Stellungnahme des Ausschusses der Regionen zu der „Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Sicherheit der Netze und Informationen: Vorschlag für einen Europäischen Politikansatz“

(2002/C 107/27)

DER AUSSCHUSS DER REGIONEN,

gestützt auf die Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Sicherheit der Netze und Informationen: Vorschlag für einen europäischen Politikansatz (COM(2001) 298 endg.),

aufgrund des Beschlusses der Kommission vom 7. Juni 2001, ihn gemäß Artikel 265 Absatz 1 des Vertrags zur Gründung der Europäischen Gemeinschaft um Stellungnahme zu diesem Thema zu ersuchen,

aufgrund des Beschlusses des Präsidenten vom 2. Juli 2001, die Fachkommission 3 „Transeuropäische Netze, Verkehr, Informationsgesellschaft“ mit der Ausarbeitung der Stellungnahme zu diesem Thema zu beauftragen,

gestützt auf den Beschluss seines Präsidenten vom 26. Oktober 2001, Frau Barrero Florez gemäß Artikel 40 Absatz 2 der Geschäftsordnung des Ausschusses der Regionen zur Hauptberichterstatterin für die Erarbeitung der Stellungnahme zu diesem Thema zu bestellen,

gestützt auf seine Stellungnahme zu der Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Schaffung einer sichereren Informationsgesellschaft durch Verbesserung der Sicherheit von Informationsinfrastrukturen und Bekämpfung der Computerkriminalität (COM(2000) 890 endg. — CdR 88/2001 fin),

gestützt auf die „Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen — Sicherheit und Vertrauen in elektronische Kommunikation — ein europäischer Rahmen für digitale Signaturen und Verschlüsselung“ (COM(97) 503 endg.),

gestützt auf die „Mitteilung der Kommission an den Rat und das Europäische Parlament — *e*Europe 2002: Auswirkungen und Prioritäten“ (COM(2001) 140 endg.),

gestützt auf den Aktionsplan *e*Europe 2002 (COM(2000) 330 endg.),

gestützt auf den Entwurf eines Übereinkommens des Europarats über Datennetzkriminalität (COM(2001) 103),

gestützt auf die Empfehlung des Rates über gemeinsame Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik ([1]),

gestützt auf die Empfehlung des Rates über Kontaktstellen mit einem rund um die Uhr erreichbaren Dauerdienst zur Bekämpfung der Hightech-Kriminalität ([2]),

gestützt auf die Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr ([3]),

gestützt auf die Entschließung Nr. 9194/01 des Rates vom 20. Juni 2001 über die operativen Anforderungen der Strafverfolgung in Bezug auf öffentliche Telekommunikationsnetze und -dienste,

gestützt auf die Schlussfolgerungen des Europäischen Rates von Stockholm vom März 2001,

gestützt auf die Richtlinie 90/388/EWG der Kommission über den Wettbewerb auf dem Markt für Telekommunikationsdienste,

---

([1]) ABl. L 93 vom 26.4.1995.
([2]) ABl. C 187 vom 3.7.2001.
([3]) ABl. L 8 vom 12.1.2001.

gestützt auf die Richtlinie 95/46/EWG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr,

gestützt auf die Richtlinie 97/33/EG über die Zusammenschaltung in der Telekommunikation im Hinblick auf die Sicherstellung eines Universaldienstes und der Interoperabilität durch Anwendung der Grundsätze für einen offenen Netzzugang (ONP),

gestützt auf die Richtlinie 97/66/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation,

gestützt auf die Richtlinie 98/10/EG über die Anwendung des offenen Netzzugangs (ONP) beim Sprachtelefondienst und dem Universaldienst im Telekommunikationsbereich in einem wettbewerbsorientierten Umfeld,

gestützt auf die Richtlinie 99/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen,

gestützt auf die Richtlinie 2000/31/EG über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt (Richtlinie über den elektronischen Geschäftsverkehr),

gestützt auf den Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation ([1]),

gestützt auf den Stellungnahmeentwurf CdR 257/2001 (Hauptberichterstatterin: Frau Barrero Florez, E/PSE, Leiterin der Hauptabteilung für Europa-Fragen, Regierung der autonomen Region Asturien),

in der Erwägung, dass die Informationsnetze und -systeme zu einem wesentlichen Faktor der wirtschaftlichen und sozialen Entwicklung unserer Gesellschaft geworden sind, und von ihrer reibungslosen Funktion hängen lebenswichtige Infrastrukturen, beispielsweise im Energie- und im Verkehrsbereich, sowie der überwiegende Teil der öffentlichen und privaten Dienste und der Wirtschaft insgesamt ab,

in der Erwägung, dass die Sicherheit der Informationsnetze und -systeme eine Voraussetzung für künftige Fortschritte bei der Erschließung neuer Dienste ist, neuer Wirtschaftsbereiche und innovativer Handelsbeziehungen usw.,

in der Erwägung, dass das Vertrauen der Anwender der Informationsnetze durch die wachsende Zahl von Verstößen gegen die Sicherheit dieser Netze stark beeinträchtigt wird,

in der Erwägung, dass das fehlende Vertrauen in die Informationsnetze und -systeme eine rasche allgemeine Verbreitung der neuen Dienste der Informations- und Wissensgesellschaft verhindert,

in der Erwägung, dass die Sicherheit dieser Netze und Systeme eine Herausforderung für die politischen Entscheidungsträger darstellt, die sich im Klaren darüber sein müssen, welche Bedeutung diese Systeme haben, welche Aspekte und Sicherheitsprobleme damit verbunden sind und welche Rolle sie bei einer Verbesserung dieser Systeme übernehmen können,

in der Erwägung, dass Zwar bereits ein umfangreiches Bündel von legislativen Maßnahmen im Telekommunikationsbereich und im Bereich des Schutzes personenbezogener Daten, sowohl auf nationaler als auch auf EU-Ebene, verabschiedet worden ist, doch sind noch keine spezifischen Maßnahmen im Bereich der Sicherheit angenommen worden,

in der Erwägung, dass nach wie vor viele Probleme im Zusammenhang mit der Sicherheit der Informationsnetze und -systeme ungelöst sind, und einige Lösungen sind auf Grund der marktinhärenten Unzulänglichkeiten noch nicht in die Praxis umgesetzt worden,

in der Erwägung, dass die Behörden bei der Nachbesserung von Marktmängeln eine Aufgabe zu erfüllen haben,

---

([1]) ABl. C 365 vom 19.12.2000.

in der Erwägung, dass spezifische politische Maßnahmen zur Behebung von Marktlücken bei der Sicherheit der Informationsnetze und -systeme könnten der Dynamik des Marktes sowie der wirksamen Funktion des rechtlichen Rahmens förderlich sein,

in der Erwägung, dass diese Maßnahmen in ein europäisches Konzept zur Förderung der Entwicklung der Informations- und Wissensgesellschaft in der EU eingebettet sein sollten, dabei auf gemeinsamen Lösungen aufbauen und ein wirksames Handeln auf internationaler Ebene ermöglichen,

in der Erwägung, dass die Vielschichtigkeit des Problems die Berücksichtigung der damit verbundenen politischen, wirtschaftlichen, organisatorischen und technischen Aspekte sowie seiner dezentralen und globalen Dimension erfordert,

in der Erwägung, dass die Sicherheitsmängel der Informationsnetze und -systeme in den europäischen Regionen mit Entwicklungsrückstand Folgen können haben, die das derzeitige digitale Gefälle zwischen diesen Regionen und den besser entwickelten, sicheren Regionen verschärfen,

in der Erwägung, dass die lokalen und regionalen Gebietskörperschaften eine wichtige Rolle bei der Durchführung einer europäischen Politik im Bereich der Sicherheit der Informationsnetze und -systeme übernehmen können, da ihre Nähe zu den Bürgern, Organisationen und Unternehmen eine wirksame und angemessene Umsetzung der konkreten Maßnahmen, die beschlossen werden, begünstigen;

verabschiedete auf seiner 41. Plenartagung am 14. und 15. November 2001 (Sitzung vom 15. November) einstimmig folgende Stellungnahme.

Einleitung

Der Ausschuss der Regionen

1. teilt die wachsende Besorgnis der Kommission über die Sicherheit der Informationsnetze und -systeme, zumal diesen Systemen eine kritische Bedeutung für die Entwicklung der Informations- und Wissensgesellschaft sowie für das globale Wirtschaftssystem zukommt;

2. stimmt der in der Mitteilung vertretenen Auffassung zu, dass die Europäische Union der Sicherheit der Informationsnetze und -systeme politische Priorität einräumen muss. Der Markt ist nicht in der Lage, allein eine Lösung zu entwickeln, da es zwar ein großes Angebot an relevanten Technologien und Sicherheitsstandards aber keine anerkannte offene und gemeinsame Norm gibt;

3. befürwortet das Ziel der Mitteilung, zu analysieren, in welchen Bereichen politische Maßnahmen auf europäischer oder nationaler Ebene eingeführt oder verstärkt werden müssen, um letztendlich eine gemeinschaftliche Politik im Bereich der Netz- und Informationssicherheit zu entwickeln;

4. wirft besorgt die Frage auf, inwieweit die Maßnahmen, die zur Verbesserung der Netz- und Informationssicherheit ergriffen werden sollen, mit der Wahrung der freiheitlichen und bürgerlichen Rechte zu vereinbaren sind, die in der Allgemeinen Erklärung der Menschenrechte, im Internationalen Pakt über bürgerliche und politische Rechte sowie in der Europäischen Menschenrechtskonvention verankert sind. Vor diesem Hintergrund wünscht er, dass Befugnissen und Zuständigkeiten, die auf eine Einschränkung der Bürgerrechte hinauslaufen könnten, klare Grenzen gesetzt werden. Nach Auffassung des Ausschusses ist es möglich, die Wahrung der freiheitlichen und bürgerlichen Rechte mit der Netz- und Informationssicherheit in Einklang zu bringen;

5. bezweifelt angesichts des grenzüberschreitenden Charakters des Problems, dass die verfolgten Sicherheitsziele durch eine auf Gemeinschaftsebene konzertierte Vorgehensweise, doch ohne Abstimmung mit den internationalen Organisationen und anderen Wirtschaftsmächten erreicht werden können;

6. fordert die Kommission auf, angesichts der Bedeutung und Dringlichkeit einer angemessenen Netz- und Informationssicherheit ausreichende Mittel für die Durchführung der entsprechenden Maßnahmen vorzusehen.

Analyse von Fragen der Netz- und Informationssicherheit

Der Ausschuss der Regionen

7. hält die in der Mitteilung vorgegebene Definition der Netz- und Informationssicherheit „als die Fähigkeit eines Netzes oder Informationssystems, mit einem vorgegebenen Niveau Störungen oder böswillige Aktionen abzuwehren, die die Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von gespeicherten oder übermittelten Daten und damit zusammenhängenden Diensten, die über dieses Netz oder Informationssystem angeboten werden bzw. zugänglich sind, beeinträchtigen“ in Bezug auf die Formulierung „mit einem vorgegebenen Niveau“ für undurchsichtig. Nach Ansicht des Ausschusses der Regionen darf es keine Einstufung böswilliger Absichten oder Einbrüche in ein Netz oder Informationssystem nach einem „vorgegebenen“ Sicherheitsniveau geben;

8. stellt mit Sorge fest, dass die Betreiber von Telekommunikationsdiensten und Anbieter von Netzzugangsdiensten in Europa allgemein weder prioritär noch verhältnismäßig in Sicherheitsmaßnahmen investieren. Hinzu kommt noch, dass kleine, auf regionaler Ebene tätige Betreiber, die in erster Linie eine wirtschaftlich rentable Marktposition anstreben und darum Sicherheitsvorkehrungen vernachlässigen, die Lage weiter erschweren;

9. ist der Ansicht, dass Vertrauen in die Verschlüsselungsprodukte weitgehend auf das Vorhandensein offener internationaler Standards und Normen zurückzuführen sein wird, und hält die unkoordinierten Bemühungen einiger Mitgliedstaaten, Software mit frei zugänglichem Quellcode für die Förderung der Verschlüsselung einzusetzen, angesichts der vehementen und unaufhaltsamen marktorientierten Initiative des Privatsektors für überflüssig;

10. bestätigt, dass der Wettbewerb zwischen Geräte- und Softwareproduzenten nicht zu höheren Investitionen in Sicherheitsmaßnahmen führen wird, und schlägt die Prüfung von Maßnahmen zur Förderung entsprechender Investitionen vor;

11. hält es für erforderlich, die Betreiber von Telekommunikationsdiensten und Anbieter von Zugangsdiensten zur Erfüllung von Mindestsicherheitsvorkehrungen zu verpflichten, die auf Gemeinschaftsebene festzusetzen sind.

Ein europäischer Politikansatz

Der Ausschuss der Regionen

12. vertritt die Auffassung, dass eine ausgewogene Entwicklung der Informations- und Wissensgesellschaft in der Europäischen Union den Zusammenhalt und die Strukturierung des Europas der Regionen erleichtern wird und daher die Gewährleistung der Netz- und Informationssicherheit unerlässlich ist;

13. stimmt mit der Kommission darin überein, dass sämtliche Investitionen in die Verbesserung der Netz- und Informationssicherheit mit sozialem Nutzen verbunden sind, und hebt hervor, dass ein Ausbleiben dieser Investitionen seitens der Hersteller, Betreiber und Diensteanbieter der Gesellschaft hohe soziale Kosten verursacht und das Gemeinwohl beeinträchtigt;

14. fordert die Kommission auf, die Notwendigkeit zu prüfen, bestimmte Sicherheitskriterien und -normen aufzustellen, die alle als grundlegend eingestuften Informationssysteme (Dienste von allgemeinem Interesse), die mit den Telekommunikationsnetzen verbunden sind, sowie die eigentlichen Netze selbst obligatorisch erfüllen müssen;

15. befürwortet eine größtmögliche Sicherheit bei gleichzeitiger Wahrung von Fazilität und Qualität des Zugangs zur Informations- und Wissensgesellschaft, hält allerdings ein bestimmtes Mindestmaß an Sicherheit für unabdingbar, auch wenn darunter die Qualität des Zugangs leiden sollte;

16. stimmt der Kommission darin zu, dass:

— ein gemeinsames Verständnis der Sicherheitsprobleme und der zu ergreifenden Maßnahmen erforderlich ist;

— politische Maßnahmen den Markt ergänzen und gleichzeitig das Funktionieren des gesetzlichen Rahmens verbessern können;

— ein europäischer Ansatz erforderlich ist, um den Binnenmarkt für solche Dienste zu sichern, um von gemeinsamen Lösungen zu profitieren und um effektiv auf globaler Ebene handeln zu können;

17. befürwortet eine Ergänzung der in der Mitteilung vorgeschlagenen Sensibilisierungsmaßnahmen durch investitionsfördernde Maßnahmen im Sicherheitsbereich, um zu verhindern, dass die wirtschaftlichen Kosten die Annahme der als notwendig erkannten Maßnahmen untergraben;

18. hebt hervor, dass die lokalen und regionalen Behörden aus operativen und praktischen Gründen eine wichtige Rolle bei jedweder Sensibilisierungskampagne in diesem Bereich zu übernehmen haben;

19. stimmt zu, dass das CERT-System der Europäischen Union dringend ausgebaut und die bestehenden Zentren personell, technisch und wirtschaftlich ausreichend ausgestattet werden müssen;

20. empfiehlt eine bessere, direktere und flexiblere Verbindung der europäischen CERT-Systeme zu den potentiellen Endnutzern;

21. befürwortet die in der Mitteilung vorgeschlagenen Maßnahmen für ein europäisches Warn- und Informationssystem und schlägt gleichzeitig eine proaktive Vorgehensweise wie beispielsweise die Einrichtung einer europäischen Agentur für Netz- und Informationssicherheit vor, die unter anderem zur Aufgabe hätte, sämtliche Software (Betriebssysteme, Navigationssysteme, E-mail-Anbieter usw.) zu prüfen und zu testen, die in öffentlichen Informationsnetzen eingesetzt werden sollen, um Sicherheitsmängel von in der EU noch nicht im Handel befindlicher Software aufzudecken. Nach Ansicht des Ausschusses der Regionen wird der Auftrag des künftigen, der gemeinsamen Forschungsstelle unterstellten Instituts für den Schutz und die Sicherheit der Bürger nicht dieser vorgeschlagenen Agentur entsprechen;

22. befürchtet, dass über die FTE-Rahmenprogramme der EU finanzierte Untersuchungen der Netz- und Informationssicherheit, die nicht auch durch die großen Softwarehersteller unterstützt werden, nicht zu den gewünschten Ergebnissen führen werden. Der Ausschuss der Regionen schlägt vor, unabhängig davon Maßnahmen zu ergreifen, um die großen Softwarehersteller auf dem Weltmarkt dazu zu bewegen, sich stärker für die Forschung im Bereich der Netz- und Informationssicherheit und ihre unmittelbare praktische Anwendung einzusetzen;

23. ist besorgt angesichts der mangelnden Interoperabilität der verschiedenen technischen Lösungen der Hersteller und angesichts deren Desinteresse an gemeinsamen offenen Normen;

24. empfiehlt, nicht die Anwendung bestimmter Lösungen oder Verschlüsselungsprodukte zu fördern, denn es ist darauf hinzuarbeiten, dass alle Lösungen in einer gemeinsamen offenen und von allen Herstellern akzeptierten Norm zusammenlaufen;

25. hält es für grundlegend, dass die verschiedenen europäischen Zertifizierungsstellen Vereinbarungen über die gegenseitige Anerkennung der von ihnen ausgestellten Zertifikate treffen. Ohne solche Vereinbarungen ist die Nützlichkeit dieser elektronischen Zertifikate sehr begrenzt und ihre Verwendung dürfte weit hinter dem erwünschten angestrebten Ausmaß zurückbleiben. Die Einrichtung von Zertifizierungsstellen auf regionaler Ebene, die nicht interoperable technologische Lösungen anwenden, würde zweifelsohne das Ziel eines strukturierten, von Zusammenhalt geprägten Europas der Regionen in weitere Ferne rücken;

26. begrüßt nachdrücklich die europäischen Initiativen zur Normung elektronischer Signaturen (EESSI), intelligente Chipkarten in *e*Europe und für Infrastrukturen für öffentliche Schlüssel (PKI);

27. stimmt zu, dass die Harmonisierung von Spezifizierungen zu erhöhter Kompatibilität führen und gleichzeitig eine schnellere Umsetzung durch die Marktteilnehmer ermöglichen wird;

28. unterstützt alle vorgeschlagenen Maßnahmen zur marktorientierten Förderung der Normung und Zertifizierung und hält die Annahme einer legislativen Maßnahme über die gegenseitige Anerkennung von Zertifikaten für erforderlich;

29. hält es für sinnvoll, regelmäßig zu überprüfen, inwieweit die Betreiber von Telekommunikationsdiensten die technischen und organisatorischen Maßnahmen umgesetzt haben, die sie im Einklang mit Artikel 4 der Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation im Hinblick auf die Gewährleistung der Sicherheit ihrer Dienste einführen müssen;

30. macht die Kommission auf die schwerwiegenden Folgen potenzieller Datennetzkriminalität seitens terroristischer Gruppen aufmerksam, die ausschließlich das Ziel verfolgen, der Gesellschaft maximalen Schaden in Form politischer Erpressung zuzufügen;

31. befürwortet alle vorgeschlagenen rechtlichen Maßnahmen und hält es für erforderlich, die nationalen Rechtsvorschriften über Datennetzkriminalität anzugleichen und zu harmonisieren, um zu verhindern, dass von einzelnen europäischen Staaten aus entsprechende Handlungen ungestraft oder unter Androhung geringer Strafen durchgeführt werden können;

32. schlägt vor, dass auf einzelstaatlicher Ebene, da, wo sie noch nicht existieren, auf Datennetzkriminalität spezialisierte polizeiliche Dienste eingerichtet werden und alle bestehenden Dienste koordiniert werden. Ferner müssen sie mit den notwendigen personellen und technischen Mitteln ausgestattet werden;

33. empfiehlt, dass zur Bekämpfung der Computerkriminalität besondere Staatsanwälte eingesetzt werden, die dank einer umfassenden Spezialausbildung die öffentliche Anklage mit der nötigen Effizienz betreiben können. Die Kommunikation und Koordination zwischen diesen Staatsanwälten ist von der gleichen grundlegenden Bedeutung wie die Ausbildung von Richtern und Justizbeamten auf diesem Gebiet. Ziel ist die wirksame strafrechtliche Verfolgung jener Taten, die die Sicherheit der Informationsnetze und deren Nutzer gefährden;

34. stimmt der Mitteilung der Europäischen Kommission darin vorbehaltlos zu, dass durch die Entwicklung elektronischer Behördendienste — auf die viele regionale und lokale Gebietskörperschaften gesetzt haben, um ihre Beziehungen zu den Bürgern, die Qualität ihrer Dienstleistungen und überhaupt das Wohlbefinden und die demokratische Teilhabe der Bürger zu verbessern — die öffentliche Verwaltung sowohl zum potenziellen Vorbild für wirksame und sichere Lösungen als auch zum Marktbeteiligten wird, der in der Lage ist, durch seine Beschaffungsentscheidungen die Entwicklungen zu beeinflussen. Diesbezüglich haben die öffentlichen Behörden im Einklang mit ihren Zuständigkeiten eine Impulsgeberfunktion bei der Entwicklung der Informations- und Wissensgesellschaft. Ohne die Sicherheit der von den Behörden genutzten Informationsnetze und -systeme wird auch das Vertrauen der Bürger fehlen, wodurch wiederum der Entwicklung der neuen Gesellschaft großer Schaden zugefügt werden wird;

35. schlägt vor, dass die Maßnahmen im Zusammenhang mit der öffentlichen Verwaltung auf die drei Verwaltungsebenen (kommunal, regional und national) ausgerichtet werden und dass die Kompatibilität der eingesetzten Lösungen unabdingbar sein muss;

36. befürwortet nachdrücklich die Förderung des Dialogs mit internationalen Organisationen und Partnern über Netzsicherheit und insbesondere über die Verbesserung der Stabilität von elektronischen Netzen, und fordert die Kommission auf, sich für die Einberufung eines globalen Gipfeltreffens über die Netz- und Informationssicherheit, an dem auch die Hersteller und Betreiber teilnehmen, sowie für die Einrichtung eines europäischen Forums zur Bekämpfung der Computerkriminalität einzusetzen. Auch fordert er die Mitgliedstaaten auf, die vor kurzem verabschiedete internationale Konvention gegen die Datennetzkriminalität zu unterzeichnen, damit sie so bald wie möglich in Kraft treten und die in ihr genannten rechtlichen Mittel angewandt werden können.

Brüssel, den 15. November 2001.

Der Präsident

des Ausschusses der Regionen

Jos CHABERT