TEN/072
"Informationsgesellschaft/
Computerkriminalität"

Brüssel, den 12. September 2001

STELLUNGNAHME
des Wirtschafts- und Sozialausschusses
zu der
Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen "Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität"
(KOM(2000) 890 endg.)

Die Kommission beschloss am 31. Januar 2001, den Wirtschafts- und Sozialausschuss gemäß Artikel 262 des EG-Vertrags um Stellungnahme zu folgender Vorlage zu ersuchen:

> *" Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen - Schaffung einer sicheren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität"*
> (KOM(2000) 890 endg.)

Die mit der Vorbereitung der Arbeiten beauftragte Fachgruppe Verkehr, Energie, Infrastrukturen, Informationsgesellschaft nahm ihre Stellungnahme am 17. Juli 2001 an. Berichterstatter war Herr DANTIN.

Der Ausschuss verabschiedete auf seiner 384. Plenartagung am 12./13. September 2001 (Sitzung vom 12. September) einstimmig folgende Stellungnahme:

*
* *

1. Einleitung

1.1 Die Entwicklung der Informationsgesellschaft zeichnet sich durch weitreichende Veränderungen in allen Bereichen des menschlichen Lebens aus: in Beruf, Bildung, Freizeit, Industrie, Handel usw.

1.2 Im Jahr 1999 startete die Kommission ihre Initiative "eEurope", um sicherzustellen, dass die EU die Vorzüge der neuen Technologien nutzen und dafür sorgen kann, dass die Informationsgesellschaft zu einem Faktor der sozialen Integration wird. Im Juni 2000 billigte der Europäische Rat auf seiner Tagung in Feira den umfassenden "eEurope"-Aktionsplan und forderte seine Durchführung bis Ende 2002[1]. In dem Aktionsplan wird insbesondere betont, wie wichtig die Sicherheit der Netze und die Bekämpfung der Computerkriminalität sind.

1.3 Diese Entscheidung ist die logische Folge einer Reihe bereits getroffener Maßnahmen mit dem Ziel, über das Internet verbreitete illegale und schädliche Inhalte zu bekämpfen, vor allem um geistiges Eigentum und personenbezogene Daten zu schützen und um den elektronischen Handel zu fördern.

1.4 Die Mitteilung ist Teil umfassenderer, fortlaufender Überlegungen. So legte die Kommission 1998 dem Rat die Ergebnisse einer Studie über die Computerkriminalität ("COMCRIM-Studie") vor. Im Oktober 1999 stellte der Europäische Rat in den Schlussfolgerungen auf seiner

---

1 Stellungnahme des WSA zu der Kommissionsvorlage mit dem Titel "eEurope 2002: Eine Informationsgesellschaft für alle - Entwurf eines Aktionsplans" - KOM(2000) 330 endg.; ABl. C 123 vom 25.04.2001.

Tagung von Tampere fest, dass sich die Bemühungen zur Vereinbarung gemeinsamer Definitionen und Sanktionen auch auf den Bereich der High-Tech-Kriminalität konzentrieren sollten.

1.5 In ihrer Mitteilung wirft die Kommission die Frage nach der Notwendigkeit und möglichen Formen einer umfassenden politischen Initiative auf.

2. Die Kommissionsmitteilung

2.1 Nach einer Analyse der Chancen und Gefahren in der Informationsgesellschaft werden in der Kommissionsvorlage die Antworten aufgeführt, die auf nationaler und internationaler Ebene auf die Fragen zum Kampf gegen die Computerkriminalität gegeben wurden. Dabei unterstreicht die Kommission, dass die wichtigsten behandelten Fragen im Wesentlichen unter die Punkte "rechtswidrige Eingriffe in die Privatsphäre", "inhaltsbezogene Delikte", "Wirtschaftsdelikte und unberechtigter Zugang" sowie "Verstöße gegen das Urheberrecht" fallen, die sich wie folgt definieren lassen:

– *Rechtswidrige Eingriffe in die Privatsphäre*: Diese Verstöße richten sich gegen die Grundrechte und den Schutz der Privatsphäre durch die rechtswidrige Sammlung, Speicherung, Änderung, Publikmachung oder Verbreitung personenbezogener Daten.

– *Inhaltsbezogene Delikte:* Diese betreffen die vor allem über das Internet erfolgende Verbreitung pornografischer Inhalte und insbesondere von Kinderpornografie sowie von rassistischen Äußerungen, *von revisionistischen Erklärungen über den Nazismus* und von Aufrufen zur Gewalt.

– *Wirtschaftsdelikte, unberechtigter Zugang und Sabotage*: Diese stehen im Zusammenhang mit dem unberechtigten Zugang zu Computersystemen (u.a. Hacking, Computersabotage, Verbreitung von Computerviren, Ausspähen oder Fälschung von Daten, Computerbetrug) sowie neuen Deliktformen (z.B. Manipulation per Computer).

– *Verstöße gegen das Urheberrecht*: Diese Verstöße betreffen den rechtlichen Schutz von Computerprogrammen bzw. Datenbanken, das Urheberrecht und die verwandten Schutzrechte.

2.2 Um die Mittel und Wege zu einem Vorschlag für einen Rechtsakt zu erkunden, mit dem die nationalen Rechtsvorschriften über die Computerkriminalität angeglichen werden sollen, werden in der Mitteilung die "Fragen des materiellen Strafrechts" und die "strafverfahrensrechtlichen Fragen" geprüft (u.a. Überwachung des Fernmeldeverkehrs, Aufbewahrung von Verkehrsdaten, anonymer Zugang und anonyme Nutzung, praktische Zusammenarbeit auf internationaler Ebene).

2.3 In einem zweiten Schritt behandelt die Mitteilung alle nichtlegislativen Maßnahmen, die notwendigerweise die legislativen Maßnahmen ergänzen sollten. Im Wesentlichen sind dies: die Einrichtung von "spezialisierten Dienststellen auf nationaler Ebene", die "fachliche Schulung", die "Zusammenarbeit zwischen den verschiedenen Akteuren", "direkte Maßnahmen der Industrie" sowie die von der Europäischen Union geförderten "FTE-Projekte".

2.4 Zur "Sicherheit der Informationsinfrastrukturen" wird ausgeführt, dafür seien in erster Linie die Nutzer selbst zuständig.

2.5 Unter dem Punkt Schlussfolgerungen und Vorschläge wird in der Mitteilung wie in der Darstellung der Probleme zwischen zwei Teilbereichen unterschieden, die präzisiert und ausführlich dargestellt werden:

– die nichtlegislativen Vorschläge und
– die Legislativvorschläge.

2.5.1 **Legislativvorschläge**

Es werden Maßnahmen auf folgenden Gebieten vorgeschlagen:

– Einrichtung eines EU-Forums, in dem Strafverfolgungsbehörden, Diensteanbieter, Netzbetreiber und Verbrauchergruppen gemeinsam darauf hinarbeiten, die Zusammenarbeit auf EU-Ebene zu verbessern;

– Fortsetzung der Arbeiten zur Stärkung der Sicherheit und des Vertrauens im Rahmen ihrer Initiative "eEurope", des Aktionsplans für das Internet, des IST-Programms und des Rahmenprogramms im Bereich FTE.[2]

– Einleitung weiterer Projekte im Rahmen der bestehenden Programme;

– Bereitstellung von Finanzmitteln für Maßnahmen zur Verbesserung von Inhalt und Benutzerfreundlichkeit der durch die COMCRIME-Studie eingerichteten Datenbank über die nationalen Rechtsvorschriften.

2.5.2 **Vorschläge für legislative Maßnahmen**

In Anwendung von Titel VI des Vertrags über die Europäische Union wird die Kommission Vorschläge mit folgenden Zielen unterbreiten:

– Angleichung der Rechtsvorschriften der Mitgliedstaaten in Bezug auf Kinderpornografiedelikte[3].

---

2 Stellungnahme des WSA zu dem "*Vorschlag für einen Beschluss des Europäischen Parlaments und des Rates über das mehrjährige Rahmenprogramm 2002-2006 der Europäischen Gemeinschaft im Bereich der Forschung, technologischen Entwicklung und Demonstration als Beitrag zur Verwirklichung des Europäischen Forschungsraums"* und dem *" Vorschlag für einen Beschluss des Rates über das mehrjährige Rahmenprogramm 2002-2006 der Europäischen Atomgemeinschaft (EURATOM) im Bereich der Forschung und Ausbildung als Beitrag zur Verwirklichung des Europäischen Forschungsraums"* - KOM(2001) 94 endg. - 2001/0053 (COD) - 2001/0054 (CNS) - wird derzeit erarbeitet.

3 Vorschlag für einen Rahmenbeschluss des Rates zur Bekämpfung der sexuellen Ausbeutung von Kindern und der Kinderpornografie - KOM(2001) 854 endg. - CNS 2001/025; ABl. C 062 E vom 27.02.2001.

– stärkere Angleichung der Strafrechtsvorschriften für den Bereich High-Tech-Kriminalität.

– Anwendung des Grundsatzes der gegenseitigen Anerkennung von Anordnungen, die im Rahmen von Ermittlungsverfahren im Zusammenhang mit Computerkriminalität ergangen sind, an denen mehr als ein Mitgliedstaat beteiligt ist.

Im Lichte insbesondere der Ergebnisse, die das vorgeschlagene EU-Forum in diesem Bereich erzielt, wird die Kommission prüfen, ob Maßnahmen (insbesondere legislativer Art) zum Thema Aufbewahrung von Verkehrsdaten zu ergreifen sind.

3. **Allgemeine Bemerkungen**

3.1 Der Wirtschafts- und Sozialausschuss teilt den Standpunkt der Kommission zur Bedeutung der Verbreitung und Nutzung der neuen digitalen Techniken, insbesondere des Internets, denn die Infrastruktur der Informationsverarbeitung und die Kommunikation ist bereits jetzt ein entscheidendes Glied unserer Volkswirtschaften geworden. In bestimmten Branchen ist dieses Glied bereits so wichtig geworden, dass eine Abhängigkeit eines Teils der Wirtschaftstätigkeit von der Computerwelt festgestellt werden kann.

3.2 Er schließt sich auch der Analyse der Kommission zu den Gefahren der allgemeinen Verbreitung dieser Technologien und den notwendigen Vorsichtsmaßregeln an, denn wenn *"… unsere Gesellschaften immer häufiger auf diese Technologien zurückgreifen, müssen wirksame praktische und rechtliche Mittel eingesetzt werden, um den bestehenden Risiken entgegenzuwirken."*

3.3 Der Ausschuss begrüßt daher, dass die Mitteilung eine recht umfassende Liste der Sicherheitsprobleme in der Informationsgesellschaft erstellt hat, und dass sie Vorschläge für die Festlegung einer umfassenden Sicherheitspolitik unterbreitet. Der Ausschuss ist jedoch der Ansicht, dass die Computerkriminalität besser definiert werden sollte, um genau zwischen zwei Klassen von Verbrechen und strafbaren Handlungen zu unterscheiden: zum einen die "neuen Informatiktatbestände" (Verbreitung von Computerviren, Zerstörung von Programmen oder Dateien usw.), die Gegenstand neuer Rechtsvorschriften sein müssen, und zum anderen die traditionellen kriminellen Handlungen, die heutzutage durch die Nutzung der Rechner und Netze leichter begangen werden können (Pädophilie, Geldwäsche, Verletzungen des Urheberrechts), für die eine stärkere Harmonisierung der in den einzelnen Mitgliedstaaten bereits geltenden Vorschriften erfolgen sollte. Für den Kampf gegen die ganz unterschiedlichen strafbaren Handlungen, die von Tätergruppen begangen werden, die die Technologie gut beherrschen (Vergehen von Experten mit hoher Qualifikation), sind auch differenzierte Gegenmaßnahmen erforderlich.

3.4 In der Kommissionsmitteilung werden zahlreiche repressive Maßnahmen vorgeschlagen. Der Ausschuss ist der Auffassung, dass der Computerkriminalität nicht nur durch eine repressive Politik, sondern auch durch breiter angelegte Maßnahmen der Verhütung und Schulung sowie der Bekämpfung der Ausgrenzung gleich welcher Art (wirtschaftlich, aber auch kulturell) begegnet werden sollte. Der Ausschuss besteht darauf, dass die Rolle der einzelnen Akteure, insbesondere der öffentlichen Akteure auf allen Ebenen bei der Umsetzung dieser umfassenderen Politik zur Verhütung und Bekämpfung der Computerkriminalität definiert werden muss: Rolle der EU, der

Staaten, der Regionen, der Städte, der Unternehmen sowie aller Teile der "Zivilgesellschaft" (Schulen, Vereinigungen, Bibliotheken usw.).

3.5 Dem Ausschuss fällt jedoch auf, dass bestimmte wichtige Aspekte in den vorgelegten Analysen unterschätzt wurden. So geht aus dem Titel der Mitteilung hervor, dass zwei Hauptthemen erörtert werden: die Sicherheit der Informationsinfrastruktur und die Computerkriminalität. Der Ausschuss möchte unterstreichen, dass es in dieser Mitteilung vor allem um die Kriminalität geht, denn die Sicherheit der Infrastruktur wird in viel geringerem Maße analysiert. Aber diese Sicherheit, insbesondere die durch den technischen Betrieb der Netze gegebene Sicherheit, ist bei weitem nicht zufriedenstellend. Der beträchtliche Anstieg der Nutzerzahlen, der Umfang der zu übermittelnden Daten und die ständige Einführung noch wenig stabilisierter Techniken (hohe Übertragungsraten, Internet über Mobiltelefone usw.) können die Sicherheit gefährden. Über die Probleme der Überlastung oder Ausfälle der Telekommunikationsnetze wird sehr wenig gesprochen[4]. Man sollte sich darüber klar werden, dass mit einer steigenden Abhängigkeit der Wirtschaftstätigkeiten von der Computerwelt die technische Zuverlässigkeit der Netze unverzichtbar wird.

3.6 Zur technischen Sicherheit der Netze wäre es interessant zu wissen, welche Haftung die Betreiber der Telekommunikationsnetze übernehmen und welche Auswirkungen die Deregulierung auf die technische Qualität hat. Aus zahlreichen Wirtschaftsstudien sind die positiven Wirkungen der Deregulierung der Telekommunikation ersichtlich (Preissenkung, Diversifizierung der Verträge, neue Dienste usw.), aber in keiner der Studien werden die Folgen dieser Deregulierung für die Qualität und die Sicherheit der Infrastruktur untersucht. In der Kommissionsmitteilung wird keinerlei finanzielle Schätzung der Verluste bei den Nutzern, insbesondere der Unternehmen, aufgrund technischer Ausfälle beim Betrieb der Netze vorgenommen. Gleichwohl wäre es wichtig, die rein wirtschaftlichen Auswirkungen - neben den Folgen auf sozialer und menschlicher Ebene -einschätzen zu können, die sich aus den "technischen Funktionsstörungen der Computerwelt" im Vergleich zur "Computerkriminalität" ergeben.

3.7 Die Behandlung der Sicherheitsprobleme ist in der Kommissionsmitteilung sehr auf den Einzelfahl bezogen und stark von einer "Laisser-faire"-Haltung geprägt, wobei die Neigung besteht, die Behandlung aller Sicherheitsprobleme und des Kampfes gegen die Computerkriminalität den Nutzern zu überlassen. Die Mitteilung verweist mit Nachdruck auf die Verantwortung der Nutzer, der Einzelpersonen und Unternehmen, und scheint die Rolle der großen Akteure, nämlich der Betreiber der Telekommunikationsnetze und der Staaten, zu unterschätzen: "*Für die Sicherheit sind somit in erster Linie die Nutzer selbst zuständig, denn nur sie können ermessen, welcher Natur die Daten sind, die sie erhalten oder verschicken und welche Schutzvorkehrungen erforderlich sind."* Zweifellos hat jeder Nutzer eine Rolle zu spielen, um seine eigene Sicherheit zu gewährleisten, und der Ausschuss stimmt zu, dass die Nutzer über die im Internet bestehenden Risiken umfassend unterrichtet und geschult werden müssen, um sich zu schützen und ihre eigene Verantwortung wahrnehmen zu können. Aber für ein solches individuelles Herangehen gibt es Grenzen: Diese Verantwortung kann zwar teilweise von "starken oder versierten" Nutzern (Großunternehmen oder

4 Solche Ausfälle sind bei den Mobiltelefonnetzen spektakulär (denn alle Nutzer bemerken sie rasch), aber es gibt sie auch, wenngleich weniger sichtbar, im Internet. Von den Betreibern werden dazu leider wenig Statistiken verbreitet.

Institutionen) wahrgenommen werden, aber kann sie es wirklich auch von "schwächeren oder unerfahrenen" Nutzern (kleinen Unternehmen, Einzelpersonen und insbesondere Kindern)? Ein solches Sicherheitsverständnis reicht nicht für die "reale und konkrete Welt", geschweige denn für die virtuelle Welt. Ist das nicht eine Einladung zur Einrichtung illegaler Mittel der Selbstverteidigung, wie privater Milizen, die mit der Sicherheit und der Bekämpfung der Computerkriminalität beauftragt wären?

3.8 Ergänzend zu den vorstehenden Bemerkungen möchte der Ausschuss betonen, dass er nicht die wichtige, aktive Rolle negiert, die der Bürger heutzutage als Nutzer spielen könnte. Der Nutzer sollte gut unterrichtet und über alle Probleme im Zusammenhang mit der Sicherheit im Cyberspace informiert sein. Dies könnte durch eine Erstausbildung und eine ständige Information über die Entwicklungen auf diesem Gebiet realisiert werden. Die Initiativen eEUROPE[5] und eLearning[6] sowie der Prozess der lebenslangen allgemeinen und beruflichen Bildung können zur Verwirklichung dieses Ziels auf positive und kreative Weise beitragen.

3.9 Von Interesse wäre auch eine eingehendere Beschäftigung mit der Frage nach der Verantwortung der Akteure in der Informatikbranche: die Sicherheit macht wahrscheinlich 10 bis 15% der von den Unternehmen und Einzelpersonen aufgewendeten Kosten aus (Kauf besonderer Vorrichtungen vom Typ "Firewall", Kauf von Antivirenprogrammen, Aktualisierung dieser Software usw.)[7]. Deshalb kann die Aufforderung, Sicherheitsinstrumente zu benutzen, bei Privatpersonen und KMU fragwürdig erscheinen. Hier geht es vielmehr um eine Aufgabe der Händler und Hersteller, die von der derzeit verfügbaren Soft-und Hardware Gebrauch machen müssen, um ihre Kunden zu schützen. "Daher ist es wichtig, Innovationen und die kommerzielle Nutzung von Sicherheitstechnologien und -dienstleistungen anzuregen. "Kann man sicher gehen, dass alle Hersteller von Soft- und Hardware wirklich wünschen, die Zahl der Viren, die heute bei über 50.000 liegt und jährlich um 10.000 steigt, solle sinken?

3.10 Zum anderen erscheint es dem Ausschuss erforderlich, dass eingehender untersucht wird, welchen Einfluss die europäischen Staaten und die EU auf das Management und die Überwachung der großen Organisationen haben, die die Teilnetze des Internet verwalten[8]. So ist beispielsweise anzumerken, dass Europa in der INCANN (Zentralstelle für die Vergabe von Internet-Namen und -Adressen), die die Internet-Verwaltung gewährleistet, überhaupt nicht vertreten ist. Die ICANN ist eine privatrechtliche Einrichtung, die 1998 auf Initiative der amerikanischen Regierung gegründet wurde, um die Koordinierung im Internet zu übernehmen. Es ist eben diese privatrechtliche Institution, die neben anderen Aufgaben die Internet-Adressen (um Duplizierungen zu vermeiden) und die Namen der Internet-Bereiche für die Netzplätze (Websites) in der ganzen Welt verwaltet und die für alle geltenden Regeln des Betriebs festlegt. Das Leitungsgremium der ICANN ist jedoch aus den

---

5 Siehe Fußnote 1.

6 Initiativstellungnahme des WSA über das Thema "Die europäische Dimension der allgemeinen Bildung: Wesen, Inhalt und Perspektiven", ABI. C 139 vom 11.05.2001.

7 In Bezug auf die Anfälligkeit bestimmter Systeme sind große Unterschiede zu beobachten.

8 Siehe KOM(2000) 202 endg.

Vertretern der privaten amerikanischen Betreiber und einigen wenigen Internetnutzern (Internauten) zusammengesetzt, die "in allgemeiner Wahl im Internet gewählt" wurden, und unter denen ein europäischer Internetnutzer ist. Die Mitteilung ist in Bezug auf solche Überlegungen sehr wortkarg, und der Ausschuss hält es für erforderlich, dass eine aktive Mitwirkung der EU in den verschiedenen Einrichtungen, die das Internet verwalten und koordinieren, und nicht nur in den rein technischen Einrichtungen der Telekommunikationsbranche, gefordert wird[9]. Wäre es außerdem wegen der Folgen der Nutzung des Internets auf sozialer und gesellschaftlicher Ebene nicht nötig, dass die Verwaltung des Netzes (Festlegung von Normen, Koordinierung der elektronischen Adressen usw.) von einer internationalen Organisation übernommen wird, in der die Behörden der einzelnen Staaten in breitem Maße vertreten wären? Zu bemerken ist, dass diese Art von Organisation auf anderen Gebieten bereits existiert (beim Luftverkehr - IATA, beim Seeverkehr oder auch in der Telekommunikation).

3.11 Die Kommissionsmitteilung erörtert die Frage der Angleichung der Befugnisse der Strafverfolgungsbehörden, die *"den Schutz … verbessern (wird)"*, aber sie macht dies nicht zu einer Priorität in ihren Schlussfolgerungen. Der Ausschuss ist der Ansicht, dass diese Angleichung dringend erforderlich ist und verwirklicht werden muss, damit die Harmonisierung der Verfahren schneller vorankommt. Insbesondere muss diese Angleichung bei Wahrung der in den einzelnen Mitgliedstaaten staatlich anerkannten Rechte und Freiheiten und der Grundrechte auf den Schutz der Privatsphäre und den Schutz der in der Charta der Grundrechte der Europäischen Union aufgeführten Daten es möglich machen, die in Computern gespeicherte Daten rasch ausfindig zu machen und zu beschlagnahmen, um der Vernichtung strafrechtlichen Beweismaterials zuvorzukommen. Zudem müssen die Strafverfolgungsbehörden über Zwangsmittel verfügen können, die es ihnen erlauben, die prompte Aufbewahrung bestimmter Daten anzuordnen oder zu bewirken.

4. Besondere Bemerkungen

4.1 Notwendigkeit der Bekämpfung der Pädophilie

4.1.1 Der Wirtschafts- und Sozialausschuss begrüßt die Entscheidung der Kommission, noch in diesem Jahr einen "Vorschlag für einen Rahmenbeschluss des Rates vorzulegen, der unter anderem Bestimmungen über die Angleichung der Vorschriften und der Sanktionen für den Bereich der Kinderpornografie im Internet enthält."[10] Der Ausschuss ist der Auffassung, dass diese Angleichung der Rechtsvorschriften und Sanktionen nicht nur für die Pädophilie, sondern auch auf anderen Gebieten vorzunehmen ist: Bekämpfung von Sekten, rassistischem Gedankengut, Sexismus und allgemein der Förderung von Pornographie und Gewalttätigkeit.

---

9 Das Leitungsgremium der ICANN hat 19 Mitglieder, von denen 5 die 5 großen Weltregionen (Nordameirka, Europa, Asienpazifischer Raum, Afrika, Südamerika) vertreten. Die Wahlen erfolgten nach sehr wenig demokratischen Modalitäten: jeder Internetnutzer konnte freiwillig abstimmen, aber nur sehr wenig Internetnutzer waren von dieser "Wahl" informiert!

10 Beschluss des Rates vom 29.05.2000 zur Bekämpfung der Kinderpornographie im Internet, ABl. L 138 vom 09.06.2000.

Stellungnahme des WSA zu einem "Programm für den Kinderschutz im Internet", die derzeit erarbeitet wird.

Stellungnahme des WSA zum Thema "Kindesmissbrauch und Sextourismus"; ABl. C 284 vom 14.09.1998.

Stellungnahme des WSA zu dem "Vorschlag für eine Empfehlung des Rates zur Gewährleistung des Jugendschutzes und des Schutzes der Menschenwürde in den audiovisuellen und den Informationsdiensten" KOM(97) 570 endg.; ABl. C 214 vom 10.07.1998.

4.2 **Notwendigkeit, die Überwachung des Fernmeldeverkehrs zu reglementieren**

4.2.1 Der Ausschuss schließt sich den in der Mitteilung geäußerten Befürchtungen an: "Der wahllose Gebrauch bzw. Missbrauch von Überwachungsmöglichkeiten, insbesondere auf internationaler Ebene, wirft Menschenrechtsfragen auf und untergräbt das Vertrauen der Bürger in die Informationsgesellschaft." Der Ausschuss möchte diese Analyse jedoch ergänzen, indem er mit Nachdruck fordert, dass diese Grundsätze der Vertraulichkeit überall eingehalten werden müssen, auch im internen Geschäftsablauf der Unternehmen. In allen Unternehmen müssen die Menschenrechte gewahrt und die Privatsphäre geschützt werden. Dies betrifft u.a. den Schutz persönlicher Nachrichten, die von den Arbeitnehmern über die Kommunikationssysteme des Unternehmens verschickt bzw. empfangen werden (Schutz der Privatsphäre)[11]. Diese Achtung der Rechte erfordert auch Verhandlungen über die Nutzung der personenbezogenen Daten, die notwendigerweise im Sinne eines ordnungsgemäßen Funktionierens der Netze erhoben werden, aber eine individuelle Kontrolle der Tätigkeit und des Verhaltens jedes einzelnen Arbeitnehmers ermöglichen. Die notwendige Aushandlung einer "Charta der Nutzung der Informationstechnologien" ist ein Instrument, um einen Ausgleich zwischen der Wahrung der individuellen Freiheiten und den aus dem Geschäftsablauf der Unternehmen erwachsenden Zwängen zu finden (u.a. doppelte Mailbox für die elektronische Post).

In der Mitteilung der Kommission wird lediglich in einer Fußnote das weltweit wirkende Überwachungsnetz mit der Bezeichnung ECHELON erwähnt. Der Ausschuss begrüßt die Bemühungen des Untersuchungsausschusses des Europäischen Parlaments, die ganze Wahrheit über dieses Netz ans Licht zu bringen, dessen Instrumente (Ausrüstungen, Abhörzentrale usw.) teilweise in einem Mitgliedstaat installiert sind. Es wäre paradox, detaillierte Verfahren zur Regelung der Überwachung des Fernmeldeverkehrs zu erarbeiten, wenn gegen diese Regeln von einer Gruppe von Staaten permanent verstoßen wird, wobei mit einem Alibi der militärischen Sicherheit weniger leicht zu offenbarende Ziele der Wirtschaftsspionage verdeckt werden. Deshalb fordert der Ausschuss den Ministerrat auf, in dieser Frage mit Nachdruck zu intervenieren.

4.3 **Notwendigkeit, bestimmte Verkehrsdaten aufzubewahren**

4.3.1 Die Straftaten im Internet weisen allgemein bekannte Merkmale auf: sie können relativ leicht begangen werden (sofern die Informationstechniken beherrscht werden), sie erfordern wenig Mittel und können ohne jede physische Präsenz begangen werden, sie können plötzlich eine Vielzahl von Internetnutzern treffen und erhebliche Schäden verursachen. Sie hinterlassen hingegen Spuren in den verschiedenen Teilen der Netze, die von den illegalen Daten benutzt wurden.

4.3.2 Technisch ist alles so angelegt, dass die einzelnen Akteure daran interessiert sind, die Spuren zu beseitigen, sobald die Abrechnung abgeschlossen ist, wodurch die Arbeit der Polizeikräfte fast unmöglich gemacht wird. Der Ausschuss ist der Ansicht, dass dieses Problem eines der dringendsten ist und gelöst werden muss, um einen reibungslosen Betrieb des Internets zu gewährleisten;

11 So garantiert beispielsweise eine kürzlich von dem Unternehmen Deutsche Telekom unterzeichnete Vereinbarung die vollständige Vertraulichkeit der von den Arbeitnehmern über das Intranet des Unternehmens und über das Internet verschickten Nachrichten.

er unterstützt die Position der Kommission, die *"alle Beteiligten (auffordert), die komplexe Frage der Aufbewahrung von Verkehrsdaten vorrangig und ausgiebig zu erörtern"*. Diese Prüfung sollte es ermöglichen, die technischen Fragen (welche Informationen sollen aufbewahrt werden? für wie lange?) und die wirtschaftlichen Fragen (wer finanziert die neuen Geschäftsvorgänge?) zu erörtern[12]. Der Entwurf des Europarats für ein Übereinkommen über Cyberkriminalität[13] enthält eine Reihe vom Modalitäten zur Aufbewahrung der Daten. Die Annahme und Umsetzung dieses Übereinkommens könnte sich jedoch sehr lange hinziehen, so dass es erforderlich ist, die Einrichtung spezifischer Instrumente der Mitgliedstaaten der EU zu beschleunigen[14].

4.4 **Notwendigkeit, den anonymen Zugang und die anonyme Nutzung zu reglementieren**

4.4.1 Die Mitteilung erinnert daran, dass die Frage der Anonymität im Internet im Mittelpunkt eines Dilemmas steht: Einerseits ist die Möglichkeit, anonym zu bleiben, wesentlich, wenn die Grundrechte auf Achtung der Privatsphäre gewahrt werden sollen: andererseits erstickt die Fähigkeit zur Online-Kommunikation ohne Offenbarung der eigenen Identität schon im Keim die Möglichkeit, bestimmte Straftaten zu bekämpfen. Der Ausschuss pflichtet der Auffassung der Kommission bei, dass auf das Internet die auch sonst geltenden Rechtsgrundsätze anzuwenden sind: *"Das Internet ist kein gesetzloser Freiraum, in dem die Regeln der Gesellschaft nicht gelten."* Der Ausschuss ist der Auffassung, dass technische und rechtliche Lösungen gefunden werden sollten, damit Zugang zum und Navigation im Internet, nicht zum Ausspähen des privaten Verhaltens von Internauten führen. Das Verschicken anonymer, unerwünschter Nachrichten an eine bestimmte individuelle Adresse[15], insbesondere von kollektiv genutzten Orten aus (wie Cybercafés, Bibliotheken usw.), muss ebenfalls untersagt werden. Die Zunahme anonymer Sendungen bedroht nämlich nicht nur alle Einzelpersonen, sondern auch die Gesellschaft insgesamt. Der Ausschuss ist sich der Schwierigkeiten bewusst, die ein solches - wenngleich eingeschränktes -Verbot der Anonymität aufwirft. Dagegen ist jedoch die Behauptung zu nuancieren, wonach "… die Möglichkeit, anonym zu bleiben, wesentlich (ist), wenn die Grundrechte auf Achtung der Privatsphäre und freie Meinungsäußerung im Cyberraum bewahrt werden sollen." Die Anerkennung einer solchen Rechtsauffassung könnte mit dem Recht der (nominativen oder generischen) Empfänger der Nachrichten kollidieren, die - um ihre Privatsphäre und ihre Interessen zu schützen - ihrerseits die Möglichkeit haben müssen, die genaue Identität ihrer Kommunikationspartner zu erfahren.

---

12 Das Problem stand in mehreren Staaten bereits auf der Tagesordnung (u.a. Belgien, Niederlande, Vereinigtes Königreich) wobei unterschiedliche Antworten gefunden wurden.

13 Europarat - Entwurf eines Übereinkommens über Cyberkriminalität –Emtwurf Nr. 25 vom 9. Januar 2001.

14 Initiativstellungnahme des WSA über die "Auswirkungen des elektronischen Handels auf den Binnenmarkt (BBS)"; ABl. C 123 vom 25.04.2001.

15 An öffentliche oder private Foren geschickte Nachrichten können anonym bleiben, weil alle Teilnehmer diese Anonymität akzeptieren.

4.5 **Rolle der spezialisierten Dienststellen auf nationaler Ebene**

4.5.1 Der Ausschuss begrüßt die Forderung, auf nationaler Ebene spezialisierte Dienststellen einzurichten, denen verschiedene Aufgaben, u.a. die Verfolgung der Computerkriminalität und die Festlegung von Ermittlungstechniken übertragen werden. Der Ausschuss schließt sich auch der Ansicht der Kommission zur Notwendigkeit an, Statistiken über die Computerkriminalität anzulegen*: "Daher ist es erforderlich, stichhaltige Belege für das Ausmaß der Computerkriminalität zusammenzutragen."* Daher fordert der Ausschuss, die Zuständigkeiten dieser spezialisierten Dienststellen, die für die Erstellung detaillierter und aussagekräftiger und öffentlich gemachter Statistiken über die Computerkriminalität auszudehnen, damit diese Aufgabe nicht privaten Untersuchungseinrichtungen übertragen wird, die stets enge Bande zur Informatikbranche unterhalten. Für die Bekämpfung der Unsicherheit und der Computerkriminalität bedarf es einer Schätzung des Ausmaßes der Kriminalität, der Kenntnis ihrer Quellen und Ursachen und insbesondere einer Schätzung der von Einzelpersonen und Unternehmen aufgrund von Sicherheitssystemen oder aufgrund der Folgen von Verstößen und Virusangriffen zu tragenden Kosten.

4.6 **Einrichtung eines EU-Forums**

4.6.1 Der Ausschuss billigt den Vorschlag der Kommission, ein EU-Forum einzurichten, das eine Vielzahl von Akteuren mit dem Ziel vereint, die Zusammenarbeit auf EU-Ebene umfassend zu verbessern, und er ersucht nachdrücklich darum, dass dieses Forum in erster Linie ein Gremium sein solle, das einen Meinungsaustausch über die wahren oder falschen Annahmen bezüglich der Informationsgesellschaft ermöglicht. Dieses Forum muss vor allem dazu dienen, dass die Notwendigkeit der Einrichtung von Regulierungssystemen begründet, umfassend dargestellt und bei den Institutionen und Bürgern bekannt gemacht wird. Immerhin muss zugestanden werden, dass sich das Internet zum Teil außerhalb der hergebrachten Regulierungsmechanismen entwickelt hat: dies war einer der Gründe für seine sehr schnelle Entwicklung. Das Internet ist aber so groß geworden, dass es nicht mehr ohne jede Regulierung bestehen kann. Die Internet-Fans bestehen weiter auf der Behauptung *"jede Reglementierung des Internets würde die Entwicklung des Internets bremsen"*. Außerdem stützen sie sich auf das Ideal der Verbände und die Freiheitsliebe einer gewissen Zahl der Internetnutzer, um weiter der Idee Vorschub zu leisten, das "digitale Weltdorf" dürfe nicht von den Staaten reguliert werden und solle sich mit Verhaltenskodizi begnügen.

Es ist an der Zeit, dass Europa zur Entwicklung von Gedanken über die Notwendigkeit der Regulierung und Reglementierung etwas beisteuert. Es sollte daran erinnert werden, dass das Internet ein Instrument wie jedes andere und wie jede andere Wirtschaftstätigkeit zu regulieren ist. Die Entwicklung des elektronischen Geschäftsverkehrs in der Privatwirtschaft und der Online-Kommunikation mit der Verwaltung wird nur Realität werden, wenn die Verbraucher und Bürger Vertrauen in das Internet haben. Dieses Vertrauen ist aber an die rasche Festlegung politischer, wirtschaftlicher und steuerlicher Regeln gebunden und entsteht nicht nur durch den Kauf von Sicherheitssystemen durch die Unternehmen und Privatpersonen. Neben einem solchen Beitrag zu diesen Überlegungen, der eine der wichtigsten Aufgaben des EU-Forums sein könnte, müssen sich die Menschen dessen bewusst werden, dass sich alle Internetnutzer von extremen Standpunkten (zu viel Naivität oder zu viel Paranoia) fernhalten sollten.

4.6.2 Der Ausschuss wird angesichts des Nutzens eines solchen Austauschs für die organisierte Zivilgesellschaft an diesem Forum mitwirken.

4.7 **Direkte Maßnahmen der Industrie**

4.7.1 Der Ausschuss pflichtet der Analyse in dem Vorschlag bei: *"Zahlreiche Industriezweige (z.B. in den Bereichen Banken, elektronische Kommunikation, Kreditkarten und Urheberrechte) mitsamt ihrer Kunden sind durch Computerstraftaten gefährdet."* Er ist jedoch der Auffassung, dass in der Mitteilung nicht mit genügend Nachdruck die enormen Risiken aufgeführt werden, die den KMU durch die Sicherheitslücken im Internet entstehen. Es muss ein Anreiz für die Anbieter von kommerziellen Web-sites für Unternehmen geschaffen werden, die im Bereich der Sicherung zur Verfügung stehenden Mittel zu nutzen. Die großen Unternehmen haben zwar die personellen und finanziellen Mittel, eine gewisse Sicherheit zu gewährleisten, viele mittelständische Unternehmen können dafür aber nicht die erforderlichen Mittel aufbringen. Diese Unternehmen müssen daher erhebliche finanzielle Schäden hinnehmen (Zerstörung und Verlust von Dateien, Diebstahl vertraulicher Dateien usw.) oder gar vorübergehende oder endgültige Einstellungen ihrer Geschäftstätigkeit (Viren in den Informationssystemen usw.). Zudem können bestimmte betrügerische Praktiken bei der Benutzung des Internets ganz erhebliche "verdeckte" Kosten verursachen: So kann die Praxis des massenhaften Verschickens von Werbung über die elektronische Post ("spam") beim Empfänger der Sendungen Kosten und vor allen nicht zu vernachlässigende Zeitverluste verursachen[16]. Derzeit wird zu wenig gegen solche Praktiken vorgegangen. Der Ausschuss erinnert daran, dass er ein "Opt-in-System" für gewerbliche elektronische Post befürwortet[17].

4.8 **Von der EU geförderte FTE-Projekte**

4.8.1 Der Ausschuss billigt die Grundzüge des FTE-Rahmenprogramms, auf das in der Mitteilung verwiesen wird. Er besteht jedoch darauf, dass die Überlegungen und Forschungen zu zwei Themen fortgeführt werden müssen, die ihm wesentlich erscheinen.

4.8.1.1 **Thema Nr. 1 (Studien technischer Art):** Bis zu welcher Stufe der Komplexität kann das Internet entwickelt werden, ohne dass es zu einer nicht mehr hinnehmbaren Anfälligkeit kommt? Allgemein wird anerkannt, dass die Anfälligkeit eines Systems an seine Komplexität geknüpft ist. Wann wird wegen der steigenden Abhängigkeit der Wirtschaftstätigkeiten von der Computerwelt ein aus miteinander verbundenen Netzen bestehendes Ganzes gefährlich, weil es zu anfällig für technische Ausfälle und zu leicht verletzlich für Computerkriminalität ist? Alle menschlichen Erfindungen weisen erhebliche Einschränkungen auf (Flugzeuge, Schiffe, Tunnel, Türme usw.) und

16 Einer kürzlich (Februar 2001) vorgelegten Studie der EU zu Folge, macht das massenhaften Verschickens von Werbung über die elektronische Post 500 Mio. Nachrichten in der ganzen Welt täglich aus. Dieser zusätzliche Verkehr, der vom Empfänger der Nachricht bezahlt werde, koste die Gemeinschaft der Internetnutzer über 10 Mrd. Euro.

17 Stellungnahme des WSA zu dem "Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation" - KOM (2000) 385 endg. - 2000/0189 (COD); ABl. C 123 vom 25.04.2001.

Gigantismus führt immer auch zur Anfälligkeit. Sollten diese Gegebenheiten für das Internet und die Netze nicht gelten?

4.8.1.2 **Thema Nr. 2 (Studien psychologischer, soziologischer und kultureller Art):** Welche Besonderheiten hat die Computerkriminalität in der immateriellen Welt gegenüber der üblichen Kriminalität in der "realen und konkreten" Welt? Wahrscheinlich spielt das Fehlen "sichtbarer" Konsequenzen eine große Rolle. Wie können die Wirkungen der Computerkriminalität "sichtbar" und leicht wahrnehmbar gemacht werden, damit jeder ihre negativen Folgen spüren kann? Wie kann beispielsweise begreiflich gemacht werden, dass das Stehlen eines Programms strafbar ist, obwohl der bestohlene Nutzer keinerlei sichtbaren Schaden erlitten hat, denn er verfügt weiterhin über das Programm (im Gegensatz zum Opfer eines "Diebstahls" in der traditionellen Welt)? Wie können die finanziellen Verluste "sichtbar" gemacht werden, die durch die Verbreitung eines Virus entstehen, was häufig eine größere Wirtschaftssabotage ist als ein Brand oder ein Sprengstoffanschlag, wenngleich die physischen Wirkungen weniger spektakulär sind (keine Flammen, kein Lärm …)? Wie kann man die Computerkriminalität bekämpfen, obwohl ein großer Teil der wirtschaftlichen Computerstraftaten (insbesondere die Verbreitung von Viren und das Eindringen in bestimmte Informationssysteme) nicht aus den hergebrachten Motiven (Geld, Macht, Rache usw.) begangen werden, und es häufig anscheinend "sinnlose" Taten sind, eher aus Größenwahn *("ich bin stärker als die raffiniertesten Systeme "*) und um bekannt zu werden, als aus Gewinnsucht? Welche Beziehungen bestehen zwischen Computerkriminalität und Ausgrenzung? Welche Politik ist zur Verhütung denkbar?

4.8.2 Das Vertrauen in das Internet kann nur gestärkt werden, wenn diese Art von Problemen besser untersucht und besser bekannt sind, damit sie besser gelöst werden können.

5. Schlussfolgerungen

5.1 Der Wirtschafts- und Sozialausschuss teilt den Standpunkt der Kommission zur Bedeutung der Verbreitung und Nutzung der neuen digitalen Techniken. In bestimmten Bereichen ist deren Bedeutung bereits so groß, dass eine "Abhängigkeit eines Teils der Wirtschaftstätigkeit von der Computerwelt" festgestellt werden kann. Diese "Abhängigkeit von der Computerwelt" nimmt weiter zu.

5.1.1 Dabei stimmt der Ausschuss ebenfalls der Analyse der Kommission zu, dass stets wirksamere praktische und rechtliche Mittel eingesetzt werden müssen, je mehr die Wirtschaft von diesen Technologien abhängig wird.

In diesem sich entwickelnden Umfeld begrüßt der Ausschuss die von der Kommission in ihrer Mitteilung ins Auge gefassten Initiativen. Der Ausschuss verweist mit Nachdruck auf die Dringlichkeit gewisser Entscheidungen und auf die Notwendigkeit, die Festlegung der Modalitäten der Regulierung zu beschleunigen.

5.2 Um einen Beitrag zu den Überlegungen zu leisten, möchte der Ausschuss folgende Aspekte unterstreichen:

5.2.1 In der Kommissionsmitteilung werden zahlreiche repressive Maßnahmen vorgeschlagen. Es ist notwendig, diese um breiter angelegte Maßnahmen in den Bereichen Verhütung, Schulung und Bekämpfung der Ausgrenzung zu ergänzen.

5.2.2 Die Sicherheit der Informationsinfrastrukturen sollte noch stärker berücksichtigt werden.

5.2.3 Wenngleich die Nutzer - wie die Kommission angibt - zum Teil für die Sicherheit verantwortlich sein können, so muss doch auch die Rolle der großen Akteure, nämlich der Betreiber der Telekommunikationsnetze und der Staaten definiert werden. Diese Sicherheit kann zwar teilweise von "starken oder versierten" Nutzern (Großunternehmen oder Institutionen) gewährleistet werden, aber können wirklich auch "schwächere oder unerfahrene" Nutzer (kleine Unternehmen, Einzelpersonen und insbesondere Kinder) für diese Sicherheit sorgen?

5.2.4 Es muss eingehender untersucht werden, welchen Einfluss die Mitgliedstaaten und die EU auf das Management und die Überwachung der großen Organisationen haben, die das Internet verwalten.

5.2.5 Die Angleichung der Befugnisse der Strafverfolgungsbehörden muss eine Priorität werden, damit der "Opferschutz" verbessert wird. Die den Strafverfolgungsbehörden zu übertragenden neuen Befugnisse müssen die Grundrechte des Schutzes der Privatsphäre und des Schutzes der in der Charta der Grundrechte der Europäischen Union aufgeführten Daten wahren.

5.2.6 Gemäß der Erläuterung seitens der Kommission ist es notwendig, die Überwachung des Fernmeldeverkehrs zu reglementieren. Diese Vorgabe sollte jedoch ausgeweitet werden, indem darauf zu bestehen ist, dass diese Grundsätze der Vertraulichkeit überall, auch im internen Geschäftsablauf der Unternehmen, eingehalten werden. Der Ausschuss begrüßt und unterstützt die Bemühungen des Europäischen Parlaments, die ganze Wahrheit über das weltweit wirkende Überwachungsnetz mit der Bezeichnung ECHELON ans Licht zu bringen, und fordert den Ministerrat auf, in dieser Frage mit Nachdruck zu intervenieren.

5.2.7 Damit ein reibungsloser Betrieb des Internets gewährleistet wird und die Computerkriminalität bekämpft werden kann, sind folgende Fragen am dringendsten zu behandeln: die Notwendigkeit, bestimmte Verkehrsdaten aufzubewahren, sowie die Reglementierung des anonymen Zugangs und der anonymen Nutzung.

5.2.8 Die Einrichtung eines EU-Forums, das eine Vielzahl von Akteuren mit dem Ziel vereint, die Zusammenarbeit auf EU-Ebene zu verbessern, ist eine gute Initiative. Als Vertreter der organisierten Zivilgesellschaft hat der Ausschuss beschlossen, an den Arbeiten des Forums aktiv mitzuwirken.

5.2.9 Es ist notwendig - mehr noch als dies in der Mitteilung der Fall ist - die enormen Risiken hervorzuheben und zu analysieren, die den KMU durch die Sicherheitslücken im Internet

entstehen (Zerstörung und Verlust von Dateien, Diebstahl vertraulicher Dateien, Viren in den Datenverarbeitungssystemen usw.).

5.2.10 Die Grundzüge des FTE-Rahmenprogramms, auf das in der Mitteilung verwiesen wird, gehen in die richtige Richtung. Zwei Themen haben jedoch offenbar wesentliche Bedeutung:

– Bis zu welcher Stufe der Komplexität kann das Internet entwickelt werden, ohne dass es zu einer nicht mehr hinnehmbaren Anfälligkeit kommt?

– Welche Besonderheiten hat die Computerkriminalität in der virtuellen Welt gegenüber der üblichen Kriminalität in der "realen und konkreten" Welt?

Brüssel, den 12. September 2001

Der Präsident des Wirtschafts- und Sozialausschusses	Der Generalsekretär des Wirtschafts- und Sozialausschusses
Göke FRERICHS	Patrick VENTURINI