Thomas J. Primig

Verfahrensrechtliche Regelungsversuche der Telekommunikationsüberwachung auf europäischer Ebene

Verfahrensrechtliche Regelungsversuche der Telekommunikationsüberwachung auf europäischer Ebene

Die Bestrebungen Gesetze, Verordnungen oder sonstige Regelungen zu beschließen, welche die rechtlichen und technischen Voraussetzungen für eine umfangreiche und beinahe lückenlose Überwachung der Telekommunikation schaffen, gründen sich nicht etwa auf Eigeninitiativen des österreichischen, bzw deutschen Gesetzgebers, sondern sind nur der Abschluß einer Entwicklung, welche ihren Anfang auf internationaler und europäischer Ebene schon vor zwei Jahrzehnten genommen hat.

Vor einigen Jahren noch als Schreckgespenst eingefleischter Verschwörungstheoretiker abgetan, ist aufgrund der aktuellen Entwicklung ein durchaus seriöser Standpunkt, beispielsweise zum jahrzehntelang verleugneten weltumspannenden Abhör- und Lauschsystem „ECHELON“, einzunehmen. Häufig öffnete die Grauzone zwischen bürokratischer Ineffizienz und Geheimnistuerei auf staatlicher Seite den Raum für Verschwörungstheorien. Als anderes Beispiel dafür soll das kürzlich vom FBI[1] vorgestellte Überwachungssystem „DCS1000“ alias „Carnivore“[2] dienen: „Carnivore“[3] sollte nach Auskunft des FBI nichts anderes machen als das, was jeder Router eines Providers sowieso tut: Sich ein Datenpaket ansehen, bestimmen, welcher Typ von Paket es ist, woher es kommt und wohin es geht.[4] Also eigentlich ein überflüssiges Gerät. Beide möglichen Folgerungen aus der Existenz von Carnivore „begünstigten damit libertäre Vorstellungen: Diejenige von Redundanz durch bürokratische Ineffizienz und

---

[1] „Federal Bureau of Investigation”.

[2] *http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm.*

[3] Zu den technischen Details vgl *Sober*, Independent Technical Review of the Carnivore System, im Internet unter *http://www.epic.org/privacy/carnivore/review_comments.html.*

[4] Dabei wird ein PC mit der Software vom FBI bei dem Provider eines Verdächtigen installiert und direkt mit dessen Servern verbunden. Um die Emails von und an den Verdächtigen herauszufischen, muß das System allerdings alle beim Provider ein- und ausgehenden Emails überprüfen. Angeblich könne Carnivore Millionen von Emails in einer Sekunde überprüfen. Wird eine Email von oder an den Verdächtigen gefunden, dann wird der Text der Email kopiert und gespeichert. Täglich werden die Daten aus dem, sich meist abgesperrt beim Provider befindlichen, Computer herausgelesen und analysiert.

Verschwendung von Steuergeldern, wie auch die von Verschwörungstheorien, die bis zur Vermutung der möglichen Abschaltung des Internets durch verborgene „Carnivore"-Features gingen"[5].

Den Zusammenhang zwischen ECHELON und den verschiedenen Reglementierungsversuchen der Telekommunikationsüberwachung auf europäischer Ebene darzustellen, soll im Folgenden die Aufgabe sein.

1. ECHELON – Das weltumspannende polizeiliche Abhörsystem[6]

Das staatliche Echelon-System[7] ist ein Netzwerk von elektronischen Spionage-Stationen zur Überwachung der weltweiten Kommunikation, das es in der heutigen Form seit dem Beginn der 90er Jahre gibt. Die Entwicklung dieses Überwachungssystems begann jedoch bereits in den 70er Jahren durch den US-amerikanischen Geheimdienst „*National Security Agency*" (NSA). Echelon wird von Auslandgeheimdiensten der Länder Großbritannien, Kanada, Australien und Neuseeland, sowie des „CIA"[8], unter der Führung der NSA betrieben.[9] Die

---

[5] *Mühlbauer*, Verschwörungstheorien und die Arroganz der Macht, Telepolis, das Magazin für Netzkultur vom 12.09.2001 unter *http://www.heise.de/tp/deutsch/special/libi/9515/1.html.*

[6] Siehe dazu die exzellent recherchierte „Echelon" Artikelreihe in *Telepolis* unter *http://www.heise.de/tp/deutsch/special/ech/*, bzw *Schulzki/Haddouti*, Vom Ende der Anonymität - Die Globalisierung der Überwachung[2] (2001).

[7] Zahlreiche Web-Pages haben sich im Internet dieses Themas angenommen; vor allem für jene Organisationen, die den Datenschutz - teilweise bis ins Extreme – zu forcieren suchen, bietet sich das Internet als Plattform an, um effizient und umfangreich – wenn auch ein wenig einseitig – über die Problematik zu informieren. Als Beispiele seien hier etwa die Homepages vom „Büro für den Gegeninformationsaustausch" (*http://gib.squat.net/echelon*) oder von „Allgemeiner Datenschutz.de" (*http://www.allgemeiner-datenschutz.de/echelon*) genannt. Kritische und umfangreiche Informationen zum Thema „ECHELON" finden sich – wie so oft – auf den Web-Seiten des „Heise-Verlags" *(http://www.heise.de*), der Zeitschrift „Der Spiegel" (*http://www.spiegel.de/netzwelt*) oder des „Österreichischen Rundfunks" (*http://futurezone.orf.at*). Das Online-Magazin „Telepolis" hat diesem Thema eine ganze Serie von Beiträgen gewidmet, welche wohl als die umfassendste deutschsprachige Linksammlung im gesamten WWW gelten (*http://www.heise.de/tp/deutsch/special/ech/default.html*).

[8] „Central Intelligence Agency" (*http://www.cia.gov*).

[9] „ECHELON - Weltweites Überwachungssystem, Referat der „AG Öffentliche Räume beim BGR" auf der Veranstaltung „Überwachung in der heutigen Gesellschaft" am 25.02.2000 in Leipzig, im Internet unter *http://www.nadir.org/nadir/initiativ/infoladen_leipzig/camera/text008.htm.*

Überwachung der Kommunikations- und Datennetze wird durch die Zusammenschaltung von Computersystemen mit den derzeit europaweit in Aufbau befindlichen sicherheitspolizeilichen Datenbanken und -Netzen ermöglicht.[10] Das Abhörsystem wurde errichtet, um Informationen abzufangen und sie an andere weiterzugeben. Dieser Vorgang vollzieht sich in drei Schritten, nämlich der Sammlung aller nur möglicher Informationen, ihrer Analyse und der Suche nach dem entsprechenden Kontext, sowie der Verteilung von Zuständigkeiten. Hauptquelle für Rohinformationen sind elektronische Signale. Diese werden von Radiowellen, in Kupferleitungen, oder mit Glasfaserkabeln transportiert.[11] Bereits heute würden in Europa laut Statewatch[12] alle E-Mails, Telefon- und Faxverbindungen routinemäßig von diesen Nachrichtendiensten abgehört.

Enttarnt und erstmals öffentlich bei seinem Namen genannt wurde Echelon schließlich im Jahre 1996.[13] Jahrzehntelang verleugnet, wurde von Seiten der australischen Regierung aber erst im Mai 1999 zugegeben, daß vom Satellitenkontrollzentrum „Pine Gap“ in der Nähe von Alice Springs seit mehr als 30 Jahren die Abhörsatelliten der CIA, genannt „Rhyolite“, „Aquacade“ und „Magnum“, kontrolliert werden. Nach Jahren der Kontroverse behauptete die australische Regierung schließlich, die volle Kontrolle über die Abhöranlage zu haben.[14] Seitdem aber bekannt wurde, daß Echelon eventuell auch benutzt werden könnte, um US-Bürger auszuhorchen, wurde das Überwachungssystem, dessen Existenz von US-Behörden bislang bestritten wurde, immer mehr zu einem innenpolitischen Thema. Mit der Eröffnung der Website

---

[10] *Lindau*, Das Enfopol-Komplott, im Internet unter *http://members.eunet.at/hochhaltinger/lindau_1.htm.*

[11] *Goodwins*, Wie funktioniert Echelon, ZDNet News-Report unter *http://www.zdnet.de/news/report/echelon/funktion_00-wc.html.*

[12] Statewatch - monitoring the state and civil liberties in the European Union; britische Bürgerrechtsgruppe, im Internet unter *http://www.statewatch.org*.

[13] „The global system has a highly secret codename - ECHELON. It is by far the most significant system of which the GCSB („Government Communications Security Bureau”, Anm) is a part, and many of the GCSB's daily operations are based around it. The intelligence agencies will be shocked to see it named and described for the first time in print.” Zitat aus *Hager*, Secret Power - New Zealand's Role in the International Spy Network (1996) Chapter Two – Exposing the Global Surveillance System 4 (im Internet unter *http://www.fas.org/irp/eprint/sp/sp_c2.htm*).

[14] *Campbell*, Existenz von Echelon erstmals offiziell bestätigt, Telepolis, das Magazin für Netzkultur vom 28.05.1999 unter *http://www.heise.de/tp/deutsch/special/ech/6639/1.html*.

„Echelonwatch“[15] im November 1999 warf die „*American Civil Liberties Union*“ (ACLU), die älteste und größte US-Bürgerrechtsorganisation, ihr volles politisches Gewicht in die Echelon-Debatte.[16] Erstmals in einem offiziellen Dokument,[17] welches aufgrund des Erlasses des „Freedom of Information Act“[18] der Öffentlichkeit vorgestellt wurde, wurde Echelon im Januar 2000 erwähnt.
Mittlerweile ist die Existenz von sieben Abhörstationen in den USA und Kanada, einer auf Hawaii, zwei in Asien und fünf Stationen in Australien bekannt. Für Europa gelten die Posten „Menwith Hill“ und „Morwenstow“ in England als bestätigt, in Deutschland wird in „Bad Aiblingen“ eine Abhörstation vermutet.[19]

Nach heftigen Debatten, welche vor allem von der deutschen „Grünen Partei“[20] angeführt wurden, beschloß das Europäische Parlament gemäß Artikel 150 Abs 2 seiner Geschäftsordnung in der Sitzung vom 5.07.2000 die Einsetzung eines nichtständigen Ausschusses über das Abhörsystem Echelon. Dieser legte schließlich am 11.07.2001 einen umfangreichen, beinahe 200 Seiten starken Bericht[21] vor, in dem festgestellt wird, daß „an der Existenz eines weltweit arbeitenden Kommunikationsabhörsystems, das durch anteiliges Zusammenwirken der USA, des Vereinigten Königreichs, Kanadas, Australiens und Neuseelands...funktioniert, nicht mehr gezweifelt werden (kann). Daß das System oder Teile davon, zumindest für einige Zeit, den Decknamen Echelon trugen, (könne) aufgrund vorliegender Indizien und zahlreicher übereinstimmender Erklärungen aus sehr unterschiedlichen Kreisen - einschließlich amerikanischer Quellen

---

[15] *http://www.echelonwatch.org* enthält, neben den wichtigsten Dokumenten und Links zu Ressourcen, auch einen Aufruf, sich als US-Bürger an den US-Kongress mit der Bitte um Aufklärung zu wenden.

[16] *Medosch*, Echelon wird nun überwacht, Telepolis, das Magazin für Netzkultur vom 17.11.1999 unter *http://www.heise.de/tp/deutsch/special/ech/6648/1.html*.

[17] *http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/09-03.htm.*

[18] Dieses Dokument kann unter *http://www.foia.state.gov/vstateSearch.asp* eingesehen werden.

[19] Siehe dazu das Schaubild auf der Homepage „Spiegel Online“ unter *http://www.spiegel.de/netzwelt/politik/0,1518,139443,00.html.*

[20] Vgl *Schulzki-Haddouti*, Echelon vor dem Europaparlament, Telepolis, das Magazin für Netzkultur vom 08.02.2000 unter *http://www.heise.de/tp/deutsch/special/ech/6645/1.html.*

[21] „Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), A5-0264/2001“, im Internet unter *http://www.dud.de/dud/documents/echelon-bericht010711.zip*.

- angenommen werden. Wichtig (sei) festzuhalten, daß das System nicht zum Abhören militärischer, sondern privater und wirtschaftlicher Kommunikation dient".[22]

Am 05. September 2001 stellte Gerhard *Schmid*, Berichterstatter des nicht ständigen EU-Untersuchungsausschusses zu Echelon, seinen Bericht[23] im EU-Parlament zur Abstimmung. In seiner Rede bestätigte er zwar die Existenz des Abhörsystems, hielt aber gleichermaßen fest, daß „es kein von Geheimdiensten gleich welchen Staates betriebenes Abwehrsystem, mit dem jedwede Kommunikation in Europa abgehört werden kann, (gibt)." Diese Behauptung gehöre in das Reich des „kreativen Journalismus", denn „die Telekommunikation gehorcht den Gesetzen der Physik, und wo es keinen Zugang zu Trägern der Kommunikation gibt, kann man auch nicht abhören und es gibt keine magische Sonderphysik für Geheimdienste." Das Parlament segnete den Bericht mit einer Zwei-Drittel-Mehrheit ab. Mit dieser Rede wurde die Existenz von Echelon amtlich untermauert.

2. „ENFOPOL" oder die rechtliche Reglementierung des ECHELON-Konzeptes

Den Namen *Enfopol*[24] tragen Dokumente der Europäischen Union, welche die „Dritte Säule" der Europäischen Gemeinschaft, also die polizeiliche Zusammenarbeit, betreffen. Seit Mitte der neunziger Jahre wurden etliche Enfopol-Dokumente erarbeitet und teilweise auch verabschiedet, die eine gemeinsame europäische Richtung bezüglich der polizeilichen Überwachung von Telekommunikation festlegen sollten. Dabei handelt es sich sowohl um Richtlinien für das nationale Prozedere bei Abhöraktionen, also um Aufbau und rechtliche Legitimation einer überwachungsfreundlichen Infrastruktur auf Seiten der Netzwerkbetreiber und Diensteanbieter, als auch um staatenübergreifende Zusammenarbeit und Rechtshilfe.

---

[22] Vgl Pkt 13.1 des Berichts (FN 21) 140.

[23] Die Rede ist im Volltext vom „Spiegel-Online"-Server unter *http://www.spiegel.de/netzwelt/politik/0,1518,155819,00.html* abrufbar.

[24] „Enforcement Police".

2.1. „TREVI" und Enfopol

Die Anfänge dieser geheim- und nachrichtendienstlichen Praxis stammen aus der Zeit des Kalten Krieges. Die Pläne zur globalen Überwachung entstanden 1991 im Rahmen einer „TREVI"-Konferenz[25] der EG-Minister und wurden im November 1993 in Madrid konkretisiert.[26] Ziel dieser „TREVI"-Kooperation war zunächst die gemeinsame Terrorismusbekämpfung durch Austausch von Informationen und technischen Erfahrungen der beteiligten Polizeibeamten. Im Laufe der Jahre kam es zu einer immer enger werdenden polizeilichen Zusammenarbeit, da stetig mehr innenpolitische Sachbereiche in diese Kooperation eingeschlossen wurden.
Diese mit den Mitgliedsstaaten der EU abgestimmte Koordinationsorganisation erwies sich bislang als ein effektives Instrument der Zusammenarbeit, ist jedoch wegen ihrer geheimen und damit der öffentlichen Kontrolle weitgehend entzogenen Arbeitsweise schon oftmals kritisiert worden.[27]

Ende November 1993 wurde in Brüssel beim ersten Treffen des neuen Rates der Innen- und Justizminister der Beschluß über das Abhören von Telefoneinrichtungen angenommen. EU und FBI setzten eine Expertengruppe ein, um die unterschiedlichen Systeme zwischen den USA und Europa aufeinander abzustimmen[28] und die europäischen Kommunikationssysteme aus praktischen Gründen in die bestehenden Abhörsysteme (Echelon) einzubinden.[29] Die EU-FBI-Initiative kam zum Ergebnis, daß die klassische Kontrolle traditioneller Kommunikationssysteme mit der Liberalisierung der Telekommunikation nicht mehr möglich sei. Daraus ergäbe sich die Notwendigkeit

---

[25] TREVI leitet sich aus den Anfangsbuchstaben Terrorism, Radicalism, Extremism und Violence ab. (So die weitläufigste Meinung; wahrscheinlich jedoch prägte diese Bezeichnung der Tagungsort der Minister, nämlich ein Gebäude in der Nähe der „Fontana die Trevi" in Rom – vgl *Jarzembowski/Malangre*, Die Europäische Gemeinschaft ohne Binnengrenzen, in: Europa als Auftrag (1993) 12).

[26] „*A study should be made of the effects of legal, technical and market developments within the telecommunications sector on the different interception possibilities and of what action should be taken to counter the problems that have become apparent*".

[27] Vgl *Sule*, Europol und europäischer Datenschutz (1999) 21 mwN.

[28] Bekannt wurde dies durch einen Report der Online-Datenschutzorganisation „Statewatch". Der Bericht ist im Volltext unter *http://www.privacy.org/pi/activities/tapping/statewatch_tap_297.html* abrufbar.

[29] Vgl „Das überwachte Büro - Nachrichtendienste hören mit", Datagraph 2/1998, im Internet unter *http://members.aon.at/datagraph/1998/98-1&2/4wach.htm.*

der Verankerung von Abhörmethoden und -techniken in den Rechtsnormen jener Länder, in welchen die Telekommunikation liberalisiert wird, die Verpflichtung für private Kommunikationsanbieter, ihre Systeme für uneingeschränkte Abhörmaßnahmen zu adaptieren, die Sicherstellung, daß Telefonanbieter immer und jederzeit mit Polizei und Staatspolizei (internal security) kooperieren, und schließlich auch die Pflicht zur Weiterentwicklung jener Technologien, die das Abhören von jedem Punkt der Welt aus ermöglichen, und so viele Länder wie möglich („as many countries as possible“[30]) zur Unterzeichnung dieser Vereinbarungen zu bewegen.
Länder, die nicht bereit seien, diese Bedingungen zu akzeptieren, würden gegen ihren Willen überwacht werden, da die Abhörtechnik bereits in den ausgelieferten Kommunikationssystemen installiert sei.[31]

2.2. Die Enfopol-Papiere[32]

In den Enfopol-Papieren geht es prinzipiell darum, das bereits existierende Echelon-Überwachungssystem schrittweise der Legalisierung zuzuführen. Eine große Rolle spielt dabei die Entwicklung standardisierter Schnittstellen und die Einigung auf EU-weit gültige Technologiestandards.[33] Wenn man sich die österreichische Überwachungsverordnung oder aber auch die deutsche TKUEV ansieht, verwundert es also nicht, daß beide dasselbe Ziel verfolgen, nämlich die Realisierung der in den Enfopol Papieren beschriebenen gemeinsamen Überwachungs-Schnittstellen und die Harmonisierung der technischen Gegebenheiten im Hinblick auf den ETSI-Standard, welcher ja wiederum Voraussetzung für die Effizienz des Echelon-Systems ist.

---

[30] Vgl den EU-Bericht vom 06.01.1998 („An Appraisal of Technologies of Political Control“), PE 166 499.

[31] *Lindau*, Das Enfopol-Komplott (Teil1), im Internet unter *http://members.eunet.at/hochhaltinger/lindau_1.htm.*

[32] Alle veröffentlichten „Enfopol“-Dokumente sind im englischen Originaltext unter *http://www.statewatch.org/eufbi/ abrufbar*.

[33] Vgl *Schulzki-Haddouti*, Enfopol legalisiert Echelon, Telepolis, das Magazin für Netzkultur vom 25.11.1998 unter *http://www.heise.de/tp/deutsch/special/enfo/6324/1.html.*

2.2.1. Die „International User Requirements“ (IUR)

Es war die Bürgerrechtsorganisation „Statewatch“[34], welche im Februar des Jahres 1998 die Existenz eines solchen Dokuments, dem sog „*Memorandum of Understanding*“[35] nachweislich bestätigte. Obwohl von allen EU-Staaten unterzeichnet, wurde es jedoch bis zum heutigen Tage geheimgehalten.[36] Kern des „Memorandums of Understanding“ sind die technischen Anforderungen der - innerstaatlich gesetzlich ermächtigten - Überwachungsbehörden an Netzbetreiber und Diensteanbieter bei der - innerstaatlich gesetzlich geregelten - Überwachung des Telekommunikationsverkehrs, sowie Begriffsbestimmungen im sogenannten Glossar, wie sie textgleich auch in der Ratsentschließung „*Enfopol 95*“ übernommen wurden.[37]

Bei „Enfopol 95“ handelt es sich um das erste offizielle „Enfopol“-Dokument, welches am 17.01.1995 vom Rat der Europäischen Union verabschiedet wurde. Die „*Council Resolution on the lawful interception of telecommunications*“[38], auch bezeichnet als „*International User Requirements*“, beschreibt die Anforderungen der „*Law Enforcement Agencies*“ - der behördlichen Stellen, die vom Gesetz her ermächtigt sind, Telekommunikation zu überwachen - an „*Network Operators*“ und *Service Provider*.

---

[34] http://www.statewatch.org.

[35] „ENFOPOL 112 10037/95“ vom 25.10.95, ein geheimgehaltenes bzw niemals offiziell publiziertes Dokument. Das „Memorandum of Understanding“ wurde zwar am 23.11.1995 von den Mitgliedstaaten der EU und von Norwegen unterzeichnet, nicht aber von anderen Drittstaaten. Von den USA, Australien und Kanada langten lediglich schriftliche Informationen ein, daß sie die innerstaatliche Umsetzung in ihren Ländern in die Wege leiten würden.

[36] *Wright* (An Appraisal of Technologies of Political Control (1998), im Internet unter *http://www.a42.de/archiv/echelon.clc.html*) führt dazu aus: „According to a Guardian report (25.02.97) it reflects concern among European Intelligence agencies that modern technology will prevent them from tapping private communications. EU countries should agree on international interception standards set at a level that would ensure encoding or scrambled words can be broken down by government agencies”.

[37] Vgl die „Anfragebeantwortung durch den Bundesminister für Inneres Mag. Karl *Schlögl* zur Dringlichen Anfrage (5225/J 20. GP) der Abgeordneten *Van der Bellen*, Freundinnen und Freunde an den Bundesminister für Inneres betreffend Überwachungsbefugnisse der Sicherheitsbehörden“, 4739/AB 20. GP Antwort zu Frage 27.

[38] „The 1995 „Requirements”, 17 January 1995: Council Resolution on the lawful interception of telecommunications”, erstmals veröffentlicht in: Abl. C 329 v 04.11.1996, 1. Das Dokument ist auch unter den Namen „ENFOPOL 95“, „ENFOPOL 150“ oder „International User Requirements (IUR)“ bekannt.

Die Wurzeln dieses Dokuments gehen bis ins Jahr 1993 zurück, wo sich im ersten einer ganzen Reihe von „Law Enforcement Telecom Seminars“ die Nachrichtendienste und die Polizei der Echelon-Betreiber USA, England, Kanada und Japan mit den wichtigsten EU-Staaten auf ein gemeinsames Vorgehen einigten. Bei weiteren geheimen Treffen 1994 in Bonn und 1995 in Canberra wurde das Vorgehen bereits mit den Vertretern aller EU-Staaten abgesprochen und die „Abhörstandards“ in „*International User Requirements*“ umbenannt, welche bereits im Jahr 1994 den US-Kongreß passierten. Zum EU-Ratsbeschluß wurden sie erhoben, indem sie – am EU-Parlament vorbei – durch den Fischereiausschuß „geschleust“ wurden.[39]

Von den Betreibern der technischen Infrastruktur und den Anbietern von Netzdienstleistungen wurde gefordert, im Falle einer vom Gesetz gedeckten Abhöraktion, den ermittelnden Behörden direkten Zugriff auf alle Daten der Telekommunikation, wie zB. Telefon und E-Mail, zu ermöglichen. In dem Dokument[40] heißt es:

> 1. The Council notes that the requirements of Member States to enable them to conduct the *lawful interception of telecommunications*, annexed to this Resolution („the Requirements”), constitute an important summary of the needs of the competent authorities for the technical implementation of legally authorized interception in modern telecommunications systems.
>
> 2. The Council considers that the aforementioned Requirements should be taken into account in the definition and implementation of measures which may affect the legally authorized *interception of telecommunications* and requests Member States to call upon the Ministers responsible for telecommunications to support this view and to cooperate with the Ministers responsible for justice and Home Affairs with the aim of implementing the Requirements in relation to network operators and service providers.

Im „Annex“ heißt es dann unmißverständlich, daß neben dem gesamten Inhalt einer Telekommunikation auch die Verbindungs- und Vermittlungsdaten einer Überwachung

---

[39] Siehe dazu detailliert *Moechel*, Die ETSI Dossiers – Europäische Standards für das Abhören digitaler Netze, c’t 7/2001, 59 f.

[40] „Enfopol 95“ ist im Internet beispielsweise unter *http://www.privacy.org/pi/activities/tapping/eu_tap_resolution_1995.html* abrufbar.

zugänglich gemacht werden sollen. Auch die Verpflichtung zur Einrichtung einer - in Österreich nun durch die Überwachungsverordnung definierten - technischen Schnittstelle findet sich in dem Papier, ebenso wie eine Aufforderung an die Internet Provider, verschlüsselt übertragene Dateien den Behörden „en clair“ zu übermitteln:

- Law enforcement agencies require *access to the entire telecommunications transmitted, or caused to be transmitted*, to and from the number or other identifier of the target service used by the interception subject.
- Law enforcement agencies also require *access to the call-associated data* that are generated to process the call. Law enforcement agencies require *information on the most accurate geographical location* known to the network for mobile subscribers.
- Law enforcement agencies require a *real-time, fulltime monitoring capability for the interception of telecommunications.*
- Law enforcement agencies require network operators/service providers to provide one or several *interfaces from which the intercepted communications can be transmitted to the law enforcement monitoring facility*.
- If network operators/service providers initiate *encoding, compression or encryption* of telecommunications traffic, law enforcement agencies require the network operators/service providers to *provide intercepted communications en clair*.

2.2.2. „Enfopol 98“

Aufgrund neuerer technischen Entwicklungen im Bereich des Internet und der Telekommunikation wurden im Jahre 1998 von einer dafür eingesetzten Expertengruppe Ergänzungen vorgenommen, die bestehenden „Requirements“ auf neue Technologien ausgedehnt und diese schließlich im Dokument „Enfopol 98“[41] der

[41] „Entwurf einer Ratsentschließung bezüglich der Überwachung des Telekommunikationsverkehrs betreffend erläuternder Memoranden, ergänzenden Anforderungen und Begriffsbestimmungen in bezug auf neue Technologien wie S-PCS, Internet, Bereitstellung von teilnehmer- und verbindungsrelevanten Daten, Kryptographie und Sicherheitsmaßnahmen bei Netzbetreibern/Diensteanbietern“ vom 03.09.1998, GZ 10951/98.

Öffentlichkeit präsentiert. Dem Diskussionspapier „Enfopol 87“[42] folgend, beschreibt das 42 Seiten starke Dokument[43] sehr detailliert die Voraussetzungen, die gegeben sein müssen, um eine Überwachung der Telekommunikation zu gewährleisten. Im Anhang dieses „Entwurfs einer Entschließung des Rates der Europäischen Union“ finden sich, untergliedert in 10 Teile, die Anforderungen, welche für die Überwachung von öffentlichen, auf IP basierenden (Internet)-Diensten, wie beispielsweise

- Einwähldienste
- über HFC-Kabel angeschlossene Dienste
- über Satellit gelieferte Dienste
- direkt angeschlossene Dienste, zB LAN 's, die über einen Router angeschlossen sind,

notwendig sind:

- Die gesetzlich ermächtigten Behörden benötigen Zugriff auf den gesamten Fernmeldeverkehr, der von der Rufnummer oder sonstigen Kennung des überwachten Telekommunikationsdienstes, die die überwachte Person in Anspruch nimmt, übertragen wird (oder für die Übertragung generiert wird) bzw dort ankommt. Die gesetzlich ermächtigten Behörden benötigen ferner Zugriff auf verbindungsrelevante Daten, die zur Verarbeitung des Anrufs generiert werden[44]

Einbezogen in die Überwachung soll also, neben den Fällen der Sprachtelephonie, *jede Form von Internet-Kommunikation* werden, unabhängig davon, ob jetzt beispielsweise über Modem, Kabel oder Satellit eine Verbindung hergestellt wird.
Im Zusammenhang mit dem Internet versteht man unter „Fernmeldeverkehr“ zum und vom Zieldienst auch E-Mails, die in einem E-Mail-Server zur späteren Abholung durch das Überwachungssubjekt deponiert werden, sowie dieselbe E-Mail, wenn sie vom Überwachungssubjekt abgeholt wird. Der Begriff umfaßt auch den Telekommunikationsverkehr zwischen dem Überwachungssubjekt und dem Internet Service Provider:

---

[42] „Draft Joint Action on the interception of telecommunications - Discussion paper” vom 03.07.1998, 10102/98. Dieses Diskussionspapier ging „Enfopol 98“ voran, ursprünglich mit dem Zweck, die „Reqirements“ aus 1995 rechtsverbindlich zu erlassen.

[43] Eine HTML-Version des Originaldokuments kann unter *http://www.heise.de/tp/deutsch/special/enfo/6326/1.html abgerufen* werden

[44] Anforderungen Pkt 1.

Die gesetzlich ermächtigten Behörden benötigen Zugriff auf die folgenden verbindungsrelevanten Daten:[45]

- Nummer des gerufenen Teilnehmers bei abgehenden Verbindungen, selbst wenn es nicht zum Aufbau einer Verbindung kommt
- Nummer des rufenden Teilnehmers bei ankommenden Verbindungen, wenn es nicht zum Aufbau einer Verbindung kommt
- Alle von der überwachten Einrichtung erzeugten Signale, einschließlich der nach Aufbau der Verbindung erzeugten Signale, mit denen Funktionen wie beispielsweise Konferenzschaltung und Anrufumleitung aktiviert werden
- Beginn, Ende und Dauer der Verbindung
- Tatsächliche Zielrufnummer und zwischengeschaltene Rufnummer, falls der Anruf weitergeschaltet wurde.

Auch die Art der Verbindung (Einwählen, LAN, Satellit, Kabel, etc), die Übertragungsgeschwindigkeit in beide Richtungen, wie auch Informationen, die sich auf die vom Überwachungssubjekt verwendeten E-Mail-Server beziehen, sollen Bestandteil der Überwachung sein (Pkt 1.6.). Der Anrufinhalt soll den Strafverfolgungsbehörden in Echtzeit geliefert werden. Die verbindungsrelevanten Daten sollen innerhalb von Millisekunden nach dem Anrufereignis, statt erst nach dem Anrufende, verfügbar sein (Pkt 2.), wobei jedoch „im Zusammenhang mit dem Internet ein Hinweis auf verbindungsrelevante Daten nicht anwendbar“ sei. Punkt 3 der Anforderungen enthält Details zur Verpflichtung von Telekom-Anbietern, Schnittstellen einzurichten, welche eine Überwachung ermöglichen,[46] wobei allerdings für die Bereiche des Internet-Traffic etliche Ausnahmen bestehen. Kurios mutet dagegen die Bestimmung an, daß „(es) die Aufgabe der überwachenden Behörde (sei), Nachrichten aus dem erhaltenen Produkt *zu extrahieren*, wenn ein Ziel durch *Verschlüsselung* oder durch Anwendung anderer Verfahren modifiziert (ist)“ (Pkt 3.3.). Dies wird wohl mit den technischen Mitteln, die den österreichischen Sicherheitsbehörden zur Auswertung der durch die Überwachung gewonnenen Daten zur Verfügung stehen – abhängig von der Verschlüsselungsmethode - auch in naher Zukunft nur schwer zu bewerkstelligen sein.

Sollen wirklich alle *via Internet* übertragenen Daten permanent überwacht werden, so resultiert daraus natürlich eine Beeinträchtigung der Übertragungsgeschwindigkeit.

---

[45] Vgl Anforderungen Pkt 1.4. bis Pkt 1.4.6.

[46] Vgl dazu auch die österreichische „Überwachungsverordnung“ (BGBl II 418/2001).

Gerade dies sollte jedoch – nach Punkt 4 der Anforderungen – nicht geschehen, da „sich der Betrieb des überwachten Telekommunikationsdienstes der überwachten Person als unverändert darstellen (soll)“.[47] Auszugehen ist somit davon, daß zwar alle Verbindungs- und Inhaltsdaten gespeichert werden müssen, eine *Auswertung* und *Beurteilung* unter (straf-)rechtlichen Gesichtspunkten jedoch erst im Falle einer gerichtlichen Anordnung erfolgen kann. Allerdings sei es „für die gesetzlich ermächtigten Behörden...erforderlich, daß Netzbetreiber bzw Diensteanbieter die Überwachungsmaßnahmen so rasch wie möglich durchführen (in dringenden Fällen innerhalb weniger Stunden oder Minuten)“ (Anforderungen Pkt 9.).

In einem eigenen Teil 2, betitelt „Ergänzende Anforderungen“ wird zusätzlich noch festgehalten, daß „die gesetzlich ermächtigten Behörden...den Zugriff auf Informationen über die Identität des Subjektes im Besitz von Betreibern/Anbietern von Telekommunikationsnetzen, Telekommunikationsdiensten und Internet-Diensten“ fordern, worunter (unter anderem) neben dem vollständigen Namen und der vollständige Adresse des Überwachten auch Kreditkartendetails, Benutzerkennung und Benutzercode, IP- und E-Mail Adresse, sowie „kryptographisches Schlüsselmaterial“ zu verstehen ist.

Unmittelbar nach Vorstellung dieses Entwurfs wurden 2 Revisionen[48] desselben präsentiert, welche detaillierter die Voraussetzungen beschreiben, die angesichts der technischen Entwicklung - vor allem im Bereich der Internet-Kommunikation - für eine umfassende Überwachung vonnöten sind.

Was in den nächsten Tagen und Monaten folgte, waren endlose politische Querelen um die Umsetzung und die Billigung des Dokuments, eine endgültige Ratifizierung durch den Europarat, welche eigentlich für Februar 1999 geplant gewesen wäre, scheiterte und

---

[47] Eine Überwachung von Internet-Inhalten in Echtzeit könnte nur durch die Einrichtung komplexer „Firewall-Systeme“ erfolgen. Die vom Bayerischen Staatsministerium für Unterricht, Kultus, Wissenschaft und Kunst eingesetzte Arbeitsgruppe „Hochschulnetze in Bayern” stellt dazu in ihrem 1997 erschienenen gleichnamigen Schlußbericht fest, daß „Firewalls zwei Arten von Einschränkungen nach sich ziehen: Performance-Verluste, sowie Nutzungseinschränkungen bei den möglichen Diensten. Die Performance-Verluste sind bedingt durch die (je nach Grad des Firewall-Einsatzes) erforderliche detaillierte Analyse der über die Schnittstelle fließenden Daten.“ (zitiert nach *Sieber*, Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen (II) - Zur Umsetzung von § 5 TDG am Beispiel der Newsgroups im Internet, CR 11/1997, FN 162).

[48] „Enfopol 98 Rev 1“ (10951/1/98) vom 10.11.1998 bzw „Enfopol 98 Rev 2“ (10951/2/98) vom 03.12.1998.

wurde daraufhin immer wieder verzögert.[49] Der Entwurf wurde in zwei Ausschüssen des Europäischen Parlaments (dem „Ausschuß für bürgerliche Freiheiten und innere Angelegenheiten“, sowie dem „Ausschuß für Recht und Bürgerrechte“) erörtert, die jedoch zu unterschiedlichen Schlußfolgerungen gelangten: Während der erstgenannte Ausschuß die Ansicht vertrat, die Entschließung diene der Klarstellung und Aktualisierung der Entschließung von 1995 und sei daher annehmbar, lehnte der andere Ausschuß den Entwurf wegen der Gefahr möglicher Menschenrechtsverletzungen und der den Betreibern drohenden Kosten ab und forderte die Kommission auf, nach Inkrafttreten des Vertrags von Amsterdam einen neuen Entwurf zu erstellen.[50]

Auch inhaltlich schrumpfte das Dokument aufgrund des Drucks von liberalen Bürgerrechtsorganisationen immer mehr und Teile davon, wie zB die Bestimmungen über die Überwachung von Iridium-Satellitenkommunikation, wurden eigenen Ausschüssen übertragen.[51]

Einzelne Abschnitte von Enfopol 98 fanden schließlich Eingang in das „*Europäische Rechtshilfeübereinkommen*“[52], welches am 29.05.1999 verabschiedet wurde. Das Abkommen in der Fassung vom 15. Mai 1999 sieht in den Artikeln 17 bis 22 Regelungen zur grenzüberschreitenden Kommunikationsüberwachung vor. Demnach können auch die Mitgliedsstaaten einen anderen Staat ersuchen, in seinem eigenen Interesse die Überwachung durchzuführen. Irritierend ist, daß auch diese Fassung - wie alle vorangegangen - als Geheimmaterial mit „Limite“ klassifiziert worden ist.[53]

Das Europäische Rechtshilfeabkommen regelt nicht nur die grenzüberschreitende Telekommunikationsüberwachung, sondern auch die Vernehmung per Videokonferenz

---

[49] Vgl *Möchel*, EU-Minister billigen Abhörplan, Telepolis, das Magazin für Netzkultur vom 24.02.1999 unter *http://www.heise.de/tp/deutsch/special/enfo/6374/1.html.*

[50] Vgl das Dokument „Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität“, KOM (2000) Anm 40. Aus dem Internet kann es unter:
http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComDE.pdf geladen werden.

[51] Vgl dazu den „Entwurf eines Übereinkommens über die Rechtshilfe in Strafsachen zwischen den Mitgliedstaaten der Europäischen Union zur Überwachung des Telekommunikationsverkehrs (JUSTPEN 79 - 10702/98)“.

[52] Das europäische Rechtshilfeabkommen wurde am 29.05.2000 in der Fassung vom 15.05.2000 (COPEN 32) unterzeichnet und ist idF Abl. C 197 v 12.07.2000, 1 rechtsgültig.

[53] *Schulzki-Haddouti*, Europäisches Rechtshilfeübereinkommen kurz vor der Verabschiedung, Telepolis, das Magazin für Netzkultur vom 26.05.2000 unter *http://www.heise.de/tp/deutsch/special/enfo/6807/1.html.*

oder den Einsatz gemeinsamer Gruppen für strafrechtliche Ermittlungen. Diese können bei schwierigen und aufwendigen Ermittlungen mit Bezug zu anderen Mitgliedstaaten gebildet werden, oder wenn ein koordiniertes und abgestimmtes Vorgehen erforderlich ist. Das Übereinkommen bietet jetzt die rechtliche Grundlage, grenzüberschreitend Kommunikationsdaten abzugreifen und Kommunikationsinhalte abzuhören. Tatsächlich erstreckt es sich jedoch nur auf den Bereich der Kommunikation via Telefon, eine Grundlage für das Abhören von Internet-Inhalten bietet es nicht.[54]

2.2.3. „Enfopol 19“

Die Problematik der Einrichtung von Schnittstellen zur Überwachung, welche ebenfalls keinen Eingang in das Rechtshilfeübereinkommen gefunden hat, wurde einer eigenen Arbeitsgruppe, der „*Section Lawful Interception*“ (SEC LI) übertragen, welche auch bald den ersten Entwurf über die Schaffung des sog „ETSI-Standards“[55] präsentierte. Die Thematik der Überwachung von Internet-Inhalten wiederum wurde in einem eigenen Arbeitspapier, „Enfopol 19“[56] betitelt, weiterverfolgt, wobei es sich dabei jedoch nur um eine „Neuauflage“ der „Requirements“ aus dem Jahre 1995 handelte, welche rechtlich bedeutungslos blieb. Alle brisanten Punkte aus „Enfopol 98“ wurden

---

[54] Anlaß heftiger Debatten bot vor allem der Artikel 18 des Übereinkommens, wonach in bestimmten Fällen sogar unabhängige und eigenständige Überwachungsmaßnahmen eines Staates in einem anderen Staat ohne dessen Einwilligung möglich sein sollten. Das Europäische Parlament hatte am 17.02.2000 für die Streichung des Artikels 18 votiert, andererseits jedoch dem grenzüberschreitenden Abhören in Fällen „krimineller Straftaten“ mit der Zustimmung und Unterstützung des betroffenen Staates zugestimmt. Siehe dazu sehr ausführlich *Schulzki-Haddouti*, Die Globaliosierung des Rechts, Der-Spiegel Online vom 05.11.1999 unter *http://www.spiegel.de/netzwelt/politik/0,1518,51141,00.html*.

[55] Mit Hilfe der Einführung des EU-Abhörstandards „ETSI ES 201 671“ sollen alle Formen der Telekommunikation lückenlos überwachbar werden. Verantwortlich für die Erarbeitung des technischen Standards, der die technischen Gegebenheiten dafür beschreibt, daß Kommunikation, sei es nun im Bereich der Sprachtelephonie oder aber des Internet, „abhörbar“ wird, ist die sog Sektion „*Lawful Interception*“ (SEC LI)[55] des „*European Telecom Standards Institute*“ (ETSI). Zu diesem Zweck wird von drei verschiedenen Arbeitsgruppen ein technischer Standard laufend, parallel zu den Entwicklungen auf technischem Gebiet, weiterentwickelt, um Schnittstellen zur Überwachung sämtlicher digitalen Netze - von ISDN über UMTS bis hin zum Internet - überhaupt erst zu ermöglichen.

[56] „Draft Council Resolution on the lawful interception of telecommunications in relation to new technologies (6715/99)” vom 15.03.1999, im Internet unter *http://www.fipr.org/polarch/enfopol19.html*.

aus dem Entwurf des Ratsbeschlusses eliminiert und verschwanden in einem Annex mit technischen Erläuterungen, welcher dem Parlament nicht vorgelegt wurde. Aus dem ehemals 42 Seiten starken Dokument wurde im Endeffekt ein abstrakter, vierseitiger Forderungskatalog, während die „IUR", anstatt in der Form eines Ratsbeschlusses offiziell erlassen zu werden, wieder am Parlament vorbei als europäischer Telekommunikations-Standard eingeführt wurden.[57]

ENFOPOL 19 wurde bei einem Treffen von Polizeibeamten in Brüssel am 11.03.1999 verfaßt und von der deutschen EU-Präsidentschaft am 15.03.1999 herausgegeben. Vier Abänderungsvorschläge, welche – unter Mitarbeit vor allem der österreichischen Delegation - von der „Grünen Fraktion" eingebracht wurden, wurden abgelehnt.[58] Inhaltlich wurde die Überwachung der Telekommunikation nun auch expressis verbis auf das Internet ausgedehnt:

> "The requirements of law enforcement agencies for lawful interception of telecommunications in relation to network operators and service providers, with glossary, of the Council Resolution of 17 January 1995 shall *apply also to new technologies* in existence, e.g. satellite and *internet communications*, and to future additional telecommunications technologies.
>
> The technical terms used in the Council Resolution of 17 January 1995 on the basis of the then state of telecommunications technology are to be interpreted as *applying to new telecommunications technologies* already in existence and to future additional telecommunications technologies".[59]

Zu einem Zeitpunkt, als die Diskussion um die „Enfopol-Papiere" aufgrund divergierender Interessen von Datenschützern, Sicherheitsbehörden und Kommunikationsdienstleistern als eigentlich beendet galt, sind am 07.05.1999 im Rahmen eines Sicherheitspaketes die überarbeiteten „International User Requirements" wiederum an zwei aufeinanderfolgenden Tagen auf die Tagesordnung der Sitzungen des

---

[57] Vgl *Moechel*, Die ETSI Dossiers – Europäische Standards für das Abhören digitaler Netze, c't 7/2001, 60.

[58] Maßgeblich am Entwurf dieser Abänderungsanträge beteiligt war auch der österreichische Abgeordnete Dr. Johannes *Voggenhuber*, der vor allem kritisierte, daß „die Ratsentschließung nicht nur ein technisches Update (sei), sondern jeder Telekommunikationsbetreiber dazu verpflichtet (werde), für die Polizei eine wasserdichte Hintertür einzubauen". Vgl auch *Schulzki-Haddouti*, EU-Parlament verabschiedet Enfopol-Überwachungspläne, Telepolis, das Magazin für Netzkultur vom 10.05.1999 unter *http://www.heise.de/tp/deutsch/special/enfo/6404/1.html*.

[59] Vgl Enfopol 19 Part 1: General Explanations.

EU-Parlaments gesetzt und ebenso schnell wieder entfernt worden. Als schließlich die Mehrzahl der Abgeordneten den Sitzungssaal verließen, stimmten die verbliebenen 161 Parlamentarier dennoch über die umstrittenen Regelungen in Form einer fast ausschließlichen Befürwortung ab. Obwohl vom Rat der Innen- und Justizminister nicht abgesegnet, wurde der „ETSI-Standard 206.671“ fertig gestellt, publiziert und teilweise auch schon technisch umgesetzt. Die politische Legitimation jedoch sollte durch ein, in der Form eines Ratsbeschlusses verfaßtes, Dokument unter dem Akronym „Enfopol 55“ erfolgen. Obwohl es mit „ECO 143“ das Kürzel eines Ratsbeschlusses trägt, wurde es jedoch bis heute noch nicht verabschiedet, was sich daraus ergibt, daß es bislang noch nicht in der „Eur-Lex“-Datenbank aller rechtsverbindlichen Ratsbeschlüsse enthalten ist.[60]

2.2.4. „Enfopol 55“

Das aktuellste Papier der EU Arbeitsgruppe „Polizeiliche Zusammenarbeit“, veröffentlicht von der „Foundation for Information Policy Research“, das bereits als Entschließung des Europäischen Rats formuliert ist, stellt zum heutigen Zeitpunkt das Dokument „Enfopol 55“[61] aus dem Jahre 2001 dar. Auch hier werden wiederum die „International User Requirements“ strapaziert und deren Anwendung auf moderne Formen der Internet-Kommunikation vorgeschlagen. Im Wesentlichen handelt es sich dabei um einen Versuch, technische Anforderungen zur Überwachung der neuen Telephonienetze, sowie der Satelliten- und Internetkommunikation auf politischer Ebene zu verabschieden.

Artikel 1, zugleich Kernpunkt des Dokuments, lautet wie folgt:

> “Law enforcement agencies require access to all interception subjects operating temporarily or permanently within a telecommunications system.”

---

[60] Vgl *Möchel*, Lauscher am Netz – Die ETSI Dossiers Teil 4, c’t 4/2001, 80.

[61] „Council Resolution of on law enforcement operational needs with respect to public telecommunication networks and services (Enfopol 55, ECO 143)”, 9194/01 vom 20.06.2001, im Internet unter *http://www.statewatch.org/news/2001/sep/9194.pdf*.

Generell geht es inhaltlich darum, daß die Strafverfolgungsbehörden ungehinderten Zugriff auf „alle Arten der Telekommunikation“[62] haben müssen, von ISDN über GPRS und UMTS bis hin zu E-Mail- oder Message-Diensten. Dazu gehören auch alle damit zusammenhängenden Kommunikationsdaten – etwa die technischen Identifikationsmöglichkeiten, aber auch Wohnort, Adresse des Arbeitsplatzes oder Kreditkartendaten. Im Fall von Internet-Kommunikation müssen so zur Identifizierung beispielsweise IP-Adresse, Account-Nummer, Passwort, PIN-Nummer und E-Mail-Adresse den Strafverfolgungsbehörden mitgeteilt werden.
Artikel 3 bezieht sich direkt auf die ETSI-Überwachungsschnittstellen und hält die Möglichkeit offen, Provider in nationalen Regelungen dazu zu verpflichten, eine adäquat geführte Aufzeichnung aller Überwachungs-Aktionen zu führen.

Interessant liest sich auch Artikel 8, welcher den TK-Dienstleistern die Pflicht auferlegen soll, nicht nur einen, sondern gleichzeitig mehrere Anschlüsse in Echtzeit „überwachbar“ zu machen:

“Law enforcement agencies require network operators/service providers to make provision for implementing a number of simultaneous intercepts. Multiple interceptions may be required for a single target service to allow monitoring by more than one law enforcement agency. In this case, network operators/service providers should take precautions to safeguard the identities of the monitoring agencies and ensure that confidentiality of the investigations. The maximum number of simultaneous interception for a given subscriber population will be in accordance with national requirements.”

Laut *Möchel*[63] bedeute dies nichts anderes, als daß die Identität der überwachenden Behörden voreinander strikt geheimgehalten werden müsse. Es handle sich hierbei um einen reinen „Geheimdienstparagraphen“, der jedem EU-Mitglied die Möglichkeit schaffen sollte, die ETSI-Schnittstellen seinen eigenen Geheimdiensten zu öffnen.
Artikel 5.1. verpflichtet die Netzbetreiber darüber hinaus zusätzlich zur Geheimhaltung darüber, wie viele Überwachungen stattfinden und wie diese ausgeführt werden sollen.

Notwendig ist es aber, daß „Enfopol 55“ auch als Ratsbeschluß auch vom EU-Parlament angenommen wird. Dies ist aber insofern problematisch, als der

---

[62] Siehe dazu die Ausführungen in Enfopol 55, Annex, Pkt Applicable Services.

[63] *Möchel*, Die ETSI-Dossiers, Teil 3 – Abhörstandards für digitale Netze vor der Verabschiedung, c’t 17/2001, 80.

normalerweise übliche Standardisierungsprozeß - generelle Anforderungen der Behörden werden auf politischer Ebene gestellt, technische Spezifikationen dieser Anforderungen werden ausgearbeitet und schließlich zum aktuellen technischen Standard erhoben – in diesem Fall genau umgekehrt verlief: *Nachdem* die IT-Industrie sich in jahrelangem Ringen mehrheitlich auf einen umfangreichen Schnittstellen-Standard zur Überwachung digitaler Netze in allen Details geeinigt und damit vollendete Tatsachen geschaffen hatte, wurde das Anforderungspapier der Strafverfolger diesbezüglich erst nachgereicht.

Im Endeffekt soll also nachträglich beschlossen werden, was faktisch schon längst umgesetzt ist.

2.3. Enfopol und die österreichische Gesetzgebung

Seit dem In-Kraft-Treten der Überwachungsverordnung und des im Rahmen dieser Verordnung bis zum Jahre 2005 umzusetzenden ETSI-Standards konnten natürlich auch die internationalen Zusammenhänge, die sich im Laufe der letzten Jahre vor dem Erlaß der Verordnung aufgetan haben, auch von der österreichischen Gesetzgebung und Judikatur nicht mehr ignoriert werden. Dennoch gab es auch in jüngerer Zeit Stimmen, die eben jene Beziehungen aufs heftigste dementierten:
„Enfopol ist“ – so ein Zitat von Mjr Rudolf Gollia[64] vom November 1998 - „eine ganz normale Ratsarbeitsgruppe, die sich mit dem Einsatz neuer Technologien in der polizeilichen Zusammenarbeit beschäftigt.“ Mit einem System wie dem militärischen Echelon habe Enfopol nichts zu tun, vielmehr sei da „in letzter Zeit in den Medien vieles vermischt worden.“[65]

Letzteres mag zwar durchaus zutreffen, die Zusammenhänge können jedoch nicht völlig verleugnet werden und wurden auch in der Tatsache bestätigt, daß gerade einer der ersten Entwürfe einer Entschließung des Rates zum Thema, nämlich das Arbeitspapier

---

[64] Rudolf Gollia ist Sprecher der Generaldirektion für Öffentliche Sicherheit beim BMI.

[65] Zitiert nach *Möchel*, Auf den Spuren von Enfopol, Telepolis, das Magazin für Netzkultur vom 24.11.1998 unter *http://www.heise.de/tp/deutsch/special/enfo/6321/1.html*.

„Enfopol 95“[66], auch in den Beilagen zum dem Bundesgesetz, mit dem Lauschangriff und Rasterfandung in die Strafprozeßordnung aufgenommen wurden,[67] quasi „am Rande“, nämlich ganz am Schluß der EB, erwähnt wird. So heißt es an dieser Stelle, daß „(es) die vorgeschlagene Ergänzung des Fernmeldegesetzes 1993...in Gestalt einer besonderen Verordnungsermächtigung ermöglichen (soll), technische Anforderungen zur Überwachung des Fernmeldeverkehrs allgemein festzulegen, wie sie von der Entschließung des Rates vom 17. Jänner 1995 über die Anforderungen der gesetzlich ermächtigten Behörden im Hinblick auf die rechtmäßige Überwachung des Fernmeldeverkehrs (ENFOPOL 150) eingefordert werden“[68].

Vor allem in der Zeit, als Österreich den Vorsitz des Europäischen Rates innehatte wurden die Enfopol-Pläne konkretisiert und ausgearbeitet, was schließlich – obwohl unter dem Mantel der Verschwiegenheit verborgen - auch innenpolitisch nicht unbemerkt blieb. In einer schriftlichen Anfrage[69] vom 02.02.1999, gerichtet an den Bundesminister für Inneres, wurden wesentliche Punkte betreffend Enfopol bereits angesprochen: Die sehr konkret formulierten zentralen Punkte dieser Anfrage lauteten:

- Während Österreichs EU - Präsidentschaft wurde im November 1998 das „ENFOPOL 118“[70] erarbeitet. Welche konkreten Überwachungen sollen damit ermöglicht werden?

---

[66].Enfopol 150, ABl. C 329 v 04.11.1996 S 1; siehe dazu oben, 2.2.1.

[67] BGBl I 105/1997.

[68] EBRV 49 BlgNR 20. GP 14.

[69] „Schriftliche parlamentarische Anfrage der Abgeordneten G. *Moser*, Freundinnen und Freunde an den Bundesminister für Inneres betreffend Überwachung in Österreich“, 5695/J 20. GP.

[70] Gemeint ist natürlich, was sich aus dem Kontext eindeutig ergibt, das Dokument „Enfopol 98“ und nicht der „*European Curriculum for Police Training*“ (Enfopol 118). Dabei handelt es sich „bloß“ um ein Ausbildungsprojekt der „Vereinigung Europäischer Polizeiakademien“ *AEPC (The Association of European Police Colleges)* der Europäischen Kommission. Führende Entscheidungsträger der Polizei in Bulgarien, Estland, Lettland, Litauen, Polen, Rumänien, Slowenien, der Slowakei, Tschechien und Ungarn werden in diesem Programm geschult. Auffällig ist in diesem Zusammenhang, daß, spricht man im Allgemeinen von „Enfopol“, oftmals die Auffassung vertreten werde, es handle sich bei der Tätigkeit dieser Ratsarbeitsgruppe *ausschließlich* um eine solche, welche *nur* die Überwachung der Telekommunikation im weitesten Sinne umfaßt. So zeigen sich manche Autoren in ihren Publikationen immer noch verwundert, wenn ihnen im Rahmen ihrer „Enfopol-Recherchen“ unter diesem Akronym Papiere zugänglich gemacht werden, welche sich etwa mit „Rowdytum bei Fußballspielen“ beschäftigen (beispielweise bei *Philippi/Pracher*, Eingriffe in die Grundrechte von Betreibern und Konsumenten von Telekommunikationsdiensten durch polizeiliche Überwachungsmaßnahmen: Zu Natur und Konsequenzen

- Wie werden laut ENFOPOL Verdächtige definiert?
- Wie lautet der Wortlaut von ENFOPOL?
- Was geschieht mit den Daten dieser Betroffenen, wann müssen sie gelöscht werden?
- Wie lautet die Stellungnahme des Innenministeriums zu ENFOPOL im Wortlaut?
- Wie lautet die entsprechende Stellungnahme des Justizressorts?
- Im September und Oktober 1998 wurde von Polizeivertretern die Umsetzung von ENFOPOL diskutiert und vorbereitet. Wann genau und wo fanden diese Treffen statt?
- Wie lauten die entsprechenden Berichte und Aktenvermerke über diese Treffen?

Die Beantwortung dieser Fragen, welche sehr wohl Rückschlüsse darauf zulassen, daß man praktisch - trotz des „taktisch unklugen" Verweises auf Enfopol 118 - schon sehr genau Bescheid über die Enfopol-Aktivitäten gewußt hat, könnte knapper und ausweichender nicht ausfallen. Es wird zwar – richtigerweise – erläutert, daß Enfopol 118 nichts mit den Papieren, welche die Überwachung der Telekommunikation zum Inhalt haben, zu tun hat, man bemühte sich hingegen nicht um eine weitergehende Erörterung des Problems[71]:

- „Beim Dokument ENFOPOL 118 handelt es sich um einen Bericht der Ratsarbeitsgruppe Terrorismus an den K.4 - Ausschuß vom 6. November 1998, der in keinerlei Zusammenhang mit Überwachungstätigkeiten steht. Es ist daher nicht erkennbar, auf welchen Sachverhalt sich die an dieses Dokument anknüpfenden Fragen beziehen. Darüber hinaus weise ich darauf hin, daß „ENFOPOL" die Arbeitspapiere jener Ratsarbeitsgruppen bezeichnet, die im Rahmen der 3. Säule der Europäischen Union die Fragen der polizeilichen Zusammenarbeit erörtern (Ratsarbeitsgruppen „Polizeiliche Zusammenarbeit", „Terrorismus", „Drogen und organisierte Kriminalität"). Jährlich werden im Rahmen dieser Arbeitsgruppen weit mehr als 100 ENFOPOL Dokumente erarbeitet und den Delegierten der Mitgliedstaaten vorgelegt."

---

einer europäischen Überwachungsverordnung (ENFOPOL-98-Dokument) 3; abrufbar unter *http://www.it-law.at/papers/phillipi-pra-tretter.pdf*).

[71] „Anfragebeantwortung durch den Bundesminister für Inneres Mag. Karl *Schlögl* zu der schriftlichen Anfrage (5695/J 20. GP) der Abgeordneten Dr. Gabriela *Moser* und Genossen an den Bundesminister für Inneres betreffend Überwachung in Österreich", 5386/AB 20. GP.

Wesentlich durchdachter präsentierte sich eine schriftliche Anfrage[72] an den BMI zum selben Themengebiet beinahe ein Jahr zuvor. In deren Einleitung wird – in Anbetracht der zum damaligen Zeitpunkt spärlich verfügbaren Informationsmaterien zum Thema – die Problematik außerordentlich detailliert geschildert und durch einen beinahe vollständigen Abriß der Geschichte von Echelon und Enfopol bis zum Jahre 1995, einschließlich der „International User Requirements“ und den ersten Entwürfen eines „Internationalen Rechtshilfeübereinkommens“, eine mögliche Anfragebeantwortung quasi schon vorweggenommen.
Die Fragen selbst bezogen sich auf den Zusammenhang zwischen dem Überwachungssystem Echelon und den Enfopol-Papieren bzw der den Bestimmungen zur Überwachung des Telekommunikationsverkehrs in der österreichischen Rechtsordnung. In der Anfragebeantwortung[73] führte der BMI aus, daß an einem systematischen, EU-weiten Überwachungs- und Abhörsystem nicht gearbeitet werde. Im Rahmen der Zusammenarbeit der Justiz - und Innenminister der Europäischen Union beschäftige sich die Ratsarbeitsgruppe „Polizeiliche Zusammenarbeit“ allerdings auch mit Fragen der rechtmäßigen Überwachung des Telekommunikationsverkehrs, einschließlich der Überwachung neuer Kommunikationssysteme (Mobiltelefonie, Internet, E-Mail); die Diskussion erfolge hierbei stets unter Beachtung der jeweiligen nationalen Rechtsvorschriften. Dabei werde eine Angleichung der Standards der Anforderungen der gesetzlichen ermächtigten Überwachungsbehörden an Netzbetreiber und Diensteanbieter bei der rechtmäßigen Überwachung des Telekommunikationsverkehrs angestrebt.

Aber auch auf wissenschaftlicher Ebene hat man sich mit dem Problem „Enfopol“ auseinandergesetzt: Im Auftrag des „Forum Mobilkommunikation“ wurde von Univ.-Prof. DDr. Heinz *Mayer* und RA Mag. Michael *Pilz* ein Gutachten verfaßt, in welchem die verfassungsrechtlichen und strafprozessualen Aspekte des Konzeptes Enfopol – vor

---

[72] „Schriftliche parlamentarische Anfrage der Abgeordneten *Barmüller*, *Kier* und weiterer Abgeordneter an den Bundesminister für Inneres betreffend Entwicklung eines EU - Überwachungssystems für den europäischen Telekommunikationsverkehr“ vom 16.04.1998, 4317/J 20. GP.

[73] „Anfragebeantwortung durch den Bundesminister für Inneres Mag. Karl *Schlögl* zu der schriftlichen Anfrage (4317/J 20. GP) der Abgeordneten *Barmüller*, *Kier* und weiterer Abgeordneter an den Bundesminister für Inneres betreffend Entwicklung eines EU - Überwachungssystems für den europäischen Telekommunikationsverkehr“, 4014 AB/20. GP.

allem unter den Aspekten des Grundrechts- und Datenschutzes – beleuchtet werden. Seitens der Auftraggeber, der Interessensgemeinschaft der österreichischen Mobilfunknetzbetreiber[74], wurde die Frage aufgeworfen, ob die Umsetzung der in den Enfopol-Papieren vorgesehenen Überwachungsszenarien mit dem geltenden nationalen Recht vereinbar sei und wie weit die Pflichten der Betreiber von Mobilfunknetzen gingen, an derartigen Überwachungsmaßnahmen mitzuwirken und welche rechtspolitischen Folgerungen aus den geplanten Maßnahmen abzuleiten seien.[75]

Sollten sich in Österreich wirklich jene Abhörstandards, welche in den Enfopol- bzw ETSI Papieren gefordert und beschrieben werden, realisieren lassen, wird man wohl nicht umhin kommen, auch die Hintergründe, die zur Schaffung dieser Regelungen geführt haben, zu beleuchten und endlich auch zu möglicherweise unangenehmen Themen – Stichwort Echelon – von parlamentarischer Ebene aus klar Stellung beziehen müssen.
Dabei nützt es jedoch herzlich wenig, wenn Österreich sich zwar als Staat von der Vision einer globalen Überwachung der Telekommunikation distanziert, gleichzeitig aber Regelungen im innerstaatlichen Recht umsetzt, welche diesbezügliche Assoziationen unweigerlich aufkommen lassen.

3. Sonstige Entwicklungen innerhalb der Europäischen Union

Mit der Gründung der Europäischen Union wurde die Zusammenarbeit in den Bereichen Justiz und Inneres als „Dritte Säule“ der EU in den K-Artikeln des EU-Vertrags (nunmehr der Art 29 ff EUV) festgelegt. Zahlreiche Initiativen zur Rechtsangleichung auf dem Gebiet der multimedialen Kriminalität wurden von den Staaten der Europäischen Union und der Europäischen Gemeinschaft selbst ergriffen.[76] Die Arbeit im Bereich der Internet-Kriminalität überschneidet sich mit den Projekten

---

[74] Http://fmk.at/fmk/index.html.

[75] Das Gutachten kann als Hartkopie unter *office@fmk.at* bestellt werden, auszugsweise ist es im Internet unter *http://www.quintessenz.at/ftp/enfopol_summary.rtf* verfügbar.

[76] Vgl *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht: Ist der Nationalstaat wirklich überholt? (2001) 180.

des Europarats zwar in einigen Bereichen, meist ergänzt sie diese jedoch. Denn wenn es die Aufgabe des *Europarats* ist, konkrete (straf)rechtliche Bestimmungen zur Schaffung von Sicherheit in Computernetzen zu schaffen, so stellt die *Europäische Union* meist nur allgemeine „Verhaltensregelungen" im Zusammenhang mit denselben her. Als Beispiel sei hier die „*Convention on Cyber-Crime*" des Europarats angeführt, welche genaue strafrechtliche Normen bezüglich Internet-Kriminalität enthält, während das Papier „*eEurope 2002*"[77] der Europäischen Union die Bekämpfung der Computerkriminalität vor allem durch die Verbesserung der Sicherheit von Informationsstrukturen schon in ihrem Keim ersticken will.

Auf lange Sicht gesehen erfordert eine effektive internationale Verfolgung von Straftaten im Internet eine Harmonisierung sowohl des materiellen, als auch des Verfahrensrechts zwischen den einzelnen Mitgliedsstaaten und den verschiedenen Organisationen im Rahmen der EU und des Europarats untereinander.

3.1. Allgemeines und historische Entwicklung

Vorschläge in Hinblick auf eine solche Rechtsangleichung bzw der Schaffung einschlägiger Bestimmungen - nicht nur alleine die europäische Ebene betreffend - reichen beinahe 20 Jahre zurück: So diskutierte beispielsweise in den Jahren 1983 bis 1985 ein „Ad-hoc-Komitee" der OECD die Möglichkeiten einer Bekämpfung von Computer-bezogenem Verbrechen durch die Harmonisierung von Rechtsnormen. Im Jahr 1986 erarbeitete das „*Select-Commitee of Experts for Computer-related Crime*" des Europarats eine Serie von Vorschlägen[78], um die Probleme, welche sich im Rahmen des Datenschutzes bei einer länderübergreifenden Strafverfolgung stellen, zu erörtern.[79] Rechtliche Fragen bezüglich Computer-Kriminalität wurden auch vom „*Legal Advisory Board*" (LAB) der Europäischen Kommission diskutiert. Im Dezember 1987 wurde ein

---

[77] Vgl dazu unten, 3.2.

[78] Vgl *Sieber*, Proposal for a Council of Europe Initiative in the Field of Computer-Related Economic Crime, Council of Europe Doc No PC-R-CC (86) (1987).

[79] Vgl „*Intermediate Evaluation of the Safer Internet Action Plan*, Conducted for the European Commission" der Business Development Research Consultants vom 31.05.2001, 5 f.
Im Internet ist dieses Dokument unter
h*ttp://europa.eu.int/information_society/programmes/evaluation/pdf/report1iap_en.pdf* abrufbar.

erster Report über „The Legal Aspects of Computer Crime and Security“[80] der LAB vorgelegt, welcher schließlich zu einem Treffen der Mitglieder der Kommission und des Europarats im März 1990 in Luxemburg geführt hat. Damit wurde ein Grundstein für zukünftige internationale Aktionen auf dem Gebiet der Internet-Kriminalität gelegt.
Im September 1990 veröffentlichte die Kommission der Europäischen Gemeinschaften einen Ratsentwurf,[81] welcher sich zum Ziel gesetzt hatte, einen Aktionsplan für den Schutz elektronisch gespeicherter Daten zu schaffen. Dieser Aktionsplan beinhaltete neben strafrechtlichen Bestimmungen auch generelle Vorschriften zur Spezifikation und Standardisierung von Sicherheitsmaßnahmen innerhalb der Informationsgesellschaft.[82]

Hervorzuheben sind des weiteren die im selben Jahr am achten Kongreß der „United Nations“ geführten Diskussionen über Computerkriminalität, welchen schließlich in einer Resolution Ausdruck in dem Sinne verliehen wurde, daß ein Maßnahmenkatalog zur Verhinderung mißbräuchlicher Verwendung von Computersystemen erarbeitet wurde.[83] Die Diskussionen wurden weitergeführt, 1994 im „Manual on the Prevention and Control of Computer-Related Crime“[84] festgehalten und – erweitert speziell um die rechtlichen Probleme im Zusammenhang mit dem Internet – in einem neuen Projekt aufgegriffen.

Mit den speziellen Problemen betreffend bestimmter strafbarer Internet-Inhalte („*harmful and illegal content*“) beschäftigte man sich im Rahmen der Europäischen Union erstmals im Februar 1997, als der „Telecommunications Council“ eine Resolution[85] zu diesem Themenschwerpunkt adoptierte. Interessant an dieser Resolution ist, daß sie quasi einen Gegenpol zur „*Council Resolution on the lawful interception of*

---

[80] *Sieber/Kaspersen/Vandenberghe/Stuurman*, The Legal Aspects of Computer Crime and Security - A Comparative Analysis with Suggestions for Future International Action (1987).

[81] Vgl Kommission der Europäischen Gemeinschaft, Kom (90) 314 final – SYN 287 und 288 vom 13.09.1990.

[82] Vgl näher bei *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society (1998) 159.

[83] „Eight UN Congress on the Prevention onn Crime and the Tratment of Offenders, Doc A/Conf.144/L.11” vom 04.09.1990. Siehe dazu näher *Amann*, Harmonic Convergence - Constitutional Criminal Procedure in an International Context, im Internet unter *http://www.law.indiana.edu/ilj/v75/no3/amann.pdf*.

[84] „UN Manual on the Prevention and Control of Computer-Related Crime”, Nos 43 und 44, pp 19 et seq.

[85] „Resolution of the Coucil and of the Representatives of the Governments of the Member States’ Meeting within the Coucil on illegal and harmful content on the Internet”, OJ C/70/1 vom 06.03.1997.

telecommunications“[86] aus dem Jahre 1995 darstellt, bzw diese ergänzt: Wurden in letzterer nämlich die technischen Voraussetzungen festgehalten, welche zur Überwachung von Internet-Inhalten nötig sind, so beschreibt die Erstgenannte vor allem Maßnahmen, welche „selbstregulierend“ auf das Internet wirken sollen, um solche schädlichen und illegalen Internet-Inhalte gar nicht erst aufkommen zu lassen. Die Entschließung enthält einen Forderungskatalog, der sich an den Rat, die Kommission und die Mitgliedstaaten richtet. Was illegale Inhalte anbelangt, werden in der Entschließung unter anderem die Mitgliedstaaten aufgefordert, im Rahmen ihres Strafrechts gemeinsame Mindeststandards festzulegen und die administrative Zusammenarbeit auf der Grundlage von gemeinsamen Leitlinien zu verbessern und wird die Kommission beauftragt, nach Konsultation des Europäischen Parlaments einen *gemeinsamen Rahmen für Selbstkontrolle auf EU-Ebene* vorzuschlagen, der sich (unter anderem) auf Folgendes erstrecken sollte:

1. Maßnahmen, um die an der Einrichtung von Computernetzen beteiligten Unternehmen und Industrien dazu zu veranlassen, die Software für den Schutz und das Filtern von Material zu verbessern und sie den Netzteilnehmern automatisch bereitzustellen, und
2. geeignete Vereinbarungen, um sicherzustellen, daß alle in elektronischen Netzen festgestellten Fälle von Kinderpornographie der Polizei gemeldet und an Europol und Interpol weitergeleitet werden.[87]

Des weiteren verweist die Entschließung auf die Notwendigkeit einer internationalen Zusammenarbeit zwischen der Europäischen Union und ihren wichtigsten Partnerländern auf der Grundlage von Konventionen oder durch Anwendung neuer internationaler Rechtsinstrumente und fordert die Kommission dringend auf, Vorschläge für eine gemeinsame Regelung der Haftbarkeit für Inhalte im Internet vorzulegen. Schließlich werden die Mitgliedstaaten und die Kommission nachdrücklich

---

[86] Siehe oben, 2.2.1.

[87] Siehe im Zusammenhang mit dieser Resolution auch die Stellungnahme des Innen- und Rechtsausschusses des Schleswig-Holsteinischen Landtages mit dem Titel „Kinderpornographie im Internet”, abrufbar unter *http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/material/themen/divers/kipoinet.htm.*

aufgefordert, die Zusammenarbeit zwischen den Anbietern von Internet-Zugängen zu fördern, um so zu Selbstkontrollmaßnahmen zu ermutigen.

Am 24.04.1997 nahm das Europäische Parlament die Entschließung über die Mitteilung der Kommission „Illegale und schädigende Inhalte im Internet“ an[88], und am 03.06.1997 wurde unter Berücksichtigung der Stellungnahmen der endgültige Bericht fertiggestellt.[89]

3.2 Die „Comcrime“-Studie

Im Dezember 1997 wurde durch die Justiz- und Innenminister der G8-Länder ein 10-Punkte Aktionsplan erarbeitet, welcher im Mai 1998 auf dem Gipfeltreffen in Birmingham durch den Ministerrat für Justiz und Inneres angenommen und vom Europäischen Rat auf seiner Tagung in Amsterdam bestätigt wurde.[90]
Der Aktionsplan enthielt eine Aufforderung an die Kommission, bis Ende 1998 eine Studie über die Computerkriminalität zu erstellen. Die Kommission legte diese sogenannte „COMCRIME“ - Studie der Arbeitsgruppe „Organisierte Kriminalität“ des Rates im April 1998 dem Rat der Innen- und Justizminister vor. Die Kommission hielt es für angemessen, vor Erstellung dieser Mitteilung informelle Gespräche mit Vertretern der nationalen Strafverfolgungsbehörden und Kontrollstellen für den Datenschutz[91], sowie mit Repräsentanten der europäischen Industrie, va mit Anbietern von Internet-Diensten und Telekommunikationsbetreibern, zu führen.[92]

---

[88] Im Internet ist die Entschließung unter *http://europa.eu.int/ISPO/legal/de/internet/wp2de-2.html* abrufbar.

[89] Vgl „Illegale und schädigende Inhalte im Internet - Initiativen in den EU-Mitgliedstaaten zur Bekämpfung“, Zwischenbericht der Europäischen Kommission vom 04.06.1997, abrufbar unter *http://europa.eu.int/ISPO/legal/de/internet/wp2de.html.*

[90] Vgl *http://ue.eu.int/ejn/index.htm*.

[91] Die nationalen Kontrollstellen entsenden auf EU-Ebene Vertreter zur „Arbeitsgruppe für den Schutz von Personen bei der Verarbeitung personenbezogener Daten“.

[92] Die Protokolle dieser Unterredungen mit den Strafverfolgungsbehörden, den Vertretern der Industrie, als auch den Datenschutzgremien können schriftlich angefordert werden bei:
Europäische Kommission, Referat INFSO/A5 bzw Europäische Kommission, Referat JAI/B2, Rue de la Loi 200, B-1049 Brüssel (Belgien).

Im Jahre 1997 wurde Dr. Ulrich *Sieber*, damals Professor an der Juridischen Fakultät der Universität Würzburg, von der Europäischen Kommission beauftragt, einen Bericht über die aktuelle Situation im Bereich der Computer-Kriminalität zu erstellen und die rechtlichen Aspekte der Internet-Kriminalität in bezug auf die Informationsgesellschaft zu erarbeiten. Als Ergebnis wurde der Kommission am 01.01.1998 die „COMCRIME"-Studie[93] präsentiert, welche auf 256 Seiten Maßnahmen sowohl im Rahmen der ersten, als auch der dritten Säule der EU fordert:

So stellt der Bericht fest, daß auf inter- und supranationaler Ebene durch verschiedene Organisationen eine Harmonisierung und Koordinierung der Aktivitäten gegen Computer-Kriminalität erreicht wurde. Neben der Europäischen Union gehörten zu jenen Organisationen vor allem der Europarat, die P8- und OECD Länder, die Interpol und die UNO. Während es in den 70- er und 80- er Jahren dieses Jahrhunderts überhaupt keine internationalen Aktivitäten auf dem Gebiet der Computer-Kriminalität gegeben habe, so liege das Problem heutzutage darin, die unterschiedlichen Programme der einzelnen Organisationen miteinander zu verbinden und untereinander zu koordinieren.
Darüberhinaus seien viele der Aktionen zu unbestimmt und konzentrierten sich zu stark auf rechtliche Belange („*many of the present international and supranational answers are too vague and concentrate too much on legal issues"*).[94]

Als Voraussetzung zur Entwicklung brauchbarer Strategien zur Bekämpfung von Computer-Kriminalität analysiert der Report die grundsätzlichen Veränderungen der internationalen Risiko- und Informationsgesellschaft, welche ja die treibende Kraft hinter dieser Form der Kriminalität darstellten. Basierend auf dieser Analyse hebt die Studie drei Hauptvoraussetzungen für die Wirksamkeit zukünftiger Strategien hervor: Effektive Lösungsmethoden sollten *international*, *umfassend* und – speziell am rechtlichen Sektor – den *Besonderheiten der Information* an sich angepaßt werden („*must be...devoted to the specifics of information*").[95]

---

[93] *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society (1998), im Internet abrufbar unter *http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html.*

[94] Vgl Sieber, Legal Aspects of Computer-Related Crime in the Information Society 4.

[95] Vgl Sieber, Legal Aspects of Computer-Related Crime in the Information Society 4.

3.2.1. Maßnahmen im Rahmen der „Ersten Säule“ der EU

Rechtliche Maßnahmen betreffend die *Europäische Gemeinschaft* könnten nach dieser Studie auf Art 100a des EU-Vertrags (heute: Art 95 EUV) gestützt werden und sich in erster Linie auf

- die Ausarbeitung einer Richtlinie betreffend eine generelle (zivil- und strafrechtliche) Verantwortlichkeit von Access- und Serviceprovidern,
- die Schaffung einer Richtlinie, welche die Termini „legale“, „illegale“ und „schädliche“ Internet-Inhalte definiert, was wiederum die Mitgliedsstaaten dazu bewegen könnte, effektive Maßnamen gegen solche illegalen und schädlichen Inhalte auszuarbeiten, es aber auch verhindert wird, daß der freie internationale Datenverkehr der Länder untereinander unterbunden wird,
- das Erstellen einer Liste illegaler Tätigkeiten, welche von adäquaten Sanktionen in zukünftigen nationalen Richtlinien (Beispiel: „E-Commerce“) abgedeckt und verhindert werden, um Sicherheit und Konsumentenschutz in europäischen Computernetzwerken zu garantieren und
- das Bereitstellen verbesserter Informationen über die rechtliche Situation in den Mitgliedstaaten (beispielsweise durch das Ändern und Aktualisieren der „Corpus Juris Datenbank“ über Regelungen betreffend Computer-Kriminaltät),

beziehen.[96]

3.2.2. Maßnahmen im Rahmen der „Dritten Säule“ der EU

Rechtliche Maßnahmen im Rahmen der *Dritten Säule der EU*, also der Zusammenarbeit in den Bereichen Justiz und Inneres, können sich nach der Studie auf kollektive Maßnahmen in Zusammenarbeit mit dem Europarat und der P 8-Gruppe[97] stützen. Die EU solle sich um eine engere Zusammenarbeit ihrer Organisationen untereinander

---

[96] Vgl *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society 5 f (nach eigener Übersetzung).

[97] Die P 8-Gruppe hochrangiger Persönlichkeiten (Lyon Gruppe), die sich mit der internationalen organisierten Kriminalität beschäftigt, entwickelt rechtliche und technische Verfahren, die es

bemühen und für die Ausarbeitung bestimmter Mindestregelungen am strafrechtlichen Sektor zur internationalen Verfolgung von Computer-Kriminalität einstehen. Dabei sei vor allem das Gewicht der Grundrechtseingriffe, welche mit solchen Maßnahmen verbunden wären, mit dem Interesse an der Strafverfolgung im Internet abzuwägen. Wichtig seien auch Regelungen in bezug auf das internationale Strafrecht, nämlich dahingehend, in wie weit und in welchen Fällen die nationale Jurisdiktion auf Sachverhalte mit Auslandsbezug Anwendung findet.

Weiters sollte die Europäische Kommission, um überflüssige Arbeit durch die verschiedenen inter- und supranationalen Organisationen zu vermeiden, eine gemeinsame Konferenz oder einen Workshop ansetzen, an der (dem) die Europäische Union, der Europarat, die OECD, die Interpol und die Vereinten Nationen mit dem Ziel, die verschiedenen Aktionen im Kampf gegen Computer-Kriminalität aufeinander abzustimmen, teilnehmen sollen.[98]

3.3. Die Initiative „eEurope 2002" der Europäischen Kommission

Im April 1998 legte die Kommission dem Rat die Ergebnisse der „Comcrime-Studie" zur Begutachtung vor und später, in den Schlußfolgerungen zu seiner Tagung in Tampere, stellte dieser fest, daß sich „die Bemühungen zur Vereinbarung gemeinsamer Definitionen und Sanktionen auch auf den Bereich der High-Tech-Kriminalität konzentrieren sollten."[99] Ein weiteres Dokument in diesem Zusammenhang stellte der „Gemeinsame Standpunkt"[100] des Rates der Europäischen Union zu Fragen betreffend Internet-Kriminalität dar, worin wiederum auf die Zusammenarbeit mit dem Europarat

---

ermöglichen, auf internationaler Ebene rechtzeitig mit strafrechtlichen Mitteln gegen Computerkriminalität vorzugehen.

[98] Vgl *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society 6 (nach eigener Übersetzung).

[99] Vgl KOM (2000) 890 (FN 894) 2.

[100] „Entwurf eines Gemeinsamen Standpunktes zu den Verhandlungen im Europarat über den Entwurf des Übereinkommens zur Cyber-Kriminalität des EU-Rats vom 23. April 1999", im Internet abrufbar unter *http://www.spiegel.de/netzwelt/politik/0,1518,46797,00.html*.

und die Unterstützung der Bemühungen um eine Bekämpfung der Internet-Kriminalität hingewiesen wurde.[101]

3.3.1. Aufgaben und Ziele

Im Jahre 1999 startete die Kommission ihre Initiative „eEurope 2002" „um sicherzustellen, daß Europa die digitalen Technologien nutzen und eine Informationsgesellschaft entstehen kann".[102]
Die Initiative eEurope selbst ist eine politische Initiative, welche garantieren soll, daß die Europäische Gemeinschaft von den Veränderungen in der Informationsgesellschaft, welche die Zukunft bringen wird, profitiert. Kernpunkte der Initiative[103] sind:

- Die beschleunigte Schaffung der notwendigen rechtlichen Rahmenbedingungen. Auf europäischer Ebene wird zur Zeit eine Reihe von Vorschlägen für Rechtsvorschriften ausgearbeitet und diskutiert. eEurope soll ihre Verabschiedung dadurch beschleunigen, daß allen Beteiligten kurze Fristen gesetzt werden.
- Die Unterstützung neuer Infrastruktureinrichtungen und Dienste in ganz Europa. Fortschritte hängen hier wesentlich von privaten Investitionen ab. Solche Aktivitäten können zwar mit europäischen Finanzmitteln unterstützt werden, vieles aber hängt weitgehend von Maßnahmen der Mitgliedstaaten ab. Diese Maßnahmen dürfen jedoch nicht die Budgetdisziplin gefährden.

---

[101] Es solle, so der „Gemeinsame Standpunkt", vor allem eine zügige Zusammenarbeit bei computerbezogenen und computergestützten Straftaten erleichtern werden. Dies solle durch rund um die Uhr besetzte Ansprechstellen bei den Strafverfolgungsstellen - ganz nach dem Vorbild der 24-Stunden-Kontaktgruppe der G-8-Staaten – erreicht werden. Wesentlich sei auch die Erarbeitung einer einheitlichen Regelung darüber, wie lange Daten gespeichert werden können und unter welchen Bedingungen auf sie zugegriffen werden kann. Dadurch solle auch eine grenzüberschreitende Computerfahndung ermöglicht werden.

[102] Vgl KOM (2000) 890, 2.

[103] Siehe dazu das Dokument „eEurope 2002 - vorbereitet von Rat und Europäischer Kommission zur Vorlage auf der Tagung des Europäischen Rates am 19./20. Juni 2000 in Feira vom 14.06.2000, 2. Abrufbar ist das Dokument im Internet unter *http://europa.eu.int/information_society/eeurope/action_plan/pdf/actionplan_de.pdf.*

- Die Anwendung des offenen Koordinierungsverfahrens und des Leistungsvergleichs („Benchmarking“).
  Dies soll sicherstellen, daß die Maßnahmen effizient durchgeführt werden, die gewünschte Wirkung haben und in allen Mitgliedstaaten einen hohen Rang genießen. Außerdem soll dieses Verfahren mit dem allgemeinen Leistungsvergleich koordiniert werden, der in jedem Frühjahr in Zusammenhang mit dem europäischen Sondergipfeltreffen vorgenommen wird.

Bis zum heutigen Zeitpunkt wurden zahlreiche eEurope-Dokumente veröffentlicht, welche sich jedoch allesamt nur generell mit den Risiken und Chancen der Informationsgesellschaft auseinandersetzen, nicht aber im Speziellen auf Internet-bezogene Kriminalität eingehen. Diese Problematik wurde durch eine, ebenfalls unter dem Namen „eEurope2002“ laufende, Parallelinitiative weiterverfolgt.

3.3.2. Der „Internet Action Plan“

Mit einer Entscheidung[104] des Europäischen Parlaments und des Europäischen Rates wurde im selben Jahr der Grundstein für einen großangelegten Aktionsplan gelegt, welcher, als Teil des Programms „eEurope2002, innerhalb der Europäischen Union für mehr Aufmerksamkeit und Transparenz - bezogen auf die Nutzungsmöglichkeiten des Internet und der dadurch hervorgerufenen Gefahren, insbesondere im Bereich der Computer-Kriminalität - hinweisen sollte.
Der Umfang der im Internet vorgehaltenen schädlichen und illegalen Inhalte sei, so die einleitenden Worte zum „Aktionsplan“, zwar begrenzt, könne aber die Schaffung des notwendigen günstigen Umfeldes zum Gedeihen von Initiativen und Unternehmen nachteilig beeinflussen. Auch dem Schutz der Verbraucher wird in dem Sinne Rechnung getragen, daß durch die Bekämpfung der illegalen Nutzung der technischen Möglichkeiten des Internet, insbesondere bei Straftaten gegen Kinder und zum Zwecke

---

[104] „Action Plan on Promoting Safer Use of the Internet“, Entscheidung Nr 276/1999/EG des Europäischen Parlaments und des Rates über die Annahme eines mehrjährigen Aktionsplans der Gemeinschaft zur Förderung der sicheren Nutzung des Internet durch die Bekämpfung illegaler und schädlicher Inhalte in globalen Netzen vom 25.01.1999; im Folgenden „Aktionsplan“ genannt.

des Menschenhandels, oder bei der Verbreitung rassistischen und fremdenfeindlichen Gedankenguts, „ein sichereres Umfeld für die Internet-Nutzung“ geschaffen werde.
Hiezu solle die Gemeinschaft durch spezifische Maßnahmen beitragen, die jene Politik unterstützen und ergänzen, welche von den Mitgliedstaaten im Bereich der Information der Verbraucher über die sicherere Nutzung des Internet verfolgt werde.[105]
In Übereinstimmung mit dem „eEurope 2002“-Programm wird auch im Aktionsplan die besondere Bedeutung, welche Filter- und Ratifizierungssystemen für Internet-Inhalte in der heutigen Zeit zukommt, hervorgehoben. Dies betreffe zB den vom internationalen World-Wide-Web-Konsortium mit Unterstützung der Gemeinschaft initiierten PICS-Standard (*Platform for Internet Content Selection*).[106]

Der Aktionsplan ist mit 31.12.2002 befristet, hat also eine Laufzeit von vier Jahren. Wesentlichstes Anliegen ist es generell, die sicherere Nutzung des Internet zu fördern und auf europäischer Ebene auf ein für die Entwicklung der Internet-Branche günstiges Umfeld hinzuwirken.

Ermöglicht werden soll dies durch Maßnahmen wie zB

- der Schaffung eines europäischen Hotline-Netzes, welches es den Benutzern ermöglichen soll, Inhalte zu melden, auf die sie bei der Nutzung des Internet stoßen und welche sie für illegal halten. Die Verantwortung für die Verfolgung und Bestrafung der für illegale Inhalte Verantwortlichen soll dabei nach wie vor bei den nationalen Strafverfolgungsbehörden liegen. Mit den Hotlines soll nur die Existenz von illegalem Material im Hinblick auf die Eindämmung seiner Verbreitung aufgedeckt werden,

- der Förderung der Selbstkontrolle und von Verhaltenskodizes, wozu eine Ausschreibung zur Auswahl von Organisationen durchgeführt werden soll, die Selbstkontrollorganen bei der Entwicklung und Umsetzung solcher Verhaltensregelungen helfen können. Im Zusammenhang mit der Ausarbeitung von Verhaltenskodizes wird ein System erkennbarer Qualitätskennzeichen für

[105] Vgl Pkt 1-4 der Einleitung zum Aktionsplan.

[106] Vgl Pkt 15 der Einleitung zum Aktionsplan.

Websites gefördert, welches auch den Endnutzern ermöglicht, Anbieter von Internetdiensten zu erkennen, die sich an die Verhaltenskodizes halten und

- der Entwicklung von Filter- und Bewertungssystemen, welche Internet-Inhalte entsprechend einem allgemein anerkannten Schema (beispielsweise zu den Themenkreisen „Sex“ und „Gewalt“) beschreiben, sowie Filtersysteme mit denen der Benutzer auswählen kann, welche Inhalte er erhalten möchte. Bewertungen könnten entweder durch den Inhaltsanbieter zugeordnet oder durch einen unabhängigen Bewertungsdienst vergeben werden.

Weitere Punkte des Aktionsplans stellen zB die Erleichterung internationaler Abkommen über Bewertungssysteme, die Förderung von Sensibilisierungsmaßnahmen, die Koordinierung mit ähnlichen internationalen Maßnahmen und schlußendlich die Evaluierung der Auswirkung der Gemeinschaftsmaßnahmen dar.

3.3.3. Der Endbericht an den Rat der EU

Die Regelungen des eben diskutierten Aktionsplans sind sehr weit und allgemein gehalten und weisen keinen *konkreten* Bezug zur *Bekämpfung* von Internet-Kriminalität als solche mit den Mitteln des (internationalen) Strafrechts auf, bildeten aber die Grundlage für zahlreiche Initiativen und Projekte auf EU-Ebene, welche allesamt schließlich in einem offiziellen Dokument der Kommission der Europäischen Gemeinschaft vom 26.01.2001 präsentiert wurden.
In dieser *Mitteilung der Kommission an den Rat der Europäischen Union*[107] wird Folgendes einleitend festgehalten:

> „Im Lichte der Analyseergebnisse und der Empfehlung der COMCRIME-Studie, der...gezogenen Schlußfolgerungen, der sich durch den Vertrag von Amsterdam bietenden neuen Möglichkeiten, sowie der bereits auf Ebene der EU, der G 8 und des Europarates geleisteten Arbeiten, beleuchtet diese Mitteilung im folgenden verschiedene Optionen für das weitere Vorgehen der EU gegen die Computerkriminalität. Dabei darf die für die EU-Ebene befürwortete

[107] KOM (2000) 9.

Vorgehensweise selbstverständlich weder zu einer Behinderung oder Fragmentierung des Binnenmarkts, noch zu Maßnahmen, die den Schutz der Grundrechte untergraben, führen."

3.3.3.1. Allgemeines zum Inhalt der Mitteilung

Das Papier beschreibt detailliert, welche Maßnahmen gesetzt werden müssen, um Handlungen auf strafrechtlicher Ebene zu begegnen.

Dazu gehöre insbesondere die Bekämpfung von kinderpornographischem Material im Internet, wie es auch der EU-Rat in einem von ihm angenommenen Beschluß zu diesem Thema ausgeführt hat.[108] Weiters anerkennt die Kommission die Bedeutung von Regelungen, welche sich gegen Wirtschaftsdelikte, Spionage und Straftatbestände im Zusammenhang mit dem unberechtigten Zugang zu Computersystemen (Hacking, Computersabotage, der Verbreitung von Computerviren, Ausspähung oder Fälschung von Daten, etc) richten. Das Tatobjekt sei bei diesen Delikten meist nicht physisch greifbar, was auch neue Formen der Täuschung, zB beim Computerbetrug, mit sich bringe, da ja nicht der Mensch, sondern eine Maschine durch Manipulation „getäuscht" werde.[109] Aber nicht nur der Bekämpfung von Kinderpornographie und den verschiedenen Formen des „Hacking" wird durch diese Mitteilung Rechnung gezollt. Es sollen auch Maßnahmen zur Eindämmung von *Rassismus* und *Fremdenfeindlichkeit* im Internet ergriffen werden: Ebenfalls unter dem Titel VI des EU-Vertrags sollte demnach ein Vorschlag ausgearbeitet werden, welcher vor allem Auswertungsergebnisse in bezug auf die Umsetzung der „Gemeinsamen Maßnahme vom 15.07.1996"[110] durch die Mitgliedstaaten berücksichtige.[111] Dies stelle auch im Hinblick des zur Zeit der Veröffentlichung dieser Mitteilung gefällten „Yahoo-Urteils", bzw der Problematik des

---

[108] „Beschluß zur Bekämpfung von Kinderpornographie im Internet", Abl. L 138 v 09.06.2000 S 1; im Internet abrufbar unter *http://europa.eu.int/ISPO/docs/policy/docs/42000X0375/de.pdf*.

[109] Vgl KOM (2000) 14.

[110] „Gemeinsame Maßnahme betreffend die Bekämpfung von Rassismus und Fremdenfeindlichkeit" vom 15.07.1996, Abl. L 185 v 24.07.1996 S 1, im Internet unter *http://europa.eu.int/scadplus/leg/de/lvb/l33058.htm*.

[111] Vgl KOM (2000) 17.

„Geo-Tracking“[112], einen bedeutsamen Aspekt des Kampfes gegen Straftaten im Internet dar.
Es bedürfe weiters globaler, oder zumindest auf EU-Ebene aufeinander abgestimmter und angeglichener Vorschriften, welche dem Opferschutz im Bereich der Computer-Kriminalität dienen und es auch ermöglichen, die Täter zur Verantwortung zu ziehen. So wären beispielsweise bestimmte Bereiche der Rechtshilfe nur dann möglich, wenn die betreffenden Handlungen in beiden beteiligten Ländern strafbar sind.[113]

Im Bereich der Verstöße gegen das *Urheberrecht*, welche ja einen Hauptteil der Internet-Kriminalität ausmache, bezieht sich die Kommission auf eine Richtlinie[114], welche sich mit dem rechtlichen Schutz von Computerprogrammen bzw Datenbanken befaßt und führt weiters aus, welche Maßnahmen in diesem Bereich in der Zukunft noch zu treffen wären.[115]

---

[112] Die Webportal-Firma „Yahoo“ mit Hauptsitz in Kalifornien wurde im April 2000 von den Organisationen LICRA (Ligue internationale contre le racisme et l'antisémitisme) und UEJF (Union des étudiants juifs de France) der nationalsozialistischen Wiederbetätigung angeklagt, da im Yahoo-eigenen Internet-Auktionshaus diverse Nazi-Devotionalien gezeigt und versteigert wurden. Zwar hat das Unternehmen verhindert, daß diese Gegenstände auf der französischen Website angeführt wurden, auf der (offiziellen) amerikanischen Homepage waren dieselben jedoch auch für Internet-Surfer aus Frankreich zugänglich. Mit dem Spruch des französischen Höchstgerichts wurde dem Unternehmen die Pflicht auferlegt, ein System zu schaffen, welches effektiv den Zugriff auf diese Angebote aus Frankreich verhindert. Yahoo Inc. kam der richterlichen Anordnung insoweit nach, als die Gesellschaft nach einer Änderung ihrer Firmenpolitik grundsätzlich die Versteigerung von Gegenständen unterbindet, die – wie Nazi-Memorabilia und Symbole des Ku-Klux-Klan – Hass und Gewalt propagieren; jedoch beantragte Yahoo Inc. vor dem „United States District Court for the Northern District of California“ am 21.12.2000 die Feststellung, daß die Entscheidung des französischen Gerichts von Yahoo Inc. weder zu beachten sei, noch gegen sie vollstreckt werden könne. Ein Jahr später entschied ein US-Gericht allerdings, daß die Firma nur amerikanischem Recht unterstehe, in dem die Meinungsfreiheit einen lockeren Umgang mit Nazi-Relikten und rassistischen Äußerungen erlaube und durch den „Ersten Zusatzartikel“ geschützt sei. Es wies das Urteil des französischen Gerichts aus Gründen der Extraterritorialität zurück.

[113] Vgl KOM (2000) 15 f.

[114] „Richtlinie 91/250/EWG des Rates über den Rechtsschutz von Computerprogrammen“, ABl. L 122 v 17.05.1991 S 41.

[115] Vgl KOM (2000) 14.

Besonders im Bereich des „Internet-Urheberrechts“ ist die Entwicklung einschlägiger Bestimmungen sehr rasch vorangeschritten[116]; die im Mai 2001 verabschiedete „Urheberrechts-Richtlinie“[117] sollte binnen 18 Monaten innerstaatlich umgesetzt werden.

Auch die Arbeit an der, sich zum Zeitpunkt der Erstellung dieser Mittelung noch im Entwurfstadium befindlichen, „*Convention on Cybercrime*“ des Europarats wird gewürdigt und der Wunsch zum Ausdruck gebracht, nicht nur ähnliche, sondern auch weiterreichende Regelungen auf EU-Ebene zu schaffen. Dies sollte in Form eines Legislativvorschlags im Rahmen des Titels VI des Vertrags über die Europäische Union[118], welcher auf die Angleichung der Strafrechtsvorschriften für den Bereich der High-Tech-Kriminalität abstellt, geschehen und sich insbesondere mit der Notwendigkeit einer Vereinheitlichung der Rechtsvorschriften der Mitgliedsstaaten in bezug auf das „Hacking“ oder Angriffe auf sonstige Internet-Dienste im Allgemeinen befassen, wie auch EU-weite Definitionen zu diesem Bereich der Kriminalität enthalten. Für besonders schwere Fälle von Internet-Kriminalität könne der Vorschlag – anders als die „*Convention on Cybercrime*“ – auch *Mindeststrafen* festlegen.
Computerstraftaten und Internet-Kriminalität fielen – so denn ein Pendant zur „Convention on Cybercrime“ auf EU-Ebene erstellt werden würde - unter das Gemeinschaftsrecht, wodurch auch Zwangsmaßnahmen durch die Europäische Union möglich wären.[119]

---

[116] So führte das Europaparlament bereits im März 1999 aus, daß „die Freiheit der privaten Kopie im Informationszeitalter zugunsten einer möglichst weitgehenden Einzelabrechnung zurückzuschrauben (sei) und Ausnahmen vom ausschließlichen Recht der Urheber zur Vervielfältigung und Verbreitung ihrer Werke nur unter der Bedingung erlaubt werden (sollten), daß die Rechtsinhaber eine angemessene Vergütung erhalten“ (vgl *http://www.heise.de/tp/deutsch/special/copy/11547/1.html*).

[117] „Richtlinie 2001/29/EG des Europäischen Parlaments und des Rates zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft“ ABl. L 006 v 10.01.2002 S 71.

[118] Vgl Art 94 EUV: „Der Rat erläßt einstimmig auf Vorschlag der Kommission und nach Anhörung des Europäischen Parlaments und des Wirtschafts- und Sozialausschusses Richtlinien für die Angleichung derjenigen Rechts- und Verwaltungsvorschriften der Mitgliedstaaten, die sich unmittelbar auf die Errichtung oder das Funktionieren des Gemeinsamen Marktes auswirken“.

[119] Vgl KOM (2000) 14.

3.3.3.2. Vereinheitlichung des (Straf-) Verfahrensrechts

Mehr noch als sonstige grenzüberschreitende Straftaten stellen Computerstraftaten aufgrund der ihnen eigenen Geschwindigkeit, Mobilität und Flexibilität eine große Herausforderung auch bei der Schaffung von grenzüberschreitenden *strafverfahrensrechtlichen Bestimmungen* dar. Durch eine Abstimmung und Angleichung der Befugnisse von Strafverfolgungsbehörden aufeinander bzw untereinander sollte gemäß der Mitteilung sichergestellt werden, daß jene in ihrem Zuständigkeitsbereich eigenständige Ermittlungshandlungen durchführen und Amtshilfeersuchen anderer Länder rasch Folge leisten können.[120] Dabei sollte es möglich sein, in Computern gespeicherte Daten landesweit rasch genug ausfindig zu machen und zu beschlagnahmen, um der Vernichtung strafrechtlich relevantem Beweismaterials zuvorzukommen. Die Strafverfolgungsbehörden müßten weiters über Zwangsmittel verfügen, welche es ihnen erlaubten, innerhalb ihres Zuständigkeitsbereiches Computersysteme zu durchsuchen und Daten zu beschlagnahmen, die Aushändigung bestimmter Computerdaten anzuordnen, oder die prompte Aufbewahrung bestimmter Daten gemäß den geltenden rechtlichen (Sicherheits-) Bestimmungen zu bewirken.[121]

Als Anhaltspunkt hierfür könnten die Grundsätze[122] der Gruppe „High-Tech-Kriminalität“, einer von den G 8-Staaten eingesetzten Arbeitgruppe, welche sich bereits mit der Thematik und den Problemen von grenzüberschreitenden Durchsuchungen und Beschlagungen auseinandergesetzt hat, herangezogen werden.[123]

In diesem Zusammenhang sollen die internationalen bzw europäischen polizeilichen Netzwerke, welche effektiv, wenn auch von technischer Seite aus nicht immer ohne Probleme, eine Fahndung von Straftätern ermöglichen, erwähnt werden:

---

[120] Vgl KOM (2000) 17.

[121] Vgl KOM (2000) 27.

[122] „Principles to Combat High-Tech Crime”, im Internet unter *http://www.usdoj.gov/criminal/cybercrime/principles.htm.*

[123] Vgl KOM (2000) 26.

Vorrangig zu nennen sind das Informationsnetz der (deutschen) Polizei „Inpol“ [124], das „neue“ polizeiliche Netzwerk „Inpol-Neu“ und das „Schengener Informationssysten (SIS).

Physikalisch stellt sich beispielsweise das seit 1972 bestehende „Fahndungsnetz“ INPOL als ein sternförmiges Sondernetz für die Übertragung digitaler Daten dar, das die Datenverarbeitungssysteme der (deutschen) Länderpolizeien miteinander verbindet und als Mittelpunkt die Zentral-Datenverarbeitungsanlage des Bundes (ZDVA) im Bundeskriminalamt in Wiesbaden hat.[125] Das System war der modernen Datenflut jedoch längst nicht mehr gewachsen. Regelmäßig stürzten die Computer ab und Abfragen konnten nur nach langen Wartezeiten bearbeitet werden.[126] 1992 wurde schließlich das neue Polizeisystem „*Inpol-Neu*“[127] beschlossen. 130 Personen arbeiteten seit dem Jahr 1996 beim deutschen BKA an dem Projekt, welches vom Erkennungsdienst über die Inhaftierung bis hin zur Organisierten Kriminalität Daten zentral verwalten kann. Das alte System „Inpol“ dient dabei als Vermittlungsstelle für Personendaten, sowie den Einzelheiten zu Straftaten und Tätern.[128]

Das „*Schengener Informationssystem*“[129] ist das Herzstück der Ausgleichsmaßnahmen in Zusammenhang mit dem vollständigen Abbau der Grenzkontrollen an den Binnengrenzen der Schengen-Vertragsstaaten. Diese Datenbankanwendung besteht im Wesentlichen aus dem „Zentralen Schengener Informationssystem“ (C-SIS) und den jeweiligen nationalen Informationssystemen (N-SIS), welche untereinander

---

[124] Vgl dazu beispielsweise nur *Sule*, Europol und europäischer Datenschutz (1999) 39 ff mwN; *Kersten*, Das Labyrinth der elektronischen Karteien, Teil 1 Kriminalistik 6/87, 325 und Teil 2 Kriminalistik 7/87, 357.

[125] Vgl dazu und zu den technischen Details *Ringwald*, INPOL und StA - Zum Abrufrecht der Staatsanwaltschaften aus polizeilichen Datenspeichern (1984).

[126] Vgl „Rasterfahndung – Bedingt fahndungsbereit“, Der Stern-Online unter *http://www.stern.de/computer-netze/news/topnews/artikel_37265.html.*

[127] Näheres bei *Sehr*, INPOL-Neu: System mit Merkmalen eines extremen Wandels, Kriminalistik 1999, 532.

[128] Vgl *Schulzki-Haddouti*, Desaster Inpol-neu - Das neue Polizei-Informationssystem: viel zu teuer, viel zu langsam, c’t 24/2001, 108 f, die auch die Probleme, welche aus technischer Sicht aus dem Speichern und der Abfrage personenbezogener Daten in einer großen Anzahl resultieren, erörtert.

[129] Siehe dazu *Hemesath*, Das Schengener Informationssystem, Kriminalistik 1995, 169; *Werner*, Schengen und Europol, CR 1997, 34; *Schomburg*, Das Schengener Durchführungsübereinkommen, JBl 1997, 560 ff; *Tuffner*, Das Schengener Informationssystem (SIS), Kriminalistik 2000, 39; Schuster, Europäisierung der Polizeiarbeit, Kriminalistik 2000, 79 f.

kommunizieren. Der Betrieb und die Nutzung des SIS wird zusätzlich durch ein „System des ergänzenden konventionellen Informationsaustausches“ (SIRENE) unterstützt. Weiterentwickelt wurde das SIS schließlich zu einem „Europäischen Informationssystem“, welches vor allem Europol ermöglicht, Zugriff auf den europäischen Fahndungsbestand zu erlangen.[130]

3.3.3.3. Zur Überwachung des Telekommunikationsverkehrs

In Pkt 5.1. der Mitteilung wird auch der Notwendigkeit, Regelungen für die Überwachung des Fernmeldeverkehrs zu schaffen, Rechnung gezollt. Infolge der Liberalisierung des Telekommunikationsmarktes und der verstärkten Nutzung des Internet seien zahlreiche Unternehmen in den Markt eingetreten, welche sich ebenfalls mit dieser Problematik, vor allem jener der Aufbewahrung von Vermittlungs- und Inhaltsdaten, auseinanderzusetzen hätten:

> „Die neuen Technologien machen es erforderlich, daß die Mitgliedstaaten zusammenarbeiten, um sich die Möglichkeit der rechtmäßigen Überwachung des Fernmeldeverkehrs zu bewahren. Etwaige neue technische Überwachungsanforderungen der Mitgliedstaaten an die Telekommunikationsbetreiber und Anbieter von Internet-Diensten sollten nach Ansicht der Kommission zuvor auf internationaler Ebene koordiniert werden, um eine Verzerrung des Binnenmarkts zu vermeiden, die Kosten für die Industrie so gering wie möglich zu halten und den Anforderungen in bezug auf den Schutz der Privatsphäre und den Datenschutz gerecht zu werden. Die neuen Standards sollten nach Möglichkeit veröffentlicht und transparent gemacht werden und keine Schwächung der Kommunikationsinfrastrukturen nach sich ziehen.“[131]

Verwiesen wird dabei auch auf die Bestimmungen der „*International User Requirements*“ aus dem Jahre 1995 und somit auf die Verpflichtung der Telekommunikationsbetreiber zur Einrichtung solcher Überwachungsvorkehrungen.
In bezug auf die Speicherung von „Verkehrsdaten“ sollen einzelstaatliche Legislativmaßnahmen, welche die Aufbewahrung von Verkehrsdaten für Strafverfolgungszwecke vorsehen, die Voraussetzung erfüllen, daß die ins Auge

---

[130] Vgl *Sturm*, Das Schengener Durchführungsübereinkommen, Kriminalistik 1995, 168.

[131] KOM (2000) 19.

gefaßten Maßnahmen angemessen, erforderlich und verhältnismäßig sind. Dies gelte insbesondere für Maßnahmen, die eine routinemäßige Aufbewahrung von Daten über einen Großteil der Bevölkerung vorsehen.[132]

Allerdings wird auch den Interessen der Telekommunikationsdiensteanbieter Rechnung getragen, indem ausgeführt wird, daß eine Bekämpfung von Straftaten wie dem „Hacking“ oder dem Computerbetrug nicht durch unverhältnismäßig teure Maßnahmen erreicht werden sollte.[133]

3.3.3.4. Stellungnahmen und Kritiken zur Mitteilung

Stellungnahmen durch alle an der Ausarbeitung dieses Entwurfs beteiligten Länder, bzw der betroffenen Einrichtungen und Organisationen, konnten bis zum 23.03.2001 schriftlich (sogar per E-Mail) an die Kommission gerichtet werden und wurden auf der offiziellen Homepage der EU[134] veröffentlicht. In der „Mitteilung der Ständigen Vertretung Österreichs bei der Europäischen Union“[135] heißt es treffend, daß „die bezügliche Mitteilung der Kommission primär kompilatorischen Charakter aufweist und über bereits bekannte Argumente und Ansätze kaum hinausgeht. Neben der technischen Prävention sollte die klassische Prävention im Bereich der Computerkriminalität nicht vernachlässigt werden.“ Bemängelt wurde, daß der Eindruck entstehe, die Kommission trage im Kontext mit der Speicherung von „Verkehrsdaten“ ausschließlich für Zwecke der Strafverfolgung dem erreichten Diskussionstand nicht vollumfänglich Rechnung und habe diesem nicht in der erforderlichen Klarheit Ausdruck verliehen. Die Einrichtung von Schnittstellen für Überwachungsmaßnahmen und die Aufbewahrung von Verkehrsdaten verursache enorme Kosten, welche von der Industrie nur unwillig getragen würden. Der Ausgleich zwischen den Interessen der Industrie und denen der Strafverfolgungsbehörden solle in Form eines offenen, konstruktiven Dialogs geführt werden. Bezüglich der von der Kommission vorgeschlagenen Einführung von Mindeststrafen für computerbezogene Straftaten habe sich Österreich in den bisherigen

---

[132] In einer Fußnote (No 45) des Berichts wird auch ausdrücklich auf das „Überwachungsnetz Echelon“ und den „Campbell-Bericht“ (vgl oben, FN 21) verwiesen.

[133] Vgl KOM (2000) 22.

[134] Http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/index.htm.

[135] Http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/Comments/Austria.html.

Verhandlungen im Rahmen der EU zur Vereinheitlichung von Strafbestimmungen jeweils mit Nachdruck gegen die Festschreibung von Mindeststrafen im gerichtlichen Strafrecht ausgesprochen, da solche im nationalen Recht nur für besonders schwerwiegende Eingriffe in Rechtsgüter vorgesehen werden sollten. Für vergleichsweise geringfügigere Tatbestände wäre eine solche Maßnahme, auch angesichts der Tatsache, daß das österreichische Recht kein Opportunitätsprinzip kenne, unangemessen.

3.4. Überwachungspflichten nach der „E-Commerce-Richtlinie"?

Mit der „Richtlinie 2000/31/EG des europäischen Parlaments und des Rates vom 08.06.2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt"[136] hat die Europäische Union die Frage nach der rechtlichen Zukunft des elektronischen Handels im Binnenmarkt aufgegriffen. Die Richtlinie, die sich auf Art 47 Abs 2, 55 und 95 EGV stützt, hat sich als vorrangiges Ziel gesetzt, das einwandfreie Funktionieren des Binnenmarktes, insbesondere den reinen Verkehr von Diensten der Informationsgesellschaft zwischen den Mitgliedstaaten, sicherzustellen.[137]

Besondere Bedeutung für das Internet-Strafrecht kommt den Bestimmungen der Art 12 bis 15 der Richtlinie zu, als dort nämlich die „Verantwortlichkeit der Vermittler", also der Access- und Host Provider, wie auch der Betreiber von Proxy-Cache Servern, geregelt wird. Diese Verantwortlichkeitsregelungen beruhen allesamt auf einem System „horizontaler Haftungsbeschränkung", wobei keine Haftungsvoraussetzungen, sondern umgekehrt Haftungsbefreiungsvoraussetzungen normiert werden.[138]

Zur Frage, ob denn Internet-Provider auch Überwachungspflichten träfen, bestimmt Art 15 der Richtlinie daß „die Mitgliedstaaten...Anbietern von Diensten im Sinne der Artikel 12, 13 und 14 *keine allgemeine Verpflichtung auf(erlegen), die von ihnen übermittelten oder gespeicherten Informationen zu überwachen oder aktiv nach Umständen zu forschen, die auf eine rechtswidrige Tätigkeit hinweisen*".

---

[136] ABl L 178 v 17.07.2000 S 1.

[137] Vgl Art 1 EC-RL.

[138] Vgl dazu ausführlich *Zankl*, E-Commerce-Gesetz in Sicht, AnwBl 2001, 459; *ders*, Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 326; *ders*, E-Commerce-Gesetz Rz 9, 24, 40, 48, 50, 180.

Nach Art 15 Abs 2 ist es den Mitgliedstaaten aber durchaus erlaubt, die Diensteanbieter zu verpflichten, die zuständigen Behörden über mutmaßliche rechtswidrige Tätigkeiten oder Informationen der Nutzer ihres Dienstes zu unterrichten. Auch können die Mitgliedstaaten die Anbieter dazu verhalten, den zuständigen Behörden auf Verlangen Informationen herauszugeben, anhand deren die Nutzer, mit denen sie Vereinbarungen über die Übermittlung oder Speicherung von Informationen abgeschlossen haben, ermittelt werden können. Die Bestimmung des § 149a StPO steht also mit dieser Regelung nicht im Widerspruch. Natürlich können, so denn die Voraussetzungen für eine Überwachung des Fernmelde- oder Telekommunikationsverkehrs vorliegen, auch die von der E-Commerce-RL erfaßten Access- und Hostprovider zu einer solchen Datenspeicherung und –Herausgabe verpflichtet werden. Dies wird auch in den „erläuternden Bemerkungen" dieser Richtlinie explizit festgehalten.[139]

Durch das E-Commerce-Gesetz[140], welches am 01.01.2002 in Kraft getreten ist, erfolgte die Umsetzung der E-Commerce-Richtlinie in Österreich. Dabei wurden die Vorgaben der Richtlinie nicht – wie etwa bei der Fernabsatz-Richtlinie[141] – in die jeweils betroffenen Gesetze eingefügt, sondern normativ homogen transformiert.[142]

Beinahe wörtlich wurden die *Haftungsbestimmungen* der Art 12 bis 15 der Richtlinie in die §§ 13 bis 19 ECG übernommen, wobei allerdings zusätzlich Regelungen bezüglich der Verantwortlichkeit der Betreiber von Suchmaschinen (§ 14 ECG), sowie der Haftung für Hyperlinks (§ 17 ECG) einarbeitet wurden.
Art 15 der Richtlinie entspricht § 18 ECG, wobei allerdings in Anbetracht der Tatsache, daß in Österreich (noch) keine ausdrücklichen Verpflichtung zur *Auswertung* und (straf-) rechtlichen *Beurteilung* der gespeicherten Daten durch die Diensteanbieter selbst besteht, eine Umsetzung in Form einer ausdrücklichen Regelung im ECG an sich nicht erforderlich gewesen wäre.[143]

---

[139] Erwägungsgründe 26 und 47.

[140] „Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden", BGBl I 152/2001.

[141] „Richtlinie 97/7/EG des Europäischen Parlaments und des Rates vom 20. Mai 1997 über den Verbraucherschutz bei Vertragsabschlüssen im Fernabsatz (Europäische Fernabsatz-Richtlinie)" ABl. L 144 v 04.06.1997 S 1.

[142] *Zankl*, Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325.

[143] Vgl *Zankl*, E-Commerce-Gesetz Rz 270.

3.5. Die „Europäische Datenschutzrichtlinie“

Für heftige Diskussionen, sowohl auf Seiten der Datenschützer, als auch auf EU-Rats- und Parlamentsebene sorgte der Entwurf einer EU-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation:[144]

Einerseits ging es darum, ob für die Zulässigkeit von elektronischen Massensendungen zu Werbezwecken[145] die Einwilligung des Empfängers im Vorfeld des Versendens vonnöten sei (opt-in), oder ob diese Form kommerzieller Kommunikation[146] generell zulässig ist, der Empfänger sich also *ausdrücklich gegen* den weiteren Erhalt solcher E-Mail aussprechen muß (opt-out),[147] andererseits wurde die Frage der Zulässigkeit der Erfassung und Speicherung von Verbindungsdaten im Telekommunikationsverkehr diskutiert. Während sich bei der „Spam-Abstimmung“ im Europäischen Parlament die Mehrheit der Parlamentarierer zur Zufriedenheit der Datenschützer für das sog „opt-in“-Verfahren aussprachen,[148] einigte man sich bezüglich der Überwachungspflichten durch Internet-Provider auf eine Regelung, welche es der nationalen Gesetzgebung gestattet, diese Thematik *eigenmächtig zu normieren*. Dies stellt insofern eine Überraschung dar, als sich der „Ausschuß für die Rechte und Freiheiten der Bürger“ im Europäischen Parlament am 19.04.2002 auf Vorschlag des Abgeordneten Marco *Capatto*[149] gegen den Ratsvorschlag und dafür, daß in der Richtlinie jeder Bezug auf eine Speicherung der Verbindungsdaten gestrichen werden sollte, aussprach.[150]. An dieser Stelle sei auch angemerkt, daß das Gros der österreichischen Delegation im Europäischen Parlament

---

[144] Vgl den „Gemeinsamen Standpunkt des Rates im Hinblick auf den Erlaß der Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation“ vom 21.01.2001, im Internet unter *http://register.consilium.eu.int/pdf/de/01/st15/15396d1.pdf*.

[145] Sog „Spam-Mails“; vgl dazu die Regelungen in § 101 TKG idF BGBl I 188/1999 bzw § 7 E-Commerce-Gesetz (ECG) BGBl I 152/2001. Siehe dazu mwN *Stomper*, Das österreichische Spam-Verbot nach dem E-Commerce-Gesetz, MR 2002, 45.

[146] Vgl § 3 Z 6 ECG.

[147] Siehe dazu *Zankl*, E-Commerce-Gesetz Rz 117.

[148] Vgl *Grosche*, Entscheidende Spam-Abstimmung im Europäischen Parlament steht bevor, Telepolis, das Magazin für Netzkultur vom 24.05.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/12590/1.html*.

[149] Abgeordneter des Europaparlaments und Berichterstatter für die umstrittene „Datenschutzrichtlinie“.

[150] Vgl *Schulzki-Haddouti*, Europäisches Parlament gegen Speicherung von Verbindungsdaten, Telepolis, das Magazin für Netzkultur vom 19.04.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/12355/1.html*.

als Dreierkoalition SPÖ/ÖVP/FPÖ ihre Stimmen für eine „Überwachungsunion Europa abgegeben haben“[151]; als einziger österreichischer Abgeordneter stimmte Johannes *Voggenhuber* (Die Grünen) für die Beibehaltung der Datenschutzdirektive.[152]
Im Vorfeld dieser Abstimmung wurden zahlreiche Initiativen[153] ins Leben gerufen, da ein „systematisches und präventives Speichern der Kommunikation und der Verbindungsdaten von EU Bürgern die fundamentalen Rechte auf Privatsphäre, Datenschutz, Meinungsfreiheit, Freiheit und Annahme der Unschuld unterminieren würde“.[154]

Im Zuge des Verfahrens der Mitentscheidung (*Kodezisionsverfahren*, Art 251 EUV) wurde also über folgende Bestimmung des Gemeinsamen Standpunktes des EU-Rats[155] im Europäischen Parlament abgestimmt und jene sodann angenommen:

Artikel 15
Anwendung einzelner Bestimmungen der Richtlinie 95/46/EG

(1) Die Mitgliedstaaten können Rechtsvorschriften erlassen, die die Rechte und Pflichten gemäß Artikel 5, Artikel 6, Artikel 8 Absätze 1, 2, 3 und 4 sowie Artikel 9 dieser Richtlinie beschränken, sofern eine solche Beschränkung gemäß Artikel 13 Absatz 1 der Richtlinie 95/46/EG für die nationale Sicherheit, (d. h. die Sicherheit des Staates), die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder des unzulässigen Gebrauchs von elektronischen Kommunikationssystemen notwendig ist. Zu diesem Zweck können die Mitgliedstaaten unter anderem vorsehen, dass die Daten aus den in diesem Absatz aufgeführten Gründen während einer begrenzten Zeit gemäß den allgemeinen Grundsätzen des Gemeinschaftsrechts aufbewahrt werden.

---

[151] ORF-Futurezone vom 05.06.2002 unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=121778&tmp=70744*.

[152] Vgl „Ein Gerechter in Sodom“, Quintessenz – Newsticker vom 01.06.2002 unter *http://www.quintessenz.org/cgi-bin/index?funktion=view&id=000100002047*.

[153] Beispielsweise durch die Bürgerrechtsgruppe „Stop1984” (*http://www.stop1984.com/index2.php*). Siehe dazu auch die – sich ein wenig reißerisch präsentierende – Berichterstattung des österreichischen Online-Datenschutzmagazins „Quintessenz.at“ unter *http://www.quintessenz.at/cgi-bin/index?funktion=view&id=000100002019.*

[154] „Letter to Mr. Pat Cox on Data Retention, May 22, 2002” unter *http://www.gilc.org/cox_de.html.*

[155] FN 987.

Es wird also den *Mitgliedsstaaten selbst* die Möglichkeit eingeräumt, Telekom- und Internetanbieter *zu verpflichten*, Verkehrs- und Verbindungsdaten der Nutzer[156] für einen unbestimmten Zeitraum aufzubewahren. Die Mitgliedsstaaten dürfen demnach datenschutzrechtliche Bestimmungen nur zur Verbrechensbekämpfung oder zum Schutz der öffentlichen oder nationalen Sicherheit „umgehen", wenn die durchzuführende Maßnahme innerhalb einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig ist.

Die Konsequenzen dieser Entscheidung auf EU-Ebene ließen nicht lange auf sich warten: So wurde zB im deutschen Bundesrat ein Gesetzentwurf „zur Verbesserung der Ermittlungsmaßnahmen wegen des Verdachts sexuellen Mißbrauchs von Kindern" mit der Mehrheit der Union-geführten Länder angenommen.[157] Weiters soll die bisherige Höchstspeicherfrist für Nutzungs- und Verbindungsdaten in eine Mindestspeicherfrist umgewandelt werden. Bemerkenswert an diesem Gesetzesentwurf ist auch, daß demnach nicht der Gesetzgeber, sondern die Exekutive per Rechtsverordnung den Zeitraum festlegen kann, in welchem Internet-Provider Zugangs- und Verbindungsdaten speichern müssen.[158]

4. Initiativen des Europarats

4.1. Die Vorarbeiten zur „Convention on Cyber-Crime"

Eine der treibenden Kräfte auf dem Gebiet der europäischen Rechtsangleichung ist der Europarat, dem zur Zeit 43 Staaten angehören. Gesetzgeberisch tätig wird der Europarat durch den Erlaß von Konventionen, denen für die unterzeichnenden Mitgliedstaaten

---

[156] Vgl Art 6 Richtlinie.

[157] In diesem Gesetzesentwurf wird normiert, daß die Überwachung der Telekommunikation und des Internet in Deutschland auch schon bei Vorliegen des Verdachts von Straftaten des sexuellen Mißbrauchs von Kindern und des Verbreitens (kinder-) pornografischer Schriften möglich ist; vgl dazu „Bundesrat will erweiterte Überwachung der Kommunikation" – Heise-Newsticker vom 31.05.2002 unter *http://www.heise.de/newsticker/data/fr-31.05.02-000/.*

[158] Vgl *Schulzki-Haddouti*, Bundesrat segnet Vorratsspeicherung ab, Telepolis, das Magazin für Netzkultur vom 31.05.2002 *unter http://www.heise.de/tp/deutsch//inhalt/te/12642/1.html.*

völkerrechtliche Verbindlichkeit zukommt.[159] Neben zahlreichen Empfehlungen zum Thema Datenschutz[160] und der Wahrung von Minderheitenrechten im Internet[161], wurde von den Expertengruppen des Europarats jene Vorarbeit geleistet, welche schließlich am 23.11.2001 zur Unterzeichnung der entgültigen Version der „Convention on Cyber-Crime" durch Minister und hohe Beamte aus 26 Europaratsländern, sowie den USA, Kanada, Japan und Südafrika führte. Bereits zwei Wochen zuvor hatten die Außenminister der 43 Europarats-Mitglieder dem lang geplanten Cybercrime-Abkommen zugestimmt.[162]

4.1.1. Die „Recommendation No. R (89) 9"

Eine erste Diskussion über die Einführung von Zwangsmaßnahmen im Bereich der Computer-Kriminalität wurde vom „*Select Committee of Experts on Computer-Related Crime*" des Europarats eingeleitet, welche sich jedoch vorerst nur mit generellen Fragen der Strafverfolgung beschäftigte. So wurde im „Final Report" [163] bekräftigt, daß in Zukunft die Harmonisierung von Zwangsmaßnahmen auf europäischer Ebene im Mittelpunkt der Bemühungen um die Schaffung von Regelungen betreffend der mißbräuchlichen Verwendung von Computersystemen stehen müsse.
Dieser Report wurde dann im Jahr 1999 vom Europäischen Kommitee für Verbrechensbekämpfung auf seiner 38. Plenarsitzung vorgestellt. Die „Recommendation No. R (89) 9"[164] empfahl den Mitgliedstaaten, den Report, welcher von der Arbeitsgruppe in den Jahren 1985 bis 1989 ausgearbeitet wurde, bei der

---

[159] Vgl *Bremer*, Strafbare Internet-Inhalte 179.

[160] Beginnend mit der „Convention for the Protection of Individuals with Regard to the Automatic Procession of Data" aus dem Jahr 1968 wurden zahlreiche Empfehlungen zu diesem Thema erlassen. Vgl auch die Nachweise bei *Sule*, Europol und europäischer Datenschutz 51 ff und *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society 146 ff, sowie auf der Hompepage des Europarats unter *http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm*.

[161] ZB der „Recommendation No R (97) 19" und der „Recommendation No R (97) 20".

[162] Vgl den Heise-Newsticker vom 23.11.2001 unter *http://www.heise.de/newsticker/data/hod-23.11.01-001/.*

[163] „Report On Computer-Related Crime" des „European Committee on Crime Problems", näheres bei *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society 158 f, 177.

[164] Http://cm.coe.int/ta/rec/1989/89r9.htm.

innerstaatlichen Realisierung der neuen Computerstraftatbestände zu berücksichtigen und gleichzeitig dem Generalsekretär des Europarats Bericht über die Fortschritte hinsichtlich der Entwicklungen in der nationalen Gesetzgebung zu erstatten.
Zusätzlich in die Arbeit des „*European Committe On Crime Problems*“ (CDPC)[165] einbezogen wurde ein von ihr in Auftrag gegebener und von Professor H.W.K. *Kaspersen* erarbeiteter Report,[166] in dem festgehalten wird, daß es nicht ausreiche, Empfehlungen zu verabschieden, sondern ein verbindlicheres Rechtsinstrument, wie zum Beispiel eine Konvention, geschaffen werden solle. Diese solle sich dann nicht nur mit den Fragen des materiellen Rechts auseinandersetzen, sondern vor allem auch Regelungen in bezug auf die *formelle Verfolgbarkeit von Computerstraftaten* enthalten.

4.1.2. Die „Recommendation No. R (95) 13“

Zwei Jahre nach der Adaptierung der Empfehlung No. R (89) 9 wurde ein neues „*Select Committee on Procedural Law Problems Connected with Computer-Related Crime*“ (PC-PC) gegründet und 1991 beim Europarat eingerichtet. Als Ergebnis ihrer Arbeit präsentierte dieses Komitee schließlich die „Recommendation No. R (95) 13“[167], in welcher für den damaligen Zeitpunkt schon recht umfassend die Probleme, welche sich auf prozessualer Ebene bei der Verfolgung von Straftaten in Zusammenhang mit der Informationsgesellschaft stellen, erörtert wurden.[168]

4.1.3. Das dritte „Computer-Crime Committee on Crime in Cyberspace”

Im Jahre 1997 wurde die bislang letzte Expertengruppe „*Committee of Experts on Crime in Cyberspace*“ (PC-CY) mit dem Auftrag, eine „International Treaty to Fight

---

[165] So nannte sich das Expertenkomitee in den Folgejahren.

[166] „Implementation of Recommendation No R (89) 9 on computer-related crime”, Report prepared by Professor Dr. H.W.K. *Kaspersen* (doc. CDPC (97) 5 und PC-CY (97) 5, 106).

[167] Im Internet unter *http://cm.coe.int/ta/rec/1995/95r13.htm*.

[168] Vgl dazu umfassend *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society 177 ff.

Internet-Crime“ zu erarbeiten,[169] eingesetzt. [170] In diesem Abkommen sollten Verstöße gegen Rechtsvorschriften im Internet, unter besonderer Berücksichtigung der technischen Möglichkeiten zur Strafverfolgung und der Fragen in bezug auf grenzüberschreitende Ermittlungsmaßnahmen in Netzwerken, einer Regelung unterzogen werden.[171]

4.2. Die „Convention on Cyber-Crime“

Die Gruppe PC-CY nahm ihre Arbeit im April 1997 auf und begann mit den Verhandlungen zum Entwurf einer internationalen Konvention gegen Computer-Kriminalität. Eigentlich hätten diese Arbeiten bis zum 31.12.1999 beendet werden sollen; da es jedoch grundlegende Probleme bei der Aushandlung bestimmter Regelungen der Konvention gab, wurde diese Frist bis zum 31.12.2000 erstreckt.[172] Mit Unterstützung der „European Ministers Of Justice“ wurden jedoch etliche dieser Probleme, welche vor allem die Rechtsangleichung zwischen den Mitgliedsstaaten des Europarats betrafen, ausgeräumt. Unterstützung gab es auch von Seiten der Europäischen Union, welche ihr Interesse an der Konvention durch eine „Joint Position“ vom Mai 1999 zum Ausdruck brachte.[173]

Im Zeitraum vom April 1997 bis zum Dezember 2000 fanden zahlreiche Treffen des PC-CY statt, denen nach Ablauf der eigentlichen Frist - welche zur Fertigstellung der Konvention eingehalten werden sollte - noch drei weitere folgten, um den Konventionsentwurf im Rahmen einer Parlamentarischen Versammlung einer weiteren Begutachtung zu unterziehen.

Die erste „Draft Convention On Cyber-Crime“ wurde im April 2000 freigegeben und veröffentlicht. Es folgten jedoch noch zahlreiche weitere Konventionsentwürfe, um den

---

[169] Vgl *Bremer*, Strafbare Internet-Inhalte in internationaler Hinsicht 179.

[170] Vgl die „Decision CM/Del/Dec(97)583”, beschlossen am Treffen No 583 des Ministerrates vom 04.02.1997.

[171] Vgl *Sieber*, Legal Aspects of Computer-Related Crime in the Information Society 180.

[172] Vgl die „Decision No CM/Del/Dec (99) 679” des Ministerkomitees.

[173] Vgl den „Final Activity Report” des PC-CY zu einer „Draft Convention On Cyber-Crime and Explanatory Memorandom Related Thereto”, welcher dem European Committee On Crime Problems (CDPC) am 18.06.2001 vorgelegt wurde, 38. Im Internet ist der Report unter *http://conventions.coe.int/treaty/EN/projets/cybercrime27.doc* abrufbar.

Mitgliedsstaaten des Europarats die Möglichkeit einzuräumen, zu den einzelnen Regelungen Stellung zu beziehen.

Da es nicht sehr zweckdienlich wäre, die Entstehungsgeschichte aller 27 (!) „Draft Conventions on Cyber-Crime“, und den Inhalt der jeweiligen Begutachtungs- und Beurteilungsverfahren an dieser Stelle aufzuzeigen, soll durch eine einfache „Zeittafel“ die Entwicklung innerhalb des letzten Jahres bis zur Unterfertigung der endgültigen Version der Konvention schematisch dargestellt werden:

- Erläuternde Bermerkungen „Draft Explanatory Memorandum to the Draft Convention on Cyber-Crime” am 14.02.2001 veröffentlicht.[174]

- Stellungnahme 4/2001 der „Art. 29 Gruppe der EU“ zum Entwurf einer Konvention des Europarats über Cyberkriminalität vom 22.03.2001.[175]

- Bericht an das „Committee on Legal Affairs and Human Rights” zur CyberCrime-Konvention vom 10.04.2001.[176]

- Bericht des Ausschusses für Recht und Menschenrechte an die Parlamentarische Versammlung des Europarates vom 10.04.2001.[177]

- Debatte in der Parlamentarischen Versammlung zur Cyber-Crime-Konvention am 24.04.2001.[178]

- Abgesandte im Ministerrat billigen Cyber-Crime-Konvention am 17.09.2001.[179]

---

[174] Http://www.federcomin.it/sviluppo/Produzio.nsf/all/E0D008962729F58AC12569FA00695752/$file/COE_Cybercrime_explanatory_feb2001.doc.

[175] Http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp41en.htm.

[176] Http://stars.coe.fr/doc/doc01/EDOC9031.htm.

[177] Http://stars.coe.fr/doc/doc01/EDOC9031.htm.

[178] Http://stars.coe.int/verbatim/200102/E/0104241500E.htm.

[179] Http://press.coe.int/press2/press.asp?B=30,0,0,0,0&M=http://press.coe.int/cp/2001/646a(2001).htm.

- Bericht des „Committee on Legal Affairs and Human Rights" gegenüber der Parlamentarischen Versammlung „Racism and xenophobia in cyberspace" vom 12.10.2001.[180]

- Unterzeichnung der Cyber-Crime Konvention im Ministerrat am 08.11.2001.[181]

Die überarbeitete und endgültige Version des Entwurfs wurde im Juni 2001 dem CDPC zu dessen Billigung übersandt, wonach der Text der Konvention beim Ministerkomitee zur Eröffnung des Unterschriftenverfahrens eingereicht wurde.[182]
Nach beinahe endlosen Querelen[183] mit Datenschutz- und Bürgerrechtsorganisationen wurde schließlich am 23. November 2001 die „Convention on Cyber-Crime" von den Vertretern der Mitgliedsländer des Europarats unterzeichnet.[184]

4.2.1. Gliederung des Abkommens

Die Konvention[185] besteht aus fünf Kapiteln, die in Abschnitte unterteilt sind. Die Gliederung der Abschnitte erfolgt in verschiedene Titel, welche die 48 Artikel des Übereinkommens beinhalten.

---

[180] Http://stars.coe.fr/doc/doc01/edoc9263.htm.

[181] http://press.coe.int/press2/press.asp?B=30,0,0,0,0&M=http://press.coe.int/cp/2001/820a(2001).htm.

[182] Vgl „Explanatory Memorandum" (FN 1017) 38, nach eigener Übersetzung. Es existiert von den Erläuternden Bemerkungen zur Konvention eine Arbeitsübersetzung aus dem Englischen, welche jedoch nicht vollständig ist, da nur Teile des Originaldokuments ins Deutsche übertragen wurden: *Ebinger/Klinger-Mertens/Newton*, Entwurf des Erläuternden Berichts zum Entwurf eines Übereinkommens über Datennetzkriminalität, im Internet unter *http://www.sicherheit-im-internet.de/download/cc-dt-erlaeuterungen.pdf.*

[183] Siehe dazu beispielsweise *http://www.heise.de/tp/deutsch/html/such.html?T=Cybercrime+Europarat*.

[184] Http://www.legal.coe.int/economiccrime/Default.asp?fd=cybercrime&fn=
Conf(Budapest2001)Docs.htm.

[185] Vorweg sei festgehalten, daß leider noch keine offizielle Übersetzung der Konvention aus dem Englischen seitens des Europarats veröffentlicht wurde. Es existiert aber eine Arbeitsübersetzung des (deutschen) BMJ, welche auch im Rahmen dieser Dissertation verwendet wurde: *Huttner-Thompson*, Arbeitsübersetzung der „Draft Convention On Cyber-Crime and Explanatory Memorandum Related Thereto", *http://www.uni-frankfurt.de/fb01/bizer/rechtsquellen/CyberCrime/CyberCrimeKonvention(21-05-01).pdf.*

Kapitel I enthält die Erklärungen zu den in der Konvention verwendeten Begriffen, während Kapitel III unter der Überschrift „*Internationale Zusammenarbeit*“ die Grundsätze der *Auslieferung* (Artikel 24) und *Rechtshilfe* (Artikel 25 ff) enthält. Dazu gehören auch Bestimmungen über die „Rechtshilfe beim Zugriff auf gespeicherte Computerdaten“ (Artikel 30), die Rechtshilfe bei der „Echtzeit-Erhebung von Verbindungsdaten“ (Artikel 33), sowie die „Rechtshilfe beim Abfangen von Inhaltsdaten“ (Artikel 34).
Näher eingegangen wird im Rahmen dieser Arbeit vor allem Kapitel II der Konvention - betitelt „*Maßnahmen auf nationaler Ebene*“ - welcher materielle und formelle Regelungen zur Verfolgung von Internet-Kriminalität beinhaltet.

4.2.2. Kapitel II, Abschnitt 1: Materielles Strafrecht

- Titel 1 - Straftaten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und –Systemen:

Hier finden sich jene Straftatbestände[186] im Zusammenhang mit Computer-Kriminalität, auf deren Grundlage die Vertragsparteien Regelungen im jeweils nationalen Recht erstellen sollen. Dies sind:
Der „Rechtswidrige Zugriff“ auf ein Computersystem (Art 2), das „Rechtswidrige Abfangen“ nichtöffentlicher Computerdaten (Art 3), die Eingriffe in Daten bzw Computersysteme (Art 4, 5) und der „Mißbrauch von Vorrichtungen“, welche es ermöglichen in ein Computersystem einzudringen, oder Paßwörter und Zugangscodes auszukundschaften (Art 6).

- Titel 2 – Computerstraftaten:

Unter diesem Titel finden sich die Tatbestände der „Computerurkundenfälschung“ (Art 7) und des „Computerbetrugs“ (Art 8).

- Titel 3 – Inhaltsbezogene Straftaten:

[186] Diese seien an dieser Stelle nur der Vollständigkeit halber und im Überblick genannt.

In Art 9 findet sich eine umfangreiche Regelung zur Pönalisierung von „Straftaten in bezug auf Kinderpornographie".

- Titel 4 enthält Regelungen betreffend „Straftaten im Zusammenhang mit Verletzungen des Urheberrechts und verwandter Schutzrechte" und unter den Titel 5 fallen „Nebenformen der Verantwortlichkeit und Sanktionen".

Im Zuge der laufenden Anpassung der österreichischen Strafrechtsordnung an die Bedürfnisse moderner Formen der Kommunikation hat auch die „Cybercrime Konvention" Einzug in das „Strafrechtsänderungsgesetz 2002"[187] gehalten. Vorerst sollen dabei die eigentlichen Computerdelikte - also die unerlaubten Angriffe auf Computersysteme, sowie die Begehung herkömmlicher Straftaten mit Hilfe von Computersystemen - in eine Strafrechtreform einfließen, bevor schließlich auch die restlichen materiellen Bestimmungen umgesetzt werden.[188]

4.2.3. Kapitel II, Abschnitt 2: Verfahrensrecht

4.2.3.1. Allgemeines

Die formellrechtlichen Bestimmungen der Konvention beziehen sich im allgemeinen auf alle Arten von Daten, einschließlich der drei verschiedenen Arten von Computerdaten (Verbindungsdaten, Inhaltsdaten und Kundendaten), die in zweierlei Form vorhanden sein können: als gespeicherte oder sich im Übertragungsprozeß befindliche Daten.[189]
Im Sinne des Übereinkommens (Art 1 lit d) versteht man unter „*Verbindungsdaten*"

- „alle Computerdaten in Zusammenhang mit einer Kommunikation mit Hilfe eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war,

[187] BGBl I 134/2002.

[188] Vgl die EB zum ME-StRÄG 2002, 19.

[189] Explanatory Memorandum zur Convention on Cyber-Crime Rz 123.

erzeugt wurden und aus denen Ursprung, Bestimmung, Leitweg, Uhrzeit, Datum, Umfang oder Dauer der Kommunikation oder die Art des Trägerdienstes hervorgehen".

Dies stellt eine Auflistung jener Kategorien von Daten dar, welche im Sinne der Konvention besonderer Kontrolle bedürfen: der Ursprung einer Kommunikation, ihre Bestimmung, der zurückgelegte Weg der Daten, die Uhrzeit des Versendens, ihre Größe oder Länge etc, wobei sich der Ausdruck „Ursprung" beispielsweise auf eine Telefonnummer oder eine IP-Adresse und die Bezeichnung „Bestimmung" auf die Adresse des jeweilige Endgeräts, wohin Daten verschickt werden, bezieht.[190]
Diese Definition von „Verbindungsdaten" stellt es den Mitgliedstaaten jedoch ins eigene Ermessen, weitere Unterscheidungen bezüglich ihres Schutzes, abhängig von der Sensitivität der Daten, zu treffen.[191]

Während die Konvention keine eigene Definition von Inhaltsdaten enthält,[192] fallen unter „*Kundendaten*" (Art 18 Abs 3)

- „alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Kunden seiner Dienste vorliegen, mit Ausnahme von Verbindungsdaten oder inhaltsbezogenen Daten, durch die folgendes festgestellt werden kann:
  a) die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Maßnahmen und die Dienstdauer;
  b) die Identität des Kunden, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer, sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen.
  a) gegebenenfalls andere Informationen über den Ort der Installation der Kommunikationsanlage, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen".

---

[190] Vgl Explanatory Memorandum Rz 30, nach eigener Übersetzung.

[191] Vgl Explanatory Memorandum Rz 31, nach eigener Übersetzung.

[192] Es wird nur allgemein der Begriff der „Computerdaten" (Art 1 lit b) erklärt, von denen dann Verbindungs- bzw Kundendaten abzugrenzen sind. Der Begriff „Inhaltsdaten" bezieht sich aber auf die Übertragung des Kommunikationsinhalts, dh auf die Bedeutung oder den Tenor der Kommunikation, Nachricht oder Information, die im Wege der Kommunikation übertragen wird. Alle Elemente, die keine Verbindungsdaten darstellen, werden als Teil der Kommunikation übermittelt (Explanatory Memorandum Rz 194, 214).

Grundsätzlich sind Kundendaten all jene Informationen, über die der Administrator eines Diensteanbieters verfügt und die sich auf die Kunden seiner Dienste beziehen. Sie stellen jedoch keine Verbindungs- und Inhaltsdaten dar. Kundendaten können Informationen sein, die in Form von Computerdaten oder in Form von Schriftstücken vorliegen.[193] Diese Definition wird wohl auch all jene Merkmale beinhalten, welche das Telekommunikationsgesetz[194] zur Bestimmung von „Stammdaten", also personenbezogener Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter von Telekommunikationsdiensten oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind, vorgibt.

Im Laufe eines strafrechtlichen Ermittlungsverfahrens können Kundendaten in *zwei bestimmten Fällen* benötigt werden: Im ersten Fall um festzustellen, welche Dienste und darauf bezogene technische Einrichtungen von dem Kunden genutzt worden sind, wie beispielsweise die Art des verwendeten Telefondienstes (zB Mobiltelefon), die Art anderer genutzter zugeordneter Dienste (zB Rufumleitung, Voicemail, usw), oder Telefonnummern und andere technische Adressen (zB E-Mail-Adressen). Im zweiten Fall werden Kundendaten benötigt, um, wenn eine technische Anschrift bekannt ist, einen Beitrag zur Feststellung der Identität des Betroffenen zu leisten.[195]

4.2.3.2. Erfassung und Überwachung gespeicherter Computerdaten

Artikel 16 (1) der Konvention bestimmt, daß jede Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen muß, damit ihre zuständigen Behörden die *beschleunigte Sicherung bestimmter Computerdaten*, einschließlich *Verbindungsdaten*, die mittels eines Computersystems bereits *gespeichert* wurden, anordnen, oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, daß bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

„Sicherung" bedeutet, daß Daten, die bereits in gespeicherter Form existieren, gegen jene Eingriffe geschützt werden, die ihre gegenwärtige Eigenschaft oder Beschaffenheit

---

[193] Vgl Explanatory Memorandum Rz 162.

[194] § 87 (3) Z 4 TKG.

[195] Vgl Explanatory Memorandum Rz 163.

verändern oder verschlechtern könnten. Dies umfaßt eine Sicherung gegen Änderung, Schädigung oder Löschung, bedeutet aber nicht unbedingt, daß die Daten „eingefroren" (dh unzugänglich gemacht) werden müssen und von rechtmäßigen Benutzern somit nicht mehr verwendet werden können. Die Person, an die die Anordnung gerichtet ist, kann immer noch auf die Daten zugreifen. Der Artikel schreibt nicht vor, wie die Daten zu sichern sind. Dies bleibt jeder Vertragspartei selbst überlassen.[196] Die Befugnis, die beschleunigte Sicherung von Computerdaten anzuordnen oder auf andere Weise zu bewirken, gilt für *alle Arten gespeicherter Computerdaten*.[197]
Nur für *Verbindungsdaten* gilt jedoch Artikel 17, welcher besondere Verpflichtungen in bezug auf die Sicherung und die rasche Weitergabe von *Verbindungsdaten* schafft, sodaß festgestellt werden kann, ob noch weitere Diensteanbieter an der Übertragung bestimmter Kommunikationsvorgänge beteiligt waren. Von besonderer Bedeutung kann eine solche Verpflichtung für die Feststellung der Quelle oder des Ziels einer *vergangenen* Kommunikation sein, insbesonders für die Entdeckung von Personen, die zB kinderpornographisches Material oder Computerviren verbreitet, oder einen rechtswidrigen Zugriff auf Computersysteme versucht, oder vollendet haben.[198]

Artikel 18 enthält Bestimmungen hinsichtlich der *Herausgabe* „bestimmter Computerdaten", bzw – für Diensteanbieter[199] – „Kundendaten", an die zuständige Behörde im Wirkungsbereich ihres Hoheitsgebiets[200] und Artikel 19 trifft Regelungen in bezug auf die *Durchsuchung und Beschlagnahme gespeicherter* Computerdaten:

---

[196] Vgl Explanatory Memorandum Rz 143.

[197] Vgl Explanatory Memorandum Rz 145.

[198] Vgl Explanatory Memorandum Rz 150 f.

[199] Art 18 verpflichtet den Diensteanbieter jedoch nicht, *Kundendateien* zu führen. Er haftet nach dem Übereinkommen auch *nicht* für die Richtigkeit seiner Angaben. Dies bedeutet, daß ein Diensteanbieter nicht verpflichtet ist, zB personenbezogene Daten von Nutzern sogenannter „Prepaid Cards" für mobile Telefondienste aufzunehmen. Er ist auch nicht verpflichtet, die Identität der Kunden zu überprüfen, oder seinen Kunden den Gebrauch von Pseudonymen zu verbieten (vgl Explanatory Memorandum Rz 166).

[200] Auf dem Gebiet der Elektronik und insbesondere im Online-Bereich könne eine Herausgabeanordnung bisweilen als Maßnahme im Vorfeld eines Ermittlungsverfahrens eingesetzt werden, die weiteren Maßnahmen, wie der Durchsuchung und Beschlagnahme, oder dem Echtzeit-Abfangen sonstiger Daten, vorausgeht (Explanatory Memorandum Rz 160).

Danach soll jede Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um ihren zuständigen Behörden die Befugnis zu erteilen, ein Computersystem oder einen Teil davon, sowie die darin gespeicherten Computerdaten und einen Computerdatenträger, auf dem Computerdaten gespeichert sein können, in ihrem Hoheitsgebiet zu *durchsuchen* oder in ähnlicher Weise darauf Zugriff zu nehmen (Abs 1). Des weiteren soll jede Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen treffen, um ihren zuständigen Behörden die Befugnis zu erteilen, Computerdaten, auf die Zugriff genommen wurde, zu *beschlagnahmen* oder in ähnlicher Weise sicherzustellen (Abs 3).

Diese Bestimmung soll dazu dienen, die innerstaatlichen Rechtsvorschriften über die *Durchsuchung und Beschlagnahme gespeicherter Computerdaten* zum Zweck der Erlangung von Beweismaterial für bestimmte Ermittlungen oder Verfahren in Strafsachen zu modernisieren und zu vereinheitlichen. Sie stellt die Entsprechung zu den traditionellen Durchsuchungs- und Beschlagnahmebestimmungen dar,[201] da das Sammeln von Daten im Verlauf der Durchsuchung erfolgt und sich auf Daten bezieht, die zu diesem Zeitpunkt *bereits vorhanden* sind. Die Voraussetzungen für die Erlangung der gesetzlichen Befugnis zur Vornahme einer Durchsuchung bleiben dieselben wie bei der Beschlagnahme körperlicher Gegenstände, unabhängig davon, ob die Daten nun in greifbarer, oder in elektronischer Form vorliegen. Es kann aber dennoch - aufgrund der Vernetzung zwischen Computersystemen - der Fall sein, daß Daten zwar nicht in dem bestimmten, gerade durchsuchten, Computer gespeichert sind, aber über das betreffende System leicht zugänglich gemacht werden können. Jene Daten könnten in einer zugeordneten Datenspeichervorrichtung gespeichert sein, die mit dem Computer entweder direkt oder indirekt über ein Kommunikationssystem, wie zB dem Internet, verbunden ist. Dies macht es möglicherweise erforderlich, neue Rechtsvorschriften zu erlassen, die eine Ausweitung der Durchsuchung auf den Ort, an dem die Daten tatsächlich gespeichert sind (oder eine Rückführung der Daten von diesem Ort an den durchsuchten Computer), ermöglichen.[202]

---

[201] Vgl Explanatory Memorandum Rz 169.

[202] Vgl Explanatory Memorandum Rz 171 f.

4.2.3.3. Echtzeit-Erhebung von Vermittlungs- und Inhaltsdaten

Im Laufe ihrer Erarbeitung nicht unumstritten waren die Bestimmungen der Artikel 20 und 21 der Konvention, welche die „*Echtzeit-Erhebung von Verbindungsdaten*“ bzw das „*Abfangen von Inhaltsdaten*“ betreffen: So wünschten sich im Rahmen des Ratifizierungsverfahrens zwei Delegationen, daß entsprechende Vorbehaltsklauseln eingefügt werden, nach denen diese Bestimmungen im jeweils innerstaatlichen Recht auf bestimmte Arten von Diensteanbietern nicht angewendet werden können.[203]
Geregelt wird die Sammlung von Beweisdaten, die im *Zeitpunkt der Datenübertragung* (dh in „Echtzeit“) erfaßt werden. Daten sind naturgemäß immateriell und bestehen zB als Stimmübertragungen oder Übertragungen elektronischer Impulse. Der Datenfluß wird durch die Erfassung und Überwachung nicht nachhaltig gestört; er erreicht den gewünschten Empfänger. Daten werden dabei nicht physikalisch in Besitz genommen, sondern bei der Übertragung aufgezeichnet (kopiert).[204]

Art 20 (1) der Konvention, betitelt „*Echtzeit-Erhebung von Verbindungsdaten*“, lautet demnach:

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden die Befugnis zu erteilen,

a) Verbindungsdaten, die mit bestimmten, in ihrem Hoheitsgebiet mittels eines Computersystems übertragenen Kommunikationen, in Zusammenhang stehen, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und
b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,

(i) solche Verbindungsdaten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder
(ii) bei der Erhebung oder Aufzeichnung solcher Verbindungsdaten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

Die Bestimmung bezieht sich grundsätzlich auf jede Straftat nach dem Übereinkommen. Artikel 14 Absatz 3 normiert jedoch, daß eineVertragspartei sich das Recht vorbehalten kann, die Maßnahme nur in bezug auf die in dem Vorbehalt angegebenen Straftaten

---

[203] Vgl „Draft Convention On Cyber-Crime and Explanatory Memorandum Related Thereto (Rev 27)”, Anmerkung zu den Artikeln 20 und 21.

[204] Vgl Explanatory Memorandum Rz 193.

anzuwenden, sofern der Umfang der Straftaten nicht eingeschränkter ist, als derjenige, auf den sie die Maßnahme des Abfangens von Inhaltsdaten anwendet. Ungeachtet dessen soll jede Vertragspartei, die einen solchen Vorbehalt macht, die Erfassung von Verbindungsdaten weitgehendst ermöglichen.[205] Laut „Explanatory Memorandum“[206] würden einige Staaten die in dem Übereinkommen festgelegten Straftaten normalerweise nicht als hinreichend schwer ansehen, um das Abfangen von Inhaltsdaten,,von oder in manchen Fällen sogar die Erfassung von Verbindungsdaten zu genehmigen. Dennoch seien derartige Verfahren für die Ermittlung einiger der in dem Übereinkommen festgelegten Straftaten, wie etwa Handlungen, die den rechtswidrigen Zugriff auf Computersysteme, sowie das Verbreiten von Viren und Kinderpornographie betreffen, oft unerläßlich. Die „Störungsquelle“ könne in manchen Fällen nicht ohne die Echtzeit-Erfassung von Verbindungsdaten bestimmt werden. Bisweilen sei es nicht möglich, die Art bestimmter Kommunikationsformen ohne das Echtzeit-Abfangen von Inhaltsdaten zu entschlüsseln. Daher sollte der Gebrauch technologischer Mittel zur Überwachung von Vermittlungsdaten für die Ermittlung dieser Straftaten zulässig sein.

Die Echtzeit-Erfassung von Verbindungsdaten ist nur wirksam, wenn die Personen, gegen die ermittelt wird, davon *keine Kenntnis haben*. Das Abfangen ist ein der Geheimhaltung unterliegender Vorgang und in der Weise durchzuführen, daß die Kommunikationspartner diesen Prozeß nicht bemerken. Diensteanbieter und ihre Mitarbeiter, die über das Abfangen unterrichtet sind, müssen daher einer Geheimhaltungspflicht unterliegen, damit das Verfahren erfolgreich durchgeführt werden kann.[207]

Art 21 Abs 1 der Konvention regelt das „*Abfangen von Inhaltsdaten*“ und lautet wie folgt:

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, um ihren zuständigen Behörden in Bezug auf eine Reihe schwerer Straftaten, die nach ihrem innerstaatlichen Recht zu bestimmen sind, die Befugnis zu erteilen,

---

[205] Vgl Explanatory Memorandum Rz 198.

[206] Rz 199.

[207] Vgl Explanatory Memorandum Rz 210.

a) inhaltsbezogene Daten bestimmter Kommunikationen in ihrem Hoheitsgebiet, die mit einem Computersystem übertragen wurden, durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen, und
b) einen Dienstanbieter im Rahmen seiner bestehenden technischen Möglichkeiten zu zwingen,

(i) solche inhaltsbezogenen Daten durch Anwendung technischer Mittel im Hoheitsgebiet dieser Vertragspartei in Echtzeit zu erheben oder aufzuzeichnen oder
(ii) bei der Erhebung oder Aufzeichnung solcher inhaltsbezogener Daten in Echtzeit mit den zuständigen Behörden zusammenzuarbeiten und diese zu unterstützen.

Das „Explanatory Memorandum" führt zu dieser Bestimmung aus, daß die Erfassung von Inhaltsdaten bei Telekommunikationsvorgängen von jeher ein sinnvolles Ermittlungsinstrument darstelle, um festzustellen, ob eine Kommunikation rechtswidrig ist und um Beweise für vergangene oder künftige Straftaten zu erhalten. Da unter Zuhilfenahme der Computertechnologie große Datenmengen mit Texten, visuellen Darstellungen und Tönen übertragen werden können, berge diese ein großes Potential für die Begehung von Straftaten, die auch das Verbreiten rechtswidriger Inhalte betreffen könnten. Ohne das Abfangen des Inhalts einer Nachricht könne die schädliche rechtwidrige Natur mancher Datenübertragungen nicht in Echtzeit bestimmt werden. Und ohne die Fähigkeit, den Beginn und den Verlauf von Straftaten festzustellen, müßten die Strafverfolgungsbehörden sich darauf beschränken, vergangene Straftaten zu ermitteln. Daher sei das Abfangen von Inhaltsdaten in Echtzeit ebenso wichtig wie das Abfangen von Verbindungsdaten – „wenn nicht sogar wichtiger".[208]
Es finden die vorstehenden Erläuterungen zur Erfassung oder Aufzeichnung von Verbindungsdaten, zur Verpflichtung zur Zusammenarbeit und Unterstützung der Behörden, sowie Geheimhaltungspflicht der Diensteanbieter, auch auf das Abfangen von Inhaltsdaten Anwendung. Die Bedingungen und Garantien im Hinblick auf das Echtzeit-Abfangen von Inhaltsdaten können jedoch strenger sein als diejenigen, die für die Echtzeit-Erfassung von Verbindungsdaten oder die Durchsuchung und Beschlagnahme gespeicherter Daten gelten.[209]

[208] Vgl Explanatory Memorandum Rz 213.

[209] Vgl Explanatory Memorandum Rz 215 f.

4.2.3.4. Grundrechtliche Schranken bei Ermittlungshandlungen

Die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt des Übereinkommens vorgesehenen Befugnisse und Verfahren unterliegt den Bedingungen und Garantien des innerstaatlichen Rechts jeder Vertragspartei.

Dies darf jedoch nur unter Bedachtnahme auf gesetzlich geregelte oder gerichtlich angeordnete Vorgaben oder Garantien geschehen; vordringlich ist, daß solche Vorgaben den einzelnen Normen als Bedingungen oder Garantien hinzugefügt werden, die einen Ausgleich zwischen den Erfordernissen der Strafverfolgung und dem Schutz der Privatsphäre und anderer persönlicher Rechte schaffen. Da das Übereinkommen für Vertragsparteien mit vielen unterschiedlichen Rechtssystemen und Kulturen gilt, ist es nicht möglich, die anwendbaren Bedingungen und Garantien für jede Befugnis und jedes Verfahren im Einzelnen vorzuschreiben. Es gibt jedoch einige allgemeine Standards oder Mindestgarantien, welche die Vertragsparteien des Übereinkommens erfüllen müssen.[210]

Eine solche Garantie ist darin zu sehen, daß bei der Schaffung, Umsetzung und Anwendung der Befugnisse und Verfahren die *Verhältnismäßigkeit* des Eingriffs im Hinblick auf die Art und die Umstände der Straftat zu berücksichtigen ist. Die Vertragsparteien sollten jedoch auch weitere Faktoren berücksichtigen, beispielsweise die wirtschaftliche Auswirkung einer Ermittlungshandlung auf Dritte, einschließlich der Diensteanbieter, und prüfen, auf welche Weise diese Auswirkung gemildert werden kann.[211]

Art 15 der Konvention normiert Vorgaben dahingehend, wie diese Beschränkungen innerstaatlich umgesetzt werden könnten und welche Voraussetzungen gegeben sein müssen, damit Ermittlungshandlungen gesetz- und rechtmäßig durchgeführt werden können:

> (1) Jede Vertragspartei stellt sicher, daß für die Schaffung, Umsetzung und Anwendung der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren Bedingungen und Garantien ihres innerstaatlichen Rechts gelten, die einen angemessenen Schutz der Menschenrechte und Freiheiten, einschließlich der Rechte vorsehen, die sich aus ihren Verpflichtungen nach dem Übereinkommen des Europarats zum Schutz der Menschenrechte und Grundfreiheiten (1950), dem Internationalen Pakt der Vereinten Nationen über bürgerliche und politische

[210] Vgl Explanatory Memorandum Rz 131.

[211] Vgl Explanatory Memorandum Rz 132 f.

Rechte (1966) und anderen anwendbaren völkerrechtlichen Übereinkünften über Menschenrechte ergeben und zu denen der Grundsatz der Verhältnismäßigkeit gehören muß.

(2) Diese Bedingungen und Garantien umfassen, soweit dies in Anbetracht der Art der betreffenden Befugnis oder des betreffenden Verfahrens angebracht ist, unter anderem die Kontrolle dieser Befugnis oder dieses Verfahrens durch ein Gericht, oder eine andere unabhängige Stelle, die Begründung der Anwendung und eine Begrenzung im Hinblick auf den Umfang und die Dauer dieser Befugnis oder dieses Verfahrens.

(3) Soweit dies mit dem öffentlichen Interesse, insbesondere mit der ordnungsgemäßen Rechtspflege, vereinbar ist, berücksichtigt eine Vertragspartei die Auswirkungen der in diesem Abschnitt vorgesehenen Befugnisse und Verfahren auf die Rechte, Verantwortlichkeiten und berechtigten Interessen Dritter.

Festzuhalten ist noch, daß das Recht auf *Achtung des Privatlebens* im Zusammenhang mit der *Erfassung von Verbindungsdaten* in der Regel weniger schwer wiegt, als beim *Abfangen von Inhaltsdaten*. Verbindungsdaten über Uhrzeit, Dauer und Umfang der Datenübertragung geben über eine Person oder ihr Denken idR weniger persönliche Informationen preis, als dies bei Inhaltsdaten der Fall ist.

Strengere Maßstäbe in bezug auf den Schutz des Privatlebens dürften wohl im Zusammenhang mit Daten über die *Quelle oder den Empfänger einer Datenübertragung* (zB die aufgerufenen Website) anzusetzen sein. Die Erfassung dieser Daten kann in manchen Fällen die Erstellung eines Interessensprofils einer Person und seines sozialen Umfelds ermöglichen. Demgemäß „sollten die Parteien diese Gesichtspunkte berücksichtigen, wenn sie die geeigneten Garantien und rechtlichen Voraussetzungen für die Durchführung dieser Maßnahmen nach Artikel 14 und 15 festlegen.“[212]

5. Fazit

Die eben erörterten Bestimmungen, bzw die Bestrebungen zur Schaffung ebensolcher, scheinen also – insbesondere was die Erfassung von Vermittlungsdaten betrifft – eine geeignete Grundlage für die Anordnung verschiedener Formen der „Internet-Überwachung“ zu sein.

---

[212] Explanatory Memorandum Rz 212.

Theoretisch könnten also bei Vorliegen der jeweils gesetzlich normierten Anwendungsvoraussetzungen ganze Teams von „Undercover-Agents“ in Newsgroups mit illegalen pornographischen Inhalten, in Chat-Foren, wo offensichtlich massenhaft raubkopierte Software getauscht wird und in den verwobenen Netzwerken großer Verbrechersyndikate auf Ganovenjagd gehen.

Die Realität sieht (wie zumeist) anders aus: Selbst wenn eine Überwachung rechtlich möglich ist, können sich jedoch – was die technische Möglichkeit solcher Überwachungen angeht –erhebliche Schwierigkeiten in der praktischen Durchführung ergeben:

Kommunikationsvorgänge werden heutzutage mit großer Übertragungsgeschwindigkeit durchgeführt, was pro zu überwachenden Anschluß relativ hohe Überwachungskosten[213] verursacht und nur mit erheblichem technischen Aufwand[214] durchführbar ist.[215] Zwar ist mit der Implementierung des „ETSI-Standards“ im Bereich der Überwachungstechnologie ein großer Sprung in Richtung Überwachbarkeit – va im Bereich der mobilen Telephonie – gelungen, zur Zeit mangelt es jedoch noch an der praktischen Umsetzung und der Finanzierung dieser Technologie.

Aufgrund der im Internet innerhalb kürzester Zeit übertragenen Datenmengen kommt noch ein zweites Problem hinzu: Die im Rahmen einer Überwachung gewonnenen Daten müssen für die ermittelnde Behörde noch auswertbar sein, das heißt, daß eine

---

[213] Vgl mit Hinweis auf die Kostentragungsregelung des § 18a FG: *Schmölzer*, Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 214 f.

[214] *Bär* (EDV-Beweissicherung im Strafverfahrensrecht, CR 1998, 436) spricht dabei von Übertragungsgeschwindigkeiten von 33600 bit/s oder mehr. Natürlich stellt aufgrund der rasanten technischen Entwicklung hinsichtlich der Speichermöglichkeit von Daten eine Übertragungsgeschwindigkeit in dieser Größenordnung heutzutage keine Schwierigkeit für die überwachende Stelle mehr dar. Das Problem ist jedoch nach wie vor das selbe, da sich, neben den Anlagen zur Speicherung von Daten, auch die Netzwerke selbst weiterentwickelt haben und heute ein vielfaches der zitierten Übertragungsgeschwindigkeit möglich ist.

Jaburek hingegen (*Jaburek*, Computer-Kriminalität, in: *Fischer* (Hrsg), 3.Symposium „IUS 2000“ (1999) 55) spricht davon, daß dem aus technischer Sicht nicht zuzustimmen sei. Aufgrund der Kommunikationsbeziehungen ließen sich recht genau – wenn auch mit akribischer Kleinarbeit – die Spuren von Straftätern im Internet verfolgen. Dies natürlich unter der Voraussetzung, daß damit auch rechtzeitig angefangen wird, da sonst die relevanten Spuren, wenn sie nicht schon überhaupt verschwunden, so zumindest „unter einer dicken Staubschicht neuerer Informationen verborgen“ seien.

[215] Vgl EBRV 759 BlgNR 20. GP Anm zu § 89 TKG.

erfolgreiche Überwachung in jenen Fällen, in denen sowohl der Nachrichtenabsender, wie auch der Empfänger spezielle Verschlüsselungsmechanismen einsetzen, beinahe auszuschließen ist.[216]

Es wird wohl noch etlicher legistischer Anläufe bedürfen, um den gewaltigen Komplex „Internet-Kriminalität“ einheitlichen Regelungen zu unterwerfen und diese dann auch innerstaatlich umzusetzen. Die Grenze für ein solches Vorhaben stellt aber dabei immer die technische Realisierbarkeit dar.

[216] Vgl *Bär*, EDV-Beweissicherung im Strafverfahrensrecht, CR 1998, 437.

Verzeichnis der verwendeten Literatur

Bär: EDV-Beweissicherung im Strafverfahrensrecht, CR 1998, 434.

Campbell: Existenz von Echelon erstmals offiziell bestätigt, Telepolis, das Magazin für Netzkultur vom 28.05.1999 unter *http://www.heise.de/tp/deutsch/special/ech/6639/1.html.*

Goodwins: Wie funktioniert Echelon, ZDNet News-Report unter *http://www.zdnet.de/news/report/echelon/funktion_00-wc.html*.

Grosche: Entscheidende Spam-Abstimmung im Europäischen Parlament steht bevor, Telepolis, das Magazin für Netzkultur vom 24.05.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/12590/1.html*

Hager, Nicky: Secret Power - New Zealand's Role in the International Spy Network, New Zealand 1996, im Internet unter *http://www.fas.org/irp/eprint/sp/sp_c2.htm*.

Huttner-Thompson: Arbeitsübersetzung der „Draft Convention On Cyber-Crime and Explanatory Memorandum Related Thereto“, *http://www.uni-frankfurt.de/fb01/bizer/rechtsquellen/CyberCrime/CyberCrimeKonvention(21-05-01).pdf.*

Jaburek: Computer-Kriminalität, in: *Fischer* (Hrsg), 3.Symposium „IUS 2000“, Wien 1999, 29.

Kleinz: Europäisches Parlament gegen Webseitensperrungen, Telepolis, das Magazin für Netzkultur vom 12.04.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/12300/1.html.*

Lindau: Das Enfopol-Komplott,, im Internet unter *http://members.eunet.at/hochhaltinger/lindau_1.htm.*

Möchel: Lachnummer ISP Austria, Telepolis, das Magazin für Netzkultur vom 21.2.1999 unter *http://www.telepolis.de/tp/deutsch/inhalt/te/1924/1.html.*

ders: EU-Minister billigen Abhörplan, Telepolis, das Magazin für Netzkultur vom 24.02.1999 unter *http://www.heise.de/tp/deutsch/special/enfo/6374/1.html.*

ders: Die ETSI Dossiers – Europäische Standards für das Abhören digitaler Netze, c’t 7/2001, 58.

ders: Die ETSI-Dossiers, Teil 2– Der Griff der Geheimdienste nach dem Internet, c’t 9/2001, 54.

ders: Die ETSI-Dossiers, Teil 3 – Abhörstandards für digitale Netze vor der Verabschiedung, c’t 17/2001, 78.

ders: Die ETSI Dossiers, Teil 4 - Lauscher am Netz, c't 4/2002, 80.

ders: ENFOPOL: EU-Abhörstandards für die Telekommunikationsnetze, Telepolis, das Magazin für Netzkultur vom 11.02.2002 unter *http://www.heise.de/tp/deutsch/special/enfo/11818/1.html.*

Mühlbauer: Verschwörungstheorien und die Arroganz der Macht, Telepolis, das Magazin für Netzkultur vom 12.09.2001 unter *http://www.heise.de/tp/deutsch/special/libi/9515/1.html.*

Schulzki-Haddouti: EU-Parlament verabschiedet Enfopol-Überwachungspläne, Telepolis, das Magazin für Netzkultur vom 10.05.1999 unter *http://www.heise.de/tp/deutsch/special/enfo/6404/1.html*

dies: Europäisches Rechtshilfeübereinkommen kurz vor der Verabschiedung, Telepolis, das Magazin für Netzkultur vom 26.05.2000 unter *http://www.heise.de/tp/deutsch/special/enfo/6807/1.html*.

dies: Vom Ende der Anonymität - Die Globalisierung der Überwachung[2], Hannover 2001.

dies: Desaster Inpol-neu - Das neue Polizei-Informationssystem: viel zu teuer, viel zu langsam, c't 24/2001, 108.

dies: Europäisches Parlament gegen Speicherung von Verbindungsdaten, Telepolis, das Magazin für Netzkultur vom 19.04.2002 unter *http://www.heise.de/tp/deutsch/inhalt/te/12355/1.html.*

dies: Bundesrat segnet Vorratsspeicherung ab, Telepolis, das Magazin für Netzkultur vom 31.05.2002 *unter http://www.heise.de/tp/deutsch//inhalt/te/12642/1.html.*

Sieber: Legal Aspects of Computer-Related Crime in the Information Society (1998); COMCRIME-Study Executive Summary, im Internet unter *http://europa.eu.int/ISPO/legal/en/comcrime/sieber.html.*

Schmölzer: Rückwirkende Überprüfung von Vermittlungsdaten im Fernmeldeverkehr – Anmerkungen zu OGH 6.12.1995, 13 Os 161/95, JBl 1997, 211.

Sturm: Das Schengener Durchführungsübereinkommen, Kriminalistik 1995, 168.

Sule: Europol und europäischer Datenschutz, Baden-Baden 1999.

Wright: An Appraisal of Technologies of Political Control - Scientific and Technological Options Assessment; STOA Working Document (Consultation version) PE 166 499, Luxembourg 1998, im Internet unter *http://www.a42.de/archiv/echelon.clc.html*.

Zankl: Der Entwurf zum E-Commerce-Gesetz, NZ 2001, 325.

ders: E-Commerce-Gesetz, Kommentar und Handbuch, Wien 2002.

ders: Online-Handbuch für E-Commerce und Internetrecht, im Internet unter *http://www.e-zentrum.at/handbuch/buch-cont.htm*.