5001/01/DE/endg.
WP 41

Stellungnahme 4/2001

zum Entwurf einer Konvention des Europarates über Cyberkriminalität

(Angenommen am 22. März 2001)

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 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie,

gestützt auf ihre Geschäftsordnung, insbesondere Artikel 12 und 14,

hat folgende Stellungnahme angenommen:

Einführung

Die Cyberkriminalität gehört zu den Schattenseiten der Informationsgesellschaft. Neue Technologien sind nicht nur von ungeheurem Nutzen für die Gesellschaft, sie schaffen auch Möglichkeiten zur Begehung neuer Arten von Straftaten oder aber traditioneller Straftaten unter Einsatz neuer Mittel. Die Staaten sowie eine Reihe von Organisationen und Gremien sind sich dieser Problematik bewusst, und daher wird das Thema u. a. im Rahmen der Europäischen Union[2], der G8[3], der OECD, der Vereinten Nationen und des Europarats erörtert. Das Ziel dieser Maßnahmen ist die Schaffung einer Informationsgesellschaft, die den Bürgern Freiheit und Sicherheit bietet.

Der Europarat blickt auf eine lange Erfahrung und Tradition bei der internationalen Zusammenarbeit in Fragen der Kriminalitätsbekämpfung und bei den Menschenrechten zurück. Seit 1997 arbeitet er an einer Konvention zur Cyberkriminalität. Der Sachverständigenausschuss für Fragen der Cyberkriminalität (PC-CY) hat seine Arbeit im Dezember 2000 abgeschlossen, und die Parlamentarische Versammlung des Europarates muss eine Stellungnahme dazu abgeben (voraussichtlich im Frühjahr 2001), bevor der Text dem Ministerkomitee des Europarates zur Annahme vorgelegt wird. Entsprechend der Stellungnahme der Versammlung wird eine Redaktionsgruppe mit Textänderungen beauftragt.

Die Konvention, die nunmehr im Entwurf vorliegt, kann auch von Ländern unterzeichnet werden, die nicht Mitglied des Europarates sind. Die Vereinigten Staaten, Kanada, Japan und Südafrika waren bereits an der Ausarbeitung des Entwurfs aktiv beteiligt.

Seit April 200 hat es mehrere Entwürfe der Konvention gegeben, die der Öffentlichkeit auf der Website des Europarats zugänglich gemacht wurden. Der Entwurf der Begründung wurde erst vor kurzem, nämlich im Februar 2001, erstmals veröffentlicht.

---

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

2 Siehe Mitteilung der Europäischen Kommission an den Rat und das Europäische Parlament „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität" (angenommen am 26. Januar 2001, verfügbar unter: http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/crime1.html).

3 Siehe Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internetdienstanbieter für Strafverfolgungszwecke, angenommen am 7. September 1999. WP 25, verfügbar unter http:// europa.eu.int/comm/internal_market/de/media/dataprot/wpdocs/index.htm

An der Konvention wie an der Begründung wird weiter gearbeitet. Diese Stellungnahme betrifft lediglich den Konventionsentwurf in der Fassung vom 22. Dezember 2000 (öffentliche Fassung 25[4]), nicht die Begründung.

Die Datenschutzgruppe stellt fest, dass in vielen Bereichen Anstrengungen zur Bekämpfung der Cyberkriminalität gemacht werden, und sie unterstützt die allgemeine Zielsetzung dieser Maßnahmen, soweit sie dazu beitragen, die Sicherheit der Bürger zu erhöhen, vor allem bei der Verarbeitung personenbezogener Daten. Sie möchte indessen nachdrücklich betonen, dass mit Blick auf die Tragweite der in dem Konventionsentwurf vorgeschlagenen Maßnahmen unbedingt ein sinnvolles Gleichgewicht gefunden werden muss zwischen der Notwendigkeit, die Cyberkriminalität zu bekämpfen, und der Notwendigkeit, das Grundrecht auf Schutz der Privatsphäre und Schutz personenbezogener Daten zu wahren. Diese Rechte sind verankert in der Konvention des Europarates zum Schutz der Menschenrechte und Grundfreiheiten, der Konvention des Europarates aus dem Jahr 1981 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, der Empfehlung Nr. R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich, in der Empfehlung Nr. R (95) 4 über den Schutz personenbezogener Daten im Bereich der Telekommunikationsdienste, insbesondere der Telefondienste, des Weiteren in der EU-Grundrechtecharta, den EU-Datenschutzrichtlinien und in dem Internationalen Pakt der Vereinten Nationen aus dem Jahr 1966 über bürgerliche und politische Rechte.

Aus diesen Gründen möchte die Datenschutzgruppe folgende Bemerkungen zu dem Entwurf des Europarates für eine Konvention über Cyberkriminalität machen.

Der Konventionsentwurf

Vom Inhalt her zielt der Konventionsentwurf, was die Harmonisierung des Verfahrensrechts (Kapitel II) und internationale Rechtshilfe (Kapitel III) anbelangt, auf den Austausch personenbezogener Daten (Verkehrsdaten, Inhalte von Mitteilungen usw.) bei der internationalen Zusammenarbeit in Strafsachen, nicht nur bei der Bekämpfung der Cyberkriminalität.
Kapitel III ist der internationalen Zusammenarbeit bei Ermittlungen oder Verfahren gewidmet, die Straftaten im Zusammenhang mit Computersystemen oder Daten betreffen, bzw. der Kooperation bei der Erhebung elektronischer Beweise für eine Straftat. Die meisten der aufgeführten Rechtshilfeverpflichtungen können für alle Straftaten in Anspruch genommen werden, unabhängig davon, ob sie computerbezogen sind oder nicht. Die Verpflichtungen umfassen Rechtshilfe hinsichtlich der Auslieferung, Spontanauskünfte, die Sicherung von Computer- und Verkehrsdaten, die Weitergabe von und den Zugriff auf Computer- und Verkehrsdaten, den grenzüberschreitenden Zugriff auf gespeicherte Daten so wie die Echtzeiterhebung von Verkehrsdaten und die Überwachung des Fernmeldeverkehrs. In diesem Kapitel ist ferner die Möglichkeit der beschleunigten Übermittlung von Rechtshilfeersuchen, unter anderem durch Fax und E-Mail vorgesehen. Die förmliche Bestätigung soll nur erforderlich sein, wenn die ersuchte Partei dies verlangt.

In dem Entwurf (Kapitel II Abschnitt 2) werden die Parteien ferner aufgefordert, ihr Verfahrensrecht so zu harmonisieren, dass folgende Maßnahmen ergriffen werden

[4] Siehe http://coe.fr

können: beschleunigte Sicherung gespeicherter Computerdaten, beschleunigte Sicherung und Weitergabe von Verkehrsdaten, Verpflichtung einer Person zur Herausgabe von ihrer Kontrolle unterliegenden Computerdaten und Verpflichtung eines Dienstanbieters zur Herausgabe von seiner Kontrolle unterliegenden Abonnentendaten, Fahndung nach und Sicherstellung von gespeicherten Computerdaten, Echtzeiterhebung von Verkehrsdaten und Abfangen von Inhaltsdaten.

Was das materielle Strafrecht angeht, so werden im Konventionsentwurf (Kapitel II Abschnitt 1) die Parteien aufgefordert, bestimmte Handlungen als Straftaten einzustufen, und zwar mit allen Konsequenzen, insbesondere hinsichtlich besonderer Ermittlungsbefugnisse, wie sie normalerweise für strafrechtliche Ermittlungen gelten. Das betrifft zum Beispiel den illegalen Zugriff auf Computerdaten, das illegale Abfangen von Daten, den Missbrauch von Gegenständen wie Computerprogrammen oder Passwörtern, computerbezogene Fälschungs- und Betrugsdelikte, Straftaten im Zusammenhang mit Kinderpornographie oder Verstöße gegen das Urheberrecht und verwandte Schutzrechte. Die Datenschutzgruppe bedauert, dass der Konventionsentwurf keine Bestimmung über die Strafbarkeit der Verletzung von Datenschutzvorschriften enthält.

Menschenrechte, Privatsphäre und Datenschutz

In der Präambel des Konventionsentwurfs wird auf die Konvention des Europarates zum Schutz der Menschenrechte und Grundfreiheiten aus dem Jahr 1950 verwiesen, auf den internationalen Pakt der Vereinten Nationen über bürgerliche und politische Rechte, (in Klammern) auf die Konvention des Europarates aus dem Jahr 1981 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und (in Klammern) auf die Empfehlung Nr. R (87) 15 über die Nutzung personenbezogener Daten im Polizeibereich.

Im Konventionsentwurf werden die Garantien und Voraussetzungen, die für die geplanten Maßnahmen gelten sollen, jedoch nicht auf der Grundlage der genannten Texte harmonisiert. Obwohl es im Entwurf (Artikel 15) im Zusammenhang mit dem Verfahrensrecht heißt, „die Schaffung, Implementierung und Anwendung der Befugnisse und Verfahren, die in diesem Abschnitt (Kapitel 2 Abschnitt 2) vorgesehen sind, unterliegen den Voraussetzungen und Garantien, die im nationalen Recht der jeweils betroffenen Partei festgelegt sind", wird nicht gefordert, dass solche Garantien und Voraussetzungen tatsächlich vorhanden sind.

Die Länder des Europarates sind zur Anwendung der Menschenrechtskonvention (in der das Recht auf Schutz der Privatsphäre und Datenschutz, das Briefgeheimnis, faire Gerichtsverfahren, der Schutz gegen Bestrafung ohne gesetzliche Grundlage und die Meinungsfreiheit festgeschrieben sind und in der im Einzelnen bestimmt wird, unter welchen Bedingungen diese Rechte in klaren Vorschriften rechtmäßig beschränkt werden dürfen) so wie anderer einschlägiger Instrumente verpflichtet. In diesen Ländern müssen daher entsprechende Garantien und Voraussetzungen existieren, auch wenn sie nach Art und Umfang nicht in allen Mitgliedstaaten identisch sind. Die Konvention zur Cyberkriminalität soll aber auch von Nichtmitgliedstaaten des Europarates unterzeichnet werden; diese haben nicht die gleichen Verpflichtungen wie die Mitglieder des Europarates, und im vorliegenden Konventionsentwurf werden sie auch nicht dazu verpflichtet, entsprechende Garantien und Voraussetzungen im Einklang mit internationalen Menschenrechtsinstrumenten einzuführen.

Darüber hinaus könnte die Formulierung von Artikel 15 des Konventionsentwurfs den Eindruck erwecken, dass der Schutz der Menschenrechte nur dann zu berücksichtigen ist, wenn es geboten („due") ist, und dass dieser Schutz lediglich angemessen („adequate") sein muss. Ferner wird die Gewährleistung der Verhältnismäßigkeit von Befugnissen oder Verfahren mit Blick auf Art und Umstände der Tat nicht grundsätzlich gefordert, sondern lediglich gegebenenfalls („where applicable"). Wenn dies als Einschränkung der Garantien und Verfahren interpretiert werden könnte, würde es den Schutz der Grundrechte beträchtlich mindern, wenn nicht vollständig aushöhlen.

In Kapitel III über internationale Zusammenarbeit ist ein ähnlicher Mangel an Harmonisierung hinsichtlich Voraussetzungen und Garantien festzustellen. Einige der Verpflichtungen zur Unterstützung der ersuchenden Partei sind an Voraussetzungen und Garantien nach nationalem Recht geknüpft (Echtzeiterhebung von Verkehrsdaten und Abfangen von Inhaltsdaten)[5]. Die anderen Verpflichtungen sind keinen weiteren Voraussetzungen unterworfen. Das bedeutet, dass ein Mitglied des Europarates die Zusammenarbeit nicht verweigern könnte. Es könnte dies nur in den beiden Fällen, in denen eine Störung seiner „öffentlichen Ordnung" als Ablehnungsgrund anerkannt ist[6]. Darüber hinaus kann das Erfordernis der beiderseitigen Strafbarkeit (eine andere äußerst wichtige Garantie) nur in einer begrenzten Zahl von Fällen geltend gemacht werden[7]. Folglich soll die ersuchte Partei ganz allgemein, unabhängig von nationalen oder weitergehenden Konzepten bezüglich Garantien und Voraussetzungen, die Informationen, das Material usw. liefern, das von der anderen Partei angefordert wird. Dies ist zwar ein wünschenswertes Ziel mit Blick auf eine wirksame Rechtsdurchsetzung und Kriminalitätsbekämpfung, erfüllt aber unter Umständen nicht die Anforderungen hinsichtlich Notwendigkeit, Angemessenheit und Verhältnismäßigkeit, welche in den Rechtsinstrumenten zum Schutz der Menschenrechte, die ja in den einzelnen Ländern in verfassungsrechtliche oder sonstige Rechtsvorschriften umgesetzt wurden, vorgesehen sind.

In diesem Zusammenhang weist die Gruppe auch darauf hin, dass in dem Konventionsentwurf[8] durchweg auf „Gesetze und *sonstige Maßnahmen*" Bezug genommen wird, die die Unterzeichnerstaaten zur Umsetzung der Konvention erlassen müssen. Die Gruppe möchte den Europarat, insbesondere seine Gremien, die sich derzeit mit dem Entwurf befassen, und alle potenziellen Unterzeichner der Konvention darauf aufmerksam machen, dass diese Begriffe unter Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte ausgelegt werden müssen, wenn die darauf basierenden Maßnahmen als rechtmäßige Beschränkungen der Grundrechte und -freiheiten gelten sollen.

Eine Reihe von EU-Mitgliedstaaten wendet die Richtlinie 95/46/EG auch im Bereich der „dritten Säule" an, das heißt auf die Verarbeitung personenbezogener Daten in

---

5 Siehe Artikel 33 und 34 des Entwurfs der Konvention.

6 Siehe Artikel 27 Absatz 4 Buchstabe b, der für den Fall gilt, das keine internationalen Rechtshilfeabkommen anwendbar sind, sondern lediglich dieses Kapitel des Konventionsentwurfs. Siehe Artikel 29 Absatz 5 Buchstabe b für die beschleunigte Sicherung gespeicherter Computerdaten und Artikel 30 Absatz 2 Buchstabe b für die beschleunigte Weitergabe gesicherter Verkehrsdaten.

7 Siehe Artikel 29 Absatz 3 und 4 für die beschleunigte Sicherung gespeicherter Computerdaten und Artikel 30 für die beschleunigte Weitergabe gesicherter Verkehrsdaten.

8 Siehe Artikel 14, 16, 17, 18, 19 und 20 über die Echtzeiterhebung von Verkehrsdaten (d. h. ohne richterliche Anordnung o. Ä.), Artikel 21 über das Abfangen von Inhaltsdaten sowie Artikel 23 und 26 des Konventionsentwurfs.

Strafsachen. Nach den nationalen Rechtsvorschriften dieser Länder dürfen personenbezogene Daten daher im Prinzip nur in Drittländer übermittelt werden, wenn diese ein angemessenes Schutzniveau bei der Verarbeitung personenbezogener Daten gewährleisten. Diese Länder müssen mithin nachprüfen können, ob das Datenschutzniveau im jeweiligen Drittland angemessen ist. Ist dies nicht der Fall, kann sich die Übermittlung personenbezogener Daten dennoch als für die Kriminalitätsbekämpfung erforderlich erweisen. Unter Umständen sind im nationalen Recht für diesen Fall Ausnahmen vom Grundsatz der Angemessenheit vorgesehen. Diese Notwendigkeit zur Festlegung von Bedingungen kann auch in anderen Ländern auf Grund ihres Verfassungs- oder ihres Verfahrensrechts gegeben sein. Daher sollte in der Konvention als absolutes Minimum die Möglichkeit vorgesehen werden, beide Ziele miteinander in Einklang zu bringen, indem der ersuchten Partei erlaubt wird, spezifische Garantien und Voraussetzungen vorzuschreiben, damit die Übermittlung erfolgen kann. Sonst könnten Konflikte zwischen der Verpflichtung zur Rechtshilfe und der Verpflichtung zur Beachtung von Grundrechten, wie sie von den europäischen Instrumenten und der einschlägigen Rechtssprechung garantiert werden, entstehen.

Offenbar soll diese Frage durch Artikel 27a in Verbindung mit Artikel 27 Absatz 6 gelöst werden, es ist jedoch nicht ganz klar wie. In Artikel 27a als solchem wird der Schutz personenbezogener Daten zwar nicht ausdrücklich erwähnt, aber von "Vertraulichkeit und Beschränkung der Nutzung" von "Informationen oder Material" gesprochen. Es wird lediglich die Möglichkeit („may“, also keine Verpflichtung) vorgesehen, dass die ersuchte Partei die Lieferung von Informationen oder Material davon abhängig macht, dass die Daten vertraulich behandelt oder nur für bestimmte Zwecke verwendet werden. Gleichzeitig werden diese Möglichkeiten offenbar erheblich eingeschränkt: Wie Fußnote 48 besagt, kann die Vertraulichkeit unter Umständen nicht garantiert werden, wenn nach dem Verfahrensrecht eine Offenlegung erforderlich ist. In Fußnote 49 wird erklärt, dass Artikel 27a Artikel 27 über Rechtshilfe im Falle fehlender internationaler Vereinbarungen unberührt lässt. Artikel 27 Absatz 4 erlaubt die Verweigerung der Rechtshilfe aus verschiedenen dort genannten Gründen, beispielsweise dann, wenn die Gewährung dieser Hilfe voraussichtlich die „öffentliche Ordnung“, die Souveränität, die Sicherheit oder andere wesentliche Interessen gefährden wird. Bevor sie die Rechtshilfe ablehnt oder aufschiebt, muss die ersuchte Partei erwägen, ob dem Ersuchen teilweise oder unter bestimmten Bedingungen (Artikel 27 Absatz 6) nachgekommen werden kann. Es ist allerdings unklar, ob Datenschutzanforderungen auf diese Bestimmung gestützt werden können, denn sie ist mit den in Artikel 27 Absatz 4 genannten Ablehnungsgründen verknüpft, zu denen nicht unbedingt der Datenschutz gehört.

Die Gruppe ist der Auffassung, dass diese Bestimmungen und die darin enthaltenen Beschränkungen nicht ausreichen, um die Wahrung des Grundrechts auf Schutz der Privatsphäre und Datenschutz uneingeschränkt zu garantieren. Die Bürger sind möglicherweise nicht in der Lage, vorauszusehen, wann und wie ihre Grundrechte eingeschränkt werden. Der Konventionsentwurf sollte deshalb für alle in dem Konventionsentwurf vorgesehenen Maßnahmen zumindest Bestimmungen enthalten, die umreißen, inwieweit den Bürgern, die von diesen Maßnahmen betroffen sind, Datenschutz zu gewährleisten ist. Zudem sollte von den Unterzeichnern verlangt werden, dass sie der Konvention 108[9] des Europarats beitreten, die auch Nichtmitglieder des Europarats unterzeichnen können.

[9] Dieser Vorschlag folgt dem Schengen-Modell, bei dem die Rechtshilfe für bestimmte Zwecke und der Austausch personenbezogener Daten zwischen Polizeidienststellen vom Beitritt zur Konvention 108 und den Datenschutzbestimmungen im Schengen-Abkommen selbst abhängig gemacht wird.

Es sollte insbesondere eine Klarstellung bezüglich Artikel 27a und seiner Verbindung zu Artikel 27 Absätze 4 und 6 im Lichte des oben Gesagten erfolgen. Da die Richtlinie 95/46/EG in der Regel „nahtlos" implementiert wird, d. h. auch für die Datenverarbeitung in den unter die „dritte Säule“ fallenden Bereichen, gibt es gute Gründe, davon auszugehen, dass unter „öffentliche Ordnung“ auch Situationen eingeordnet werden können, in denen das Fehlen eines angemessenen Schutzniveaus bei der Verarbeitung personenbezogener Daten in einem ersuchenden Staat die Rechte und Freiheiten der Betroffenen gefährdet. In diesem Zusammenhang wird ausdrücklich darauf verwiesen, dass das Recht der Betroffenen auf Schutz ihrer persönlichen Daten vor kurzem in Artikel 8 der EU-Grundrechtecharta verankert worden ist. Die Gewährleistung oder das Fehlen eines angemessenen Datenschutzniveaus in einem Drittland wird auch in der Europol-Konvention als wichtiges Kriterium für die Entscheidung darüber genannt, ob und in welchem Umfang Europol personenbezogene Daten zu Strafverfolgungszwecken an ein Drittland weitergeben darf.

Zwar regelt Artikel 27a, wenn er wie vorgeschlagen klarer gefasst und abgeändert wird, unter Umständen in gewissem Umfang Fragen der Vertraulichkeit und der Begrenzung der Zweckbestimmung im Zusammenhang mit der Übermittlung personenbezogener Daten in Nichtmitgliedstaaten des Europarates und der Europäischen Union, dennoch ist die Datenschutzgruppe der Auffassung, dass die Verpflichtung eines Unterzeichners zur Einhaltung der Vorschriften des Artikels 27a nicht zwangsläufig eine hinreichende Verpflichtung zum Schutz der Privatsphäre darstellt (siehe oben). Die Einbeziehung von Datenschutzvorschriften würde dazu beitragen, die in den oben genannten Rechtsinstrumenten verlangte Prüfung der Notwendigkeit, Angemessenheit und Verhältnismäßigkeit rechtlich zu verankern und zu präzisieren.

Die Gruppe ist ferner der Ansicht, dass die Unterzeichner der Konvention die Anforderungen der Datenschutzvorschriften erfüllen müssen, bevor festgestellt werden kann, dass sie die Rechte und Freiheiten der betroffenen Personen ausreichend schützen. Ein solcher Ansatz wird dazu beitragen, die Garantien und Voraussetzungen, die für die in dem Konventionsentwurf vorgesehenen Maßnahmen gelten sollen, zu vereinheitlichen. Wenn eine Partei in einem Drittland personenbezogene Daten empfangen will, muss sie in gebührender Form die Verantwortung dafür übernehmen, dass die Grundrechte der Betroffenen angemessen geschützt werden, nachdem sie die Daten erhalten hat.

Verkehrsdaten

Die Gruppe begrüßt, dass in der neuen Fassung der Konvention (Fassung 25), anders als in den Vorfassungen, kein allgemeine Aufsichtspflicht im Form einer routinemäßigen Aufbewahrung aller Verkehrsdaten mehr vorgesehen ist. Das steht im Einklang mit der von der Datenschutzgruppe am 7. September 1999 angenommenen Empfehlung 3/99 zur Aufbewahrung von Verkehrsdaten durch Internet-Dienstanbieter für Strafverfolgungszwecke[10], in der die rechtlichen Einwände gegen eine solche allgemeine Verpflichtung dargelegt werden. [11]

Außerdem sprachen sich die EU-Datenschutzbeauftragten auf ihrer Frühjahrskonferenz im Jahr 2000 in Stockholm deutlich gegen eine solche Maßnahme aus. Sie nahmen eine

[10] Verfügbar unter http:// europa.eu/comm/internal_market/de/media/dataprot/wpdocs/index.htm

[11] Insbesondere mit Verweis auf die Richtlinie 97/66/EG.

Entschließung an, in der sie „mit Besorgnis feststellen, dass es Vorschläge gibt, laut welchen ISP routinemäßig Verkehrsdaten aufbewahren sollen über die Erfordernisse der Gebührenabrechnung hinaus, um den rechtspflegenden Behörden Zugang zu denselben zu ermöglichen. Die Konferenz betont, dass eine derartige Aufbewahrung eine unzulässige Beeinträchtigung der Grundrechte darstellt, die Personen durch Artikel 8 der Europäischen Konvention über Menschenrechte zugesichert sind. Wenn in besonderen Fällen Verkehrsdaten aufbewahrt werden sollen, muss eine beweisbare Notwendigkeit vorliegen und die Zeitdauer der Aufbewahrung muss so kurz wie möglich sein; weiterhin muss die diesbezügliche Praxis klar gesetzlich geregelt sein."

In dieser Frage nähern sich die Standpunkte einander an. Auch andere Einrichtungen und Gremien haben erhebliche Vorbehalte geltend gemacht, wie die Internationale Arbeitsgruppe Datenschutz in der Telekommunikation in ihrer gemeinsamen Stellungnahme zu Datenschutzaspekten des Konventionsentwurfs[12].

Nichtsdestoweniger bestehen hinsichtlich der im Konventionsentwurf enthaltenen Bestimmungen über Verkehrsdaten ernsthafte Bedenken: Artikel 29 und 30 über beschleunigte Sicherung und Weitergabe von Verkehrs- und anderen Daten sehen für die ersuchte Partei nicht die Möglichkeit vor, ihre Hilfe aus Datenschutzgründen zu verweigern, sondern lediglich die Möglichkeit zur Verweigerung aus denselben Gründen, die bereits oben erörtert wurden (öffentliche Ordnung usw.). Gleichzeitig stellt die Verpflichtung, gespeicherte Computer- und Verkehrsdaten mindestens 60 Tage aufzubewahren, wenn dies verlangt wird, damit entschieden werden kann, warum sie benötigt und wie sie verwendet werden sollen, für die Wirtschaft (Telekom-Betreiber, Internetdienstanbieter und alle anderen) sowie für Privatpersonen eine beträchtliche Belastung dar. Ähnliche Bedenken bestehen hinsichtlich Artikel 20, der die Serviceprovider dazu verpflichtet, im Rahmen ihrer technischen Möglichkeiten Verkehrsdaten in Echtzeit zu erheben oder aufzuzeichnen.

Allgemein braucht die Wirtschaft möglicherweise mehr Rechtssicherheit hinsichtlich ihrer Verpflichtungen und deren konkreter Umsetzung. Sie könnte befürchten, dass die Verbraucher nicht genügend Vertrauen in die angebotenen Produkte und Dienste haben, wenn keine Klarheit darüber besteht, wer wann Zugang zu vertraulichen Daten und Kommunikationen hat.

Schlussfolgerungen

Die Datenschutzgruppe betont, dass der Europarat seit vielen Jahrzehnten eine wichtige Aufgabe als erfolgreicher Verfechter der Grundrechte und -freiheiten wahrnimmt. Sie ist der Ansicht, dass der Europarat, wenn er die internationale Zusammenarbeit zur Bekämpfung der Cyberkriminalität über die Grenzen seiner Mitgliedstaaten hinaus fördern will, dem Schutz der Grundrechte und -freiheiten, insbesondere dem Recht auf Schutz der Privatsphäre und Schutz personenbezogener Daten, besondere Aufmerksamkeit schenken muss.

---

12 International Working Group on Data Protection in Telecommunications, Common Position on Data Protection aspects in the Draft Convention on Cyber-crime of the Council of Europe , angenommen auf der 28. Sitzung am 13. und 14. September 2000 in Berlin, verfügbar unter: http://www.datenschutz-berlin.de/doc/int/iwgdpt/cy_en.htm.

Die Gruppe sieht deshalb Erklärungsbedarf, was den Text der Artikel im Konventionsentwurf angeht, da die Formulierungen häufig zu vage und verwirrend sind und unter Umständen die Anforderungen an einen Text, der als Grundlage für Gesetze und zwingende Maßnahmen dienen soll, mit denen Grundrechte und -freiheiten ggf. rechtmäßig eingeschränkt werden sollen, nicht erfüllen. Erläuterungen in der Begründung sind kein Ersatz für Rechtsklarheit im Text als solchen.

Die meisten Bestimmungen des Konventionsentwurfs haben weit reichende Auswirkungen auf das Grundrecht auf Schutz der Privatsphäre und Schutz personenbezogener Daten. Wie oben dargestellt nehmen die Bestimmungen im Konventionsentwurf in gewissem Umfang das Ergebnis der Prüfung vorweg, die erfolgen muss, wenn das Recht auf Schutz der Privatsphäre (Artikel 8 Menschenrechtskonvention) und andere Grundrechte eingeschränkt werden sollen[13]. Eine der Kernfragen in diesem Zusammenhang ist die, ob eine Maßnahme in einem bestimmten Fall notwendig ist, und, wenn ja, ob sie angemessen und verhältnismäßig ist und nicht über das Notwendige hinausgeht. Einige Elemente im Konventionsentwurf sind vollkommen neu, und ihre Wirkung auf die Grundrechte, insbesondere auf das Recht auf Schutz der Privatsphäre und Datenschutz, ist unter Umständen nicht hinreichend vom Sachverständigenausschuss für Cyberkriminalität (PC-CY) geprüft worden. Die Datenschutzgruppe hält es für notwendig, die geplanten Maßnahmen hinsichtlich Notwendigkeit, Angemessenheit und Verhältnismäßigkeit besser zu begründen, wie das in den genannten Instrumenten zum Schutz der Menschenrechte und zum Datenschutz gefordert wird.

Die Gruppe empfiehlt nachdrücklich, in jedem Falle in den Konventionsentwurf Datenschutzbestimmungen aufzunehmen, die umreißen, inwieweit Personen geschützt werden müssen, die von den Informationen betroffen sind, die verarbeitet werden sollen, und zwar im Zusammenhang mit allen im Konventionsentwurf vorgesehenen Maßnahmen. Artikel 27a sollte auch einbezogen (d. h. Klammern streichen) und wie ausgeführt nachgebessert werden. Die Einbeziehung von Datenschutzvorschriften wird dazu beitragen, dass die Anforderungen hinsichtlich Notwendigkeit, Angemessenheit und Verhältnismäßigkeit, die sich aus den Rechtsinstrumenten („*aquis*“) des Europarats und der EU-Mitgliedstaaten ergeben, rechtlich verankert und präzisiert werden.

Die Gruppe ist des Weiteren der Auffassung, dass die Bezugnahme auf die Konvention 108 in die Präambel aufgenommen werden sollte (die Klammern wären dementsprechend zu streichen), obwohl dies keine bindende Wirkung hat, und dass die Unterzeichner der Konvention zur Cyberkriminalität aufgefordert werden sollten, der Konvention 108 über den Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten beizutreten.

Die Datenschutzgruppe bedauert auch, dass der Konventionsentwurf keine Bestimmung über die Strafbarkeit der Verletzung von Datenschutzvorschriften enthält.

Die Gruppe sieht eine Diskrepanz zwischen Ländern, die Mitglied des Europarates sind, und solchen, die es nicht sind, denn die Mitglieder des Europarats müssen ihren Verpflichtungen aus der Europäischen Menschenrechtskonvention, der Konvention 108, den einschlägigen Empfehlungen des Europarats, der EU-Grundrechtecharta, den EU-Datenschutzrichtlinien und ihren einzelstaatlichen Rechtsvorschriften nachkommen,

[13] Das Abfangen von Kommunikationen und Verkehrsdaten zum Beispiel verletzt eindeutig das Briefgeheimnis (siehe Urteil des Europäischen Gerichtshofs für Menschenrechte im Fall Malone).

während den Nicht-Europaratsmitgliedern aus dem Konventionsentwurf in seiner jetzigen Fassung nicht dieselben oder vergleichbare Verpflichtungen erwachsen.

Die Gruppe ist zudem der Ansicht, dass die Unterzeichner der Konvention in gebührender Form die Verantwortung dafür übernehmen müssen, dass die Grundrechte der Betroffenen angemessen geschützt werden, nachdem sie deren Daten aus der Europäischen Union und den Mitgliedstaaten des Europarats erhalten haben.

Der Konventionsentwurf in seiner derzeitigen Fassung (öffentliche Fassung 25) verpflichtet die Unterzeichner nicht, die Dienstanbieter zur Aufbewahrung von Verkehrsdaten für alle Kommunikationen zu zwingen; diese derzeit vertretene Position sollte auf keinen Fall aufgegeben werden.

Die Gruppe bedauert, dass relevante Unterlagen erst sehr spät zugänglich gemacht wurden. Sie hält es für in hohem Maße wünschenswert, dass zunächst die öffentliche Diskussion weitergeführt und alle Betroffenen (Menschenrechtsorganisationen, Wirtschaft u. a.) darin einbezogen werden, bevor die Parlamentarische Versammlung des Europarates über den Entwurf diskutiert und entscheidet.

Die Datenschutzgruppe ist der Meinung, dass etliche der in dieser Stellungnahme aufgezeigten Schwächen, darauf zurückzuführen sein dürften, dass der Europarat das verfügbare Fachwissen auf dem Gebiet des Datenschutzes nicht optimal genutzt hat. Die Gruppe fordert den Europarat, und insbesondere die EU-Mitgliedstaaten daher auf, die Meinung ihrer Datenschutzexperten einzuholen, bevor sie endgültig zu dem Konventionsentwurf Stellung nehmen, und ihre Beiträge optimal zu nutzen
Die Datenschutzgruppe fordert den Europarat, die Europäische Kommission, das Europäische Parlament und die Mitgliedstaaten auf, diese Stellungnahme zu berücksichtigen.

Die Gruppe behält sich weitere Stellungnahmen vor.

Geschehen zu Brüssel am 26. Januar 2001

Für die Datenschutzgruppe

Der Vorsitzende

Stefano RODOTA