Advies van het Comité van de Regio's over de „Mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's — Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak"

(2002/C 107/27)

HET COMITÉ VAN DE REGIO'S,

gezien de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's — Netwerk- en informatieveiligheid: Voorstel voor een Europese beleidsaanpak (COM(2001) 298 def.);

gezien het besluit van de Commissie van 7 juni 2001 om het CvdR, overeenkomstig artikel 265, eerste alinea, van het EG-Verdrag, over dit onderwerp te raadplegen;

gezien het besluit van zijn voorzitter van 2 juli 2001 om commissie 3 „Trans-Europese netwerken, vervoer, informatiemaatschappij" met de voorbereidende werkzaamheden te belasten;

gezien het besluit van zijn voorzitter d.d. 26 oktober 2001 om mevrouw Barrero Floréz aan te wijzen als algemeen rapporteur voor dit advies, overeenkomstig artikel 40.2 van het reglement van orde;

gezien zijn advies over de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's — De informatiemaatschappij veiliger maken door de informatie-infrastructuur beter te beveiligen en computercriminaliteit te bestrijden (COM(2000) 890 def. — CDR 88/2001 fin);

gezien de mededeling van de Commissie aan de Raad, het Europees Parlement, het Economisch en Sociaal Comité en het Comité van de Regio's — Zorgen voor veiligheid van en vertrouwen in elektronische communicatie — Naar een Europees kader voor digitale handtekeningen en encryptie (COM(97) 503 def.);

gezien de mededeling van de Commissie aan de Raad en het Europees Parlement — eEurope 2002: Effecten en prioriteiten (COM(2001) 140 def.);

gezien het actieplan eEurope 2002 (COM(2000) 330 def.);

gezien het ontwerpverdrag over computercriminaliteit van de Raad van Europa (COM(2001) 103);

gezien de aanbeveling van de Raad inzake gemeenschappelijke veiligheidsbeoordelingscriteria voor informatietechnologie ([1]);

gezien de aanbeveling van de Raad betreffende meldpunten die 24 uur per dag operationeel zijn voor de bestrijding van hightech-criminaliteit ([2]);

gezien Verordening (EG) nr. 45/2001 van het Europees Parlement en de Raad betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens door de communautaire instellingen en organen en betreffende het vrije verkeer van die gegevens ([3]);

gezien Resolutie nr. 9194/01 van de Raad van 20 juni 2001 over de operatieve behoeften van de autoriteiten die bevoegd zijn voor de netwerken en de openbare dienstverlening op het gebied van telecommunicatie;

gezien de conclusies van het voorzitterschap van de Raad van Stockholm (maart 2001);

gezien Richtlijn 1990/388/EG over de concurrentie in de sector telecommunicatiediensten;

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

gezien Richtlijn 1995/46/EG over de bescherming van natuurlijke personen inzake de verwerking van persoonsgegevens en het vrije verkeer van deze gegevens;

gezien Richtlijn 1997/33/EG over interconnectie op telecommunicatiegebied, wat betreft de waarborging van de universele dienst en van de interoperabiliteit door toepassing van de beginselen van open network provision (ONP);

gezien Richtlijn 1997/66/EG betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector;

gezien Richtlijn 1998/10/EG inzake de toepassing van open network provision (ONP) op spraaktelefonie en inzake de universele telecommunicatiedienst in een door concurrentie gekenmerkt klimaat;

gezien Richtlijn 1999/93/EG over een gemeenschappelijk kader voor elektronische handtekeningen;

gezien Richtlijn 2000/31/EG over bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt („Richtlijn inzake elektronische handel");

gezien het voorstel voor een richtlijn van het Europees Parlement en de Raad betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie [1];

gezien het ontwerpadvies (CDR 257/2001 rev. — rapporteur: mevrouw Barrero Flórez (E/PSE), directeur-generaal Europese aangelegenheden Asturië);

overwegende dat informatienetwerken en -systemen zich hebben ontwikkeld tot een factor van cruciaal belang voor de sociaal-economische ontwikkeling van de huidige maatschappij en dat het goede functioneren hiervan cruciaal is voor essentiële infrastructuur zoals het energie- en het wegennet, voor bijna alle openbare en particuliere diensten en voor de economie in haar geheel;

overwegende dat de veiligheid van informatienetten en -systemen in de toekomst een voorwaarde zal zijn voor de ontwikkeling van bijvoorbeeld nieuwe diensten, nieuwe bronnen van economische welvaart en nieuwe handelsbetrekkingen;

overwegende dat het toenemende aantal inbreuken op de veiligheid van de informatienetwerken het vertrouwen van de gebruikers hiervan ernstig aantast;

overwegende dat de algemene invoering van de nieuwe, met de informatie- en kennismaatschappij samenhangende diensten vertraging oploopt door dit gebrek aan vertrouwen in de informatienetwerken en -systemen;

overwegende dat de veiligheid van deze netwerken en systemen inmiddels een topprioriteit is voor de politiek verantwoordelijken, die moeten inzien hoe belangrijk deze kwestie in al haar facetten is en zich rekenschap dienen te geven van de bijdrage die zij kunnen leveren aan een betere veiligheid;

overwegende dat nog steeds geen specifieke veiligheidsmaatregelen zijn genomen, hoewel op het gebied van telecommunicatie en de wettelijke bescherming van persoonsgegevens al wel heel wat nationale en EU-maatregelen zijn getroffen;

overwegende dat er wat de veiligheid van informatienetwerken en -systemen betreft nog tal van problemen bestaan en dat sommige oplossingen maar langzaam de markt bereiken door tekortkomingen in de marktwerking;

overwegende dat de diverse overheden oplossingen moeten helpen vinden om die tekortkomingen en gebreken in de marktwerking te ondervangen;

---

[1] PB C 365 van 19.12.2000.

overwegende dat de specifieke beleidsmaatregelen om de problemen met de veiligheid van de informatienetten en -systemen enigszins te verminderen ertoe zouden kunnen leiden dat de sector dynamischer wordt en de regelgeving beter toe te passen is;

overwegende dat deze maatregelen deel zouden moeten uitmaken van een Europese aanpak om te zorgen voor de ontwikkeling van de informatie- en kennismaatschappij in de EU, profijt te trekken van gemeenschappelijke oplossingen en in internationaal verband efficiënt te kunnen optreden;

overwegende dat de problemen zeer complex zijn en dat met al hun politieke, economische, organisatorische en technische aspecten en met hun algemene, decentrale karakter rekening moet worden gehouden;

overwegende dat door de gebrekkige veiligheid van de informatienetwerken en -systemen in regio's met een ontwikkelingsachterstand mogelijk het gevaar bestaat dat de digitale kloof tussen deze regio's en de meest ontwikkelde en veilige regio's alleen maar breder wordt;

overwegende dat de lokale en regionale overheden een vooraanstaande rol kunnen en moeten spelen bij de uitvoering van een Europees beleid om de veiligheid van informatienetwerken en -systemen te vergroten; zij staan namelijk dicht bij de bevolking en de betrokken organisaties en bedrijven en zijn daardoor in staat om de maatregelen efficiënt en adequaat uit te voeren,

heeft tijdens zijn 41e zitting van 14 en 15 november 2001 (vergadering van 15 november) het volgende advies met algemene stemmen goedgekeurd.

Inleiding

1. Het Comité van de Regio's begint zich evenals de Commissie steeds meer zorgen te maken over de veiligheid van de informatienetwerken en -systemen en is het met haar eens dat deze veiligheid inmiddels niet alleen cruciaal is voor de ontwikkeling van de informatie- en kennismaatschappij, maar ook voor het huidige gemondialiseerde economische systeem.

2. De Commissie is terecht van mening dat de veiligheid van de informatienetwerken en -systemen een beleidsprioriteit van de EU moet worden. De markt heeft geen uniforme oplossing kunnen bieden, waardoor het nu wemelt van de verschillende technologieën en veiligheidsnormen. Het schort aan een open, algemeen aanvaarde norm.

3. De Commissie stelt zichzelf terecht als doel om aan te geven waar aanvullende of krachtigere maatregelen van de lidstaten of de EU nodig zijn, zodat aan de hand daarvan een EU-beleid voor de veiligheid van informatienetwerken en -systemen kan worden uitgewerkt.

4. Het CvdR vraagt zich met enige zorg af in hoeverre de voorgestelde maatregelen om informatienetwerken en -systemen veiliger te maken in overeenstemming zijn met de vrijheden en burgerrechten die zijn opgenomen in de Universele Verklaring van de Rechten van de Mens, het Internationaal Verdrag inzake burgerrechten en politieke rechten en het Europees Verdrag tot bescherming van de rechten van de mens. Bevoegdheden die eventueel tot aantasting van burgerrechten zouden kunnen leiden dienen dan ook duidelijk afgebakend te worden. De veiligheid van informatienetwerken en -systemen hoeft niet op gespannen voet te staan met burgerlijke vrijheden en burgerrechten.

5. Het CvdR vraagt zich, gezien het grensoverschrijdende karakter van de problemen, echter wel af of dit veiligheidsbeleid het gewenste effect kan sorteren als andere wereldmachten en internationale organisaties er niet mee instemmen.

6. Aangezien de veiligheid van de netwerken en systemen in kwestie zo snel mogelijk gewaarborgd moet worden, doet de Commissie er goed aan om de concrete maatregelen waartoe wordt besloten zo snel mogelijk uit te voeren en hiervoor voldoende financiële middelen vrij te maken.

Analyse van de problemen met de netwerk- en informatieveiligheid

7. De definitie die de Commissie geeft van het begrip „netwerk- en informatieveiligheid" is niet erg duidelijk: „de bestandheid van een netwerk of informatiesysteem met een gegeven mate van zekerheid tegen toevallige gebeurtenissen of opzettelijke handelingen waardoor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van opgeslagen of overgedragen gegevens en de diensten die door of via het netwerk worden aangeboden, in gevaar worden gebracht". Het gaat om die „gegeven mate van zekerheid": een informatienetwerk of -systeem moet altijd bestand zijn tegen opzettelijke handelingen of inbreuken. Op dit punt mag nooit geschipperd worden.

8. Het CvdR acht het verontrustend dat het gros van de telecommunicatie-exploitanten en *providers* investeringen in veiligheid niet als een prioriteit beschouwt en er daarom ook niet voldoende middelen aan besteedt. Bovendien zijn er kleine regionale exploitanten die er vooral op uit zijn om een gunstige marktpositie te verwerven en daarbij de veiligheid uit het oog verliezen. Ook met dit probleem dient rekening te worden gehouden.

9. Voor het vertrouwen in encryptieproducten zijn vooral open internationale normen of standaarden nodig. Tegenover de onstuitbare commerciële dadendrang van het bedrijfsleven zijn de ongecoördineerde initiatieven van een aantal lidstaten om *open source software* te steunen zinloos.

10. Het CvdR is het met de Commissie eens dat de concurrentie tussen de leveranciers van hardware en software momenteel niet leidt tot meer investeringen in de veiligheid. Het verdient dan ook aanbeveling om na te gaan met welke maatregelen dit wel bereikt kan worden.

11. Telecommunicatie-exploitanten en *service providers* zouden verplicht moeten worden om een aantal in EU-verband vast te stellen minimumnormen op het gebied van de veiligheid in acht te nemen.

Een Europees beleid

12. Een evenwichtige ontwikkeling van de informatie- en kennismaatschappij zal de samenhang en de structuur van het Europa van de Regio's ten goede komen. De veiligheid van de informatienetten en -systemen moet dan ook gewaarborgd worden.

13. Het CvdR deelt het standpunt van de Commissie dat investeringen in een betere netwerkbeveiling maatschappelijke baten met zich meebrengen. Als fabrikanten, exploitanten en providers niet genoeg investeren, ondervindt de samenleving daar ernstige schade van.

14. De Commissie doet er goed aan te onderzoeken in hoeverre het nodig is dat er veiligheidsnormen worden opgesteld waaraan alle telecommunicatienetwerken en de hierop aangesloten basisinformatiesystemen (diensten van openbaar belang) in ieder geval moeten voldoen.

15. Het CvdR is van mening dat een optimale veiligheid niet ten koste mag gaan van de soepele en betrouwbare toegang waarop de informatie- en kennismaatschappij gebaseerd is. Niettemin moet te allen tijde een minimumveiligheidsniveau gehandhaafd worden, zelfs al zou de toegankelijkheid van de systemen in kwestie daardoor worden bemoeilijkt.

16. De Commissie wijst er terecht op dat:

— er een gemeenschappelijk inzicht nodig is in de onderliggende veiligheidsproblematiek en de specifieke maatregelen die moeten worden getroffen;

— de marktwerking met beleidsmaatregelen kan worden versterkt, waardoor tegelijkertijd de werking van het regelgevingskader kan worden verbeterd;

— een Europese aanpak nodig is om ervoor te zorgen dat een interne markt voor communicatie- en informatiediensten gegarandeerd is, dat van gemeenschappelijke oplossingen kan worden geprofiteerd en dat effectief optreden op mondiaal niveau mogelijk is.

17. De voorgestelde bewustmaking zou moeten worden aangevuld met maatregelen om investeringen in de veiligheid van de netwerken te ondersteunen. Anders zouden dergelijke maatregelen, die als noodzakelijk worden beschouwd, wel eens kunnen uitblijven door de kosten die ermee gemoeid zijn.

18. Uit operationeel en praktisch oogpunt is het van belang dat lokale en regionale overheden een vooraanstaande rol krijgen bij bewustmakingscampagnes op dit gebied.

19. Het CvdR deelt het standpunt van de Commissie dat het systeem van CERT's (computer emergency response teams, oftewel „computercalamiteitenteams") in de EU zo snel mogelijk moet worden uitgebreid en dat de bestaande teams van voldoende menskracht en technische en economische middelen dienen te worden voorzien.

20. De relaties tussen de Europese CERT's en hun potentiële doelgroepen moeten worden uitgebreid en dienen directer en soepeler te worden.

21. Het CvdR stemt in met de voorgestelde opzet van een Europees waarschuwings- en informatiesysteem. Tegelijkertijd pleit het CvdR voor de oprichting van een Europees bureau voor de veiligheid van informatienetwerken en -systemen, dat onder meer alle software (operationele systemen, browsers, e-mailprogramma's enz.) zou moeten onderzoeken en testen die voor openbare informatienetten bestemd is. Op die manier kunnen eventuele hiaten in de veiligheid van software die nog niet in de EU op de markt gebracht is in een vroeg stadium worden opgespoord. Gezien zijn aard en zijn taken is het nog op te richten instituut voor de bescherming en veiligheid van burgers, dat zal ressorteren onder het Gemeenschappelijk Onderzoekscentrum, hier niet geschikt voor.

22. Als via de OTO-kaderprogramma's van de EU gefinancierd onderzoek naar de veiligheid van netwerken en informatie niet wordt gesteund door de grootste softwarefabrikanten, dan valt te vrezen dat de gewenste praktische resultaten uitblijven. Er zou dan ook voor moeten worden gezorgd dat deze fabrikanten, wat het onderzoek naar de veiligheid van de netten en informatie en de directe toepassing van de resultaten betreft, een grotere betrokkenheid aan de dag leggen.

23. Het baart het CvdR zorgen dat er momenteel geen sprake is van interoperabiliteit tussen de verschillende technologische oplossingen van de fabrikanten en dat dezen er niets voor voelen om gemeenschappelijke open normen uit te werken.

24. Het gebruik van bepaalde encryptie-oplossingen of -producten moet niet gestimuleerd worden. Er moet daarentegen voor gezorgd worden dat alle oplossingen voldoen aan één gemeenschappelijke open en door alle fabrikanten aanvaarde norm.

25. Het is van fundamenteel belang dat de verschillende „certificatiedienstverleners" in Europa onderlinge afspraken maken over de wederzijdse erkenning van hun certificaten. Anders blijft het nut van elektronische certificaten zeer beperkt en zullen deze minder vaak gebruikt worden dan wenselijk is. Verontrustend is dat regionale overheden met niet-interoperabele technologische oplossingen dienst doen als certificatiedienstverleners, wat de totstandbrenging van een samenhangend en goed gestructureerd Europa van de regio's er zeker niet gemakkelijker op maakt.

26. Het CvdR is ingenomen met de Europese initiatieven ter normalisering van elektronische handtekeningen (EESSI), het chipkaartinitiatief in het kader van eEurope en de initiatieven op het gebied van *public key infrastructure* (PKI).

27. Terecht wijst de Commissie erop dat de interoperabiliteit zal toenemen als de verschillende specificaties eenmaal op één lijn zijn gebracht. Dan zullen de marktdeelnemers er snel mee uit de voeten kunnen.

28. Het CvdR staat achter alle voorgestelde marktgerichte maatregelen om standaardiserings- en certificeringswerkzaamheden te ondersteunen en vindt dat er wetgeving moet komen voor de wederzijdse erkenning van certificaten.

29. Op gezette tijden zou moeten worden nagegaan hoe het staat met de technische en organisatorische maatregelen die *service providers* krachtens artikel 4 van de Richtlijn over de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de telecommunicatiesector moeten nemen om de veiligheid van hun diensten te waarborgen.

30. Het CvdR wijst de Commissie op de grote schade die terroristische groeperingen door middel van computercriminaliteit kunnen aanrichten, met als enige doel om bij wijze van politieke chantage zo veel mogelijk schade toe te brengen aan collectieve belangen.

31. Het CvdR staat achter alle voorgestelde wetgevingsmaatregelen en is van mening dat de nationale wetten op het gebied van computercriminaliteit op elkaar afgestemd en geharmoniseerd moeten worden. Anders bestaat het gevaar dat men vanuit bepaalde Europese landen min of meer ongestraft schadelijke activiteiten kan uitvoeren.

32. De bestaande in de bestrijding van computercriminaliteit gespecialiseerde nationale politie-eenheden moeten onderling gecoördineerd worden, en in landen waar dergelijke eenheden nog niet bestaan moeten ze opgericht worden. Verder dienen deze eenheden de beschikking te krijgen over voldoende arbeidskrachten en technische hulpmiddelen.

33. In alle lidstaten zouden ter bestrijding van de computercriminaliteit speciale openbare aanklagers moeten worden aangesteld die dankzij een gerichte en grondige opleiding hun functie met de vereiste efficiëntie kunnen uitoefenen. De onderlinge communicatie tussen en coördinatie van deze openbare aanklagers is van cruciaal belang. Verder dienen rechters en andere magistraten zo te worden opgeleid dat zij daden die de veiligheid van de netwerken en de gebruikers daarvan in gevaar kunnen brengen efficiënt kunnen berechten.

34. Het CvdR is het volledig met de Commissie eens dat de ontwikkeling van de elektronische overheid — waar veel lokale en regionale overheden op hebben ingezet om hun betrekkingen met de bevolking, hun dienstverlening en in het algemeen het welzijn en de democratische participatie van de bevolking te verbeteren — overheidsdiensten enerzijds tot potentiële modelvoorbeelden van doeltreffende veilige oplossingen maakt en anderzijds tot marktdeelnemers die de ontwikkelingen via hun aankoopbeleid richting kunnen geven. Wat dit betreft is het de taak van overheidsdiensten om, al naar gelang hun bevoegdheden, de ontwikkeling van de informatie- en kennismaatschappij voort te stuwen. Als de door deze overheidsdiensten gebruikte informatienetwerken en -systemen niet veilig zijn, zal de bevolking er geen vertrouwen in stellen. Dat zal de ontwikkeling van de nieuwe maatschappij ernstige schade toebrengen.

35. De in verband met overheidsdiensten voorgestelde maatregelen zouden gericht moeten zijn op de drie overheidsniveaus (lokaal, regionaal en nationaal) en de oplossingen dienen absoluut interoperabel te zijn.

36. De Commissie is terecht van plan een intensievere dialoog te gaan voeren met internationale organisaties en partners op het gebied van netwerkveiligheid, waarbij vooral de behoefte aan veiliger elektronische netwerken aan de orde moet komen. In dit verband zou zij moeten nagaan of het wellicht nodig is om over de veiligheid van informatienetwerken en -systemen een „wereldtop" te organiseren waaraan onder andere fabrikanten en exploitanten zouden moeten deelnemen. Daarnaast zou zij de oprichting van een Europees forum ter bestrijding van computercriminaliteit moeten overwegen. Ten slotte doen de lidstaten er goed aan om het onlangs door de Raad van Europa goedgekeurde internationale verdrag ter bestrijding van computercriminaliteit te ratificeren, zodat dit zo snel mogelijk in werking kan treden en de hierin opgenomen regelgeving kan worden toegepast.

Brussel, 15 november 2001.

De voorzitter

van het Comité van de Regio's

Jos CHABERT