten, die dort veröffentlicht werden, sollten auf die Angaben beschränkt werden, die für die Ermittlung ihrer Person notwendig sind, aber keine privateren Informationen preisgeben.

Diese Anforderung ist verbunden mit einer Frage, die noch nicht in dem Richtlinienentwurf angesprochen wird: Mehrere Datenschutzbehörden sind derzeit mit Fällen befasst, bei denen es um Recherchen zur Rückverfolgung anhand von

¹⁴ Die Unterdrückung der Anzeige der Nummer des Anrufers bedeutet, dass der Teilnehmer sich dafür entschieden hat, gegenüber dem Angerufenen anonym zu bleiben. Ein Außerkraftsetzen dieses Rechts bedeutet, dass die Nummer des Anrufers auch gegen seinen Willen angezeigt werden kann. Im Hinblick auf Notfalleinrufe wird vorgeschlagen, dies auch auf Standortdaten anzuwenden, selbst wenn der Teilnehmer einer Verarbeitung solcher Daten nicht zugestimmt hat.

¹⁵ Abrufbar auf der in Fußnote 2 angegebenen Website

Verzeichnissen geht. Hierbei handelt es sich um neue Dienstleistungen auf dem liberalisierten Telekommunikationsmarkt, bei denen einfach und kostengünstig erweiterte Möglichkeiten der Verarbeitung aller in den Telefonbüchern enthaltenen Informationen angeboten werden. Es ist zum Beispiel möglich, anhand der Telefonnummer den Namen und die Adresse einer bestimmten Person herauszufinden oder anhand des Straßennamens die Namen und Telefonnummern aller Personen, die in dieser Straße wohnen. Es lässt sich sehr viel mehr über eine Person in Erfahrung bringen, als diese sich bei der Zustimmung zur Veröffentlichung ihrer Telefonnummer im Telefonbuch vorstellen kann. Es können so viele Informationen zusammengetragen werden, wie normalerweise auf einer Visitenkarte stehen (vollständiger Name, Adresse, Beruf, Arbeitsstelle). Außerdem würde der Einzelgebühreennachweis eines Bürgers, auf dem nur die angerufenen Telefonnummern erscheinen, zur Erstellung einer Liste der Namen und Anschriften sämtlicher Personen ausreichen, die die betreffende Person in einem bestimmten Zeitraum angerufen hat. Andere Rechercheprodukte beinhalten geographische Informationen ("Standortdaten", siehe Anmerkungen zu den Artikeln 2 und 9), wie zum Beispiel Stadtpläne und Datenbanken mit Photographien aller Wohnungen einer Stadt. Diese Informationen könnten problemlos mit der Adresse in einem Telefonbuch, das Mehrfachkriteriensuche zulässt, in Verbindung gebracht werden.

Dies ist eine neue Nutzungsmöglichkeit der Verzeichnisse, die mit dem ursprünglichen Zweck nicht vereinbar ist. Außerdem ist sie illegal, es sei denn die betroffene Person hat ihr Einverständnis zu der Verarbeitung ihrer persönlichen Daten für diese neuen Zwecke erteilt. Die Gruppe hat einen gemeinsamen Standpunkt zu diesem Thema angenommen und hält es für wichtig, dass sich der Richtlinienentwurf ausdrücklich mit diesem Thema befasst, und zwar in dem Sinne, dass die betreffende Person der Aufnahme von Daten in öffentliche Verzeichnisse mit der Möglichkeit der Recherche zur Rückverfolgung nach gründlicher Information über die Sachlage zustimmen muss.

Ein weiterer wichtiger Aspekt besteht darin, dass Verzeichnisse von jedermann herausgegeben werden können. Daher muss unbedingt sichergestellt werden, dass die Übertragung der darin enthaltenen Daten den (kostenlos geäußerten) Wünschen der Benutzer/Teilnehmer gegenüber dem ursprünglichen Anbieter entsprechen. Der ursprüngliche Anbieter/Betreiber muss die Benutzer/Teilnehmer vor dem Vertragsabschluss über diese Nutzungsarten (kommerziell, Rückverfolgung usw.) unterrichten.

Darüber hinaus führt die Bereitstellung von Daten auf CD-ROM bisweilen zu einem weiteren Problem hinsichtlich der Gültigkeitsdauer der Lizenz: Die Gültigkeitsdauer sollte so festgelegt werden, dass die Nutzung von Daten, die angesichts der Wahl der Betroffenen überholt sind, nicht gestattet ist.

Artikel 13 - Unerbetene Nachrichten

„Spamming“ ist die Versendung unerbetener, meist kommerzieller E-Mails in großer Zahl und zu wiederholten Malen an Personen, zu denen der Absender vorher keinen Kontakt hatte. Es stellt eine spezifische Form der Verletzung der Privatsphäre dar: Der Benutzer hat kein menschliches Gegenüber, trägt die Kosten für die Nachricht und erhält die unerbetenen Nachrichten normalerweise innerhalb des geschützten Rahmens seines privaten Heims.

Erwartungsgemäß ziehen Verbraucher erwünschte und gezielte kommerzielle Kommunikation vor; unerbetene Nachrichten sind belästigend, zeitraubend zu lesen und zu löschen und kosten Geld. Die Belästigung durch Junk-E-Mails untergräbt das Vertrauen des Kunden in den elektronischen Geschäftsverkehr.

Doch auch die Industrie fordert Rechtssicherheit: Unerbetene E-Mails zwingen Internet Service Provider, die Bandbreite und Ausrüstung zur Versendung von Junk-E-Mails bereitzustellen, die die große Mehrheit ihrer Kunden nicht wünscht. Unerbetene E-Mails von den Servern zu löschen und mit verärgerten Kunden zu verhandeln verursacht darüber hinaus beträchtliche Kosten. Es kommt manchmal vor, dass Systeme aufgrund der schieren Masse im Umlauf befindlicher unerbetener kommerzieller E-Mails abstürzen und dadurch der rechtmäßige Datenverkehr blockiert und verzögert wird. Die meisten Internet Service Provider versuchen, unerbetene E-Mails herauszufiltern, und haben Klauseln in ihren Verträgen mit Teilnehmern, dass letztere unerbetene E-Mails nicht versenden oder weitergeben dürfen. Es existieren Verzeichnisse verdächtiger Server, die als Quelle von Junk-E-Mails bekannt sind. Die Filter, die dafür verwendet werden, sind allerdings nicht 100 %ig zuverlässig, so dass sie außerdem den rechtmäßigen Datenverkehr blockieren, wenn dieser von einem Server ausgeht, der auf der schwarzen Liste steht. Da es jedoch kein gesetzliches Verbot unerbetener E-Mails gibt, bringt diese Praxis die Internet Service Provider in eine schwierige Rechtslage. Ein gesetzliches Verbot würde gezieltere Aktionen gegen die Versender von Junk-E-Mails erleichtern.

Neue Markttendenzen weisen darauf hin, dass führende Online-Direktvertreiber in den USA auf der Grundlage von "Marketing per Genehmigung" („permission based marketing“; opt-in) arbeiten, weil die auf dieser Basis gelieferten Daten von besserer Qualität sind und der Rückfluss positiver Antworten deutlich höher ist. Manche praktizieren sogar „doppeltes opt-in“ („double opt-in“): Obwohl die betreffende Person der Zusendung kommerzieller E-Mails zugestimmt hat (zum Beispiel durch Äußerung dieses Wunsches auf einer Website), wird sie beim folgenden ersten (erwünschten) E-Mail-Kontakt erneut gebeten, dem Händler diesen Wunsch zu bestätigen.

Das Internet bietet umfassende Gelegenheiten, E-Mail-Adressen von Benutzern zu sammeln, die an der Zusendung kommerzieller E-Mails zu bestimmten Themen interessiert und gewillt sind, dazu ihre Zustimmung zu geben. Mails, die mit der Zustimmung des Adressaten versandt werden, erreichen wahrscheinlich weit mehr potentielle Kunden als unerbetene E-Mails.

In fünf Mitgliedstaaten (Deutschland, Österreich, Italien, Finnland und Dänemark) ist die Versendung unerbetener kommerzieller E-Mails verboten. In den anderen Mitgliedstaaten gibt es entweder ein Opt-out-System, oder die Situation ist nicht vollständig geklärt. Unternehmen in Opt-out-Ländern können nicht nur E-Mail-Adressen in ihrem eigenen Land anschreiben, sondern auch Verbraucher in den Mitgliedstaaten mit einem Opt-in-System. Da E-Mail-Adressen darüber hinaus häufig keinerlei Aufschluss über das Wohnland des Empfängers geben, bieten unterschiedliche Regelungssysteme innerhalb des Binnenmarktes keine gemeinsame Lösung für den Schutz der Privatsphäre des Verbrauchers.

Opt-in ist eine ausgewogene und effiziente Lösung, um Hindernisse für die Versendung kommerzieller E-Mails aus dem Weg zu räumen und zugleich das Grundrecht des Verbrauchers auf Privatsphäre zu schützen.

Die Gruppe begrüßt und unterstützt daher den Vorschlag, unerbetene elektronische Post wie Voice-Mail-Systeme und Fernkopien (Faxe) zu behandeln. In allen diesen Fällen hat der Teilnehmer kein menschliches Gegenüber und trägt einen Teil oder alle Kosten der *Nachricht*. Das Ausmaß des Eingriffs in die Privatsphäre und die finanzielle Belastung sind vergleichbar (siehe Stellungnahme 1/2000).

Artikel 14- Technische Merkmale und Normung (und Erwägungsgrund 22)

Die Gruppe begrüßt und unterstützt den Vorschlag, erforderlichenfalls konkrete Maßnahmen auf Gemeinschaftsebene zu ergreifen, um eine harmonisierte Umsetzung der Datenschutzvorschriften zu gewährleisten.

Da sich Technologie „von unten nach oben“ entwickelt, könnte es nützlich sein, der Industrie ins Gedächtnis zu rufen, dass es in ihrem eigenen Interesse liegt, bei der Entwicklung von Soft- und Hardware von Beginn an die Privatsphäre nicht nur zu berücksichtigen, sondern in höherem Maße zu integrieren. Die Gruppe ist der Auffassung, dass die Technologie sich an die gesetzlichen Vorschriften halten und ihre Umsetzung erleichtern muss, insbesondere das aus Artikel 6 und 7 der Richtlinie 95/46/EG abzuleitende Prinzip der Datenvermeidung und die Achtung der Rechte der betroffenen Person. Im Hinblick auf die in verschiedenen Mitgliedstaaten gewonnenen Erfahrungen, die Empfehlung 3/97 der Gruppe zur Anonymität im Internet und ihre Empfehlung 1/99 zur unsichtbaren und automatisierten Verarbeitung personenbezogener Daten im Internet durch Software und Hardware¹⁶ wird vorgeschlagen, einen Absatz hinzuzufügen, der etwa wie folgt lauten sollte:

Für Entwurf und Auswahl von Datenverarbeitungstechnologien, einschließlich Hardware und Software, soll die Prämisse gelten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten und die Achtung der Rechte der betroffenen Person zu erleichtern. Wo es möglich ist und im Hinblick auf den erwünschten Schutz nicht unverhältnismäßig erscheint, sind anonymisierte Daten und Pseudonyme zu verwenden.

Transparenz

Nach Auffassung der Gruppe ist zwar klar, dass die Verpflichtung zur Information der betroffenen Person entsprechend der allgemeinen Datenschutzrichtlinie gilt¹⁷, es aber einen Mehrwert darstellen würde, wenn die Anbieter ausdrücklich verpflichtet würden, die Teilnehmer/Benutzer vor dem Vertragsabschluss/der Benutzung und auch danach über ihre Rechte zu informieren und ihnen damit die Möglichkeit zu geben, jederzeit alle Möglichkeiten/Rechte zu nutzen, die ihnen nach den Datenschutzrichtlinien zustehen. Diese Informationen betreffen den Zweck der beabsichtigten Verarbeitung, den Kontrollmechanismus, die Empfänger, falls eine dritte Partei beteiligt ist, die Rechte des Einzelnen usw. Es wird vorgeschlagen, dass die Anbieter/Betreiber diese Informationen veröffentlichen, damit die Teilnehmer/Benutzer jederzeit alle vorhandenen Möglichkeiten zur Wahrung ihrer Rechte nutzen können. Dies könnte beispielsweise durch Bekanntmachung der Datenschutzpolitik auf einer Website erfolgen.

¹⁶ Alle Dokumente, die von der Gruppe angenommen wurden, sind unter folgender Adresse abrufbar: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm.

¹⁷ siehe Artikel 10, 11, 12, 14 usw. der Richtlinie 95/45/EG, auf die in Erwägungsgrund 9 des Richtlinienentwurfs hingewiesen wird, ferner Artikel 4 Absatz 2, 6 Absatz 4, 7, 8, 9, 11, 12 und 13 des Richtlinienentwurfs

3. Schlussfolgerungen

Die Gruppe begrüßt die Neufassung, mit der sichergestellt werden soll, dass zu ein und derselben Dienstleistung gleichlautende Vorschriften erlassen werden, unabhängig von den Mitteln, durch die die Leistung erbracht wird. Dies bedeutet auch, dass Verbraucher und Benutzer den gleichen Schutz hinsichtlich ihrer personenbezogenen Daten und ihrer Privatsphäre genießen, ungeachtet der Technologie, mittels derer eine bestimmte Dienstleistung erbracht wird. Die Gruppe teilt und unterstützt voll und ganz die Ansicht der Kommission, dass die Aufrechterhaltung eines hohen Niveaus bei Datenschutz und Schutz der Privatsphäre der Bürger ein erklärtes Ziel ist. Die Gruppe erkennt außerdem an, dass sehr viele Anpassungen vorgeschlagen werden, um das Datenschutzniveau in allen elektronischen Kommunikationen zu erhöhen.

Die Gruppe empfiehlt der Kommission, dem Europäischen Parlament und dem Rat, ihre Anmerkungen zu berücksichtigen. Sie fordert die Kommission auf, offene Fragen zu klären, damit sich die Gruppe am laufenden Prozess beteiligen kann.

Die Gruppe schlägt vor, diesen Richtlinienentwurf in der Arbeitsgruppe für wirtschaftliche Fragen – Datenschutz des Rates zu erörtern. Dadurch könnte das Verfahren zur Annahme aller im Rahmen der Überprüfung der Rechtsvorschriften zur Telekommunikation vorgeschlagenen Richtlinien beschleunigt und der vorliegende Text den zuständigen Sachverständigen zugänglich gemacht werden.

Die Gruppe behält sich die Möglichkeit vor, weitere Änderungen des Richtlinienentwurfs zu kommentieren.

Geschehen zu Brüssel am 2. November 2000

Für die Arbeitsgruppe

Der Vorsitzende

Stefano RODOTA