Yttrande från Regionkommittén om ”Kommissionens meddelande till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén Nät- och informationssäkerhet: förslag till en europeisk strategi”

(2002/C 107/27)

BAKGRUND

Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén om nät- och informationssäkerhet: förslag till en europeisk strategi (KOM(2001) 298 slutlig).

Kommissionens beslut av den 7 juni 2001 att begära Regionkommitténs yttrande i frågan i enlighet med artikel 265 i EG-fördraget.

Beslutet av Regionkommitténs ordförande av den 2 juli 2001 att ge utskott 3 – transeuropeiska nät, transporter, informationssamhället – i uppdrag att utarbeta detta yttrande.

Beslut av Regionkommitténs ordförande av den 26 oktober 2001, om att utse Adela María Barrero Flórez till föredragande med uppdrag att förbereda ett yttrande i frågan, i enlighet med artikel 40.2 i Regionkommitténs arbetsordning.

Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén – Ett säkrare informationssamhälle – ökad säkerhet i informationsstrukturen och bekämpning av datorrelaterad brottslighet – (KOM(2000) 890 slutlig – CdR 88/2001 fin).

Meddelande från kommissionen till rådet, Europaparlamentet, Ekonomiska och sociala kommittén och Regionkommittén – Om säkerhet och pålitlighet vid elektronisk kommunikation – Mot en europeisk ram för digitala signaturer och kryptering (KOM(97) 503 slutlig).

Meddelande från kommissionen till rådet och Europaparlamentet – *e*Europe 2002: Påverkan och prioriteringar (KOM(2001) 140 slutlig).

Handlingsplanen *e*Europe 2002 (KOM(2000) 330 slutlig).

Europarådets förslag till konvention om datorbrottslighet (CM(2001) 103).

Rådets rekommendation om gemensamma kriterier för utvärdering av informations-teknologisk säkerhet ([1]).

Rådets rekommendation om kontaktpunkter som upprätthåller ett öppethållande dygnet runt för bekämpning av högteknologisk brottslighet ([2]).

Europaparlamentets och rådets förordning (EG) nr 45/2001 om skydd för enskilda då gemenskapsinstitutionerna och gemenskapsorganen behandlar personuppgifter och om den fria rörligheten för sådana uppgifter ([3]).

Rådets beslut 9194/01 om behöriga myndigheters praktiska behov när det gäller allmänt tillgängliga teletjänster och nät.

Ordförandeskapets slutsatser, Europeiska rådet i Stockholm, mars 2001.

Kommissionens direktiv 90/388/EEG om konkurrens på marknaderna för teletjänster.

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

Europaparlamentets och rådets direktiv 95/46/EG om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter.

Europaparlamentets och rådets direktiv 97/33/EG om samtrafik inom telekommunikation i syfte att säkerställa samhällsomfattande tjänster och samverkan genom tillämpning av principerna om tillhandahållande av öppna nät.

Europaparlamentets och rådets direktiv 97/66/EG om behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet.

Europaparlamentets och rådets direktiv 98/10/EG om tillhandahållande av öppna nätverk (ONP) för taltelefoni och samhällsomfattande tjänster för telekommunikation i en konkurrensutsatt miljö.

Europaparlamentets och rådets direktiv 1999/93/EG om ett gemenskapsramverk för elektroniska signaturer.

Europaparlamentets och rådets direktiv 2000/31/EG om vissa rättsliga aspekter på informationssamhällets tjänster, särskilt elektronisk handel, på den inre marknaden (”direktiv om elektronisk handel”).

Förslag till Europaparlamentets och rådets direktiv om behandling av personuppgifter och skydd för privatlivet inom sektorn för elektronisk kommunikation ([1]).

Det utkast till yttrande (CdR 257/2001 rév.) som utarbetats av föredraganden Adela María Barrero Florez, generaldirektör vid Asturiens regering, med ansvar för Europafrågor (E–PSE).

Utgångspunkter

Nät- och informationssystem har blivit en allt viktigare del av samhällets sociala och ekonomiska utveckling, och grundläggande infrastruktur, som energi och vägnät, som majoriteten av den offentliga förvaltningen samt företag är beroende av att den fungerar.

Nät- och informationssäkerhet har blivit en förutsättning för utvecklingen av nya tjänster, nya källor till ekonomisk välfärd, nyskapande handelsrelationer etc.

Det ökade antalet brott mot säkerheten har allvarligt skadat förtroendet hos informationsnätens användare.

Det bristande förtroendet för nät- och informationssystemen hindrar utbredningen av nya tjänster som rör informations- och kunskapssamhället.

Nät- och informationsäkerheten har blivit en viktig utmaning för politikerna, som måste inse omfattningen av problemet med att säkerheten står på spel, och förstå att de som politiker kan göra mycket för att få till stånd en förbättring.

Trots att man har vidtagit omfattande rättsliga åtgärder som en del av säkerhetsbestämmelserna i telekommunikations- och dataskyddslagstiftningen, både på nationell nivå och på EU-nivå, har man ännu inte vidtagit särskilda säkerhetsåtgärder på området.

Det återstår fortfarande många säkerhetsproblem att lösa när det gäller nät- och informationssystemen, och vissa lösningar har svårt att ta sig in på marknaden på grund av brister i marknadens funktion.

Myndigheterna spelar en viktig roll när det gäller att komma till rätta med bristerna i marknaderans funktion.

([1]) EGT C 365, 19.12.2000.

Politiska åtgärder för att komma till rätta med marknadens brister beträffande nät- och informationssäkerhet kan påverka marknaden och samtidigt göra lagstiftningen effektivare.

Sådana åtgärder måste utgöra en del av en europeisk strategi för att säkerställa utvecklingen av informations- och kunskapssamhället i EU, för att kunna dra nytta av gemensamma lösningar och för att gemenskapen skall kunna agera effektivt på det globala planet.

Problemets komplexitet kräver att man är medveten om såväl de politiska, ekonomiska, organisatoriska och tekniska aspekterna som de regionala och globala aspekterna.

Följderna av den bristande nät- och informationssäkerheten i unionens mindre utvecklade regioner kan öka den ”digitala klyfta” som redan existerar mellan dessa regioner och unionens mer välutvecklade och säkra regioner.

Lokala och regionala myndigheter spelar en viktig roll när det gäller att genomföra en europeisk strategi för nät- och informationssäkerhet, eftersom närheten till medborgare, företag och organisatoner gör att de effektivt kan genomföra beslutade åtgärder.

Med beaktande av ovanstående antog Regionkommittén enhälligt följande yttrande vid sin 41:a plenarsession den 14–15 november 2001 (sammanträdet den 15 november).

Inledning

1. ReK delar kommissionens oro när det gäller säkerheten i elektroniska nät och informationssystem, samt den kritik som problemet har väckt, inte bara beträffande utvecklingen av informations- och kunskapssamhället, utan även med tanke på följderna för dagens ekonomiska system på ett globalt plan.

2. Kommittén stöder meddelandet när det gäller den politiska prioritet som EU bör ge nät- och informationssäkerheten. Marknaden har ännu inte lyckats få fram en gemensam lösning, varför det förekommer olika tekniska lösningar och säkerhetsnormer men saknas en öppen och gemensam norm.

3. ReK stöder kommissionens uppfattning att man bör fastställa på vilka områden det krävs ytterligare eller utökade åtgärder från offentligt håll på Europanivå eller på det nationella planet för att kunna besluta om en gemensam strategi för nät- och informationssäkerhet.

4. Kommittén vill understryka vikten av att man i samband med de åtgärder som skall vidtas för att öka nät- och informationssäkerheten respekterar de friheter och medborgerliga rättigheter som nämns i FN:s allmänna förklaring om de mänskliga rättigheterna, i Internationella avtalet om medborgerliga och politiska rättigheter samt i Europeiska konventionen om de mänskliga rättigheterna. Kommittén menar därför att man bör upprätta tydliga gränser för befogenheter som omfattar situationer där de medborgerliga friheterna kan äventyras. Regionkommittén menar vidare att det är fullt möjligt att både respektera de medborgerliga friheterna och rättigheterna och öka säkerheten för nät- och informationssystemen.

5. Kommittén ställer sig tveksam till om denna strategi på gemenskapsnivå kan uppnå de fastställda säkerhetsmålen utan ett avtal med internationella organisationer och andra världsmakter, med tanke på att problemet är gränsöverskridande.

6. Med tanke på vikten av att man ombesörjer en nödvändig nät- och informationssäkerhet uppmanar ReK kommissionen att anslå tillräckliga ekonomiska resurser för att genomföra de beslutade åtgärderna.

Analys av frågor som rör nät- och informationssäkerhet

7. Enligt Regionkommittén är den definition av nät- och informationssäkerhet som ges i meddelandet, när man avser ”en viss tillförlitlighetsnivå”, alltför otydlig: ”förmågan hos ett nät eller ett informationssystem att tåla, vid en viss tillförlitlighetsnivå, olyckshändelser eller illvilligt uppträdande som äventyrar tillgängligheten, äktheten, integriteten och konfidentialiteten hos lagrade eller vidarebefordrade data och besläktade tjänster som tillhandahålls av eller är tillgängliga via dessa nät och system”. ReK menar att ingen form av illvilligt uppträdande eller intrång i ett nät eller informationssystem skall accepteras på någon som helst ”tillförlitlighetsnivå”.

8. ReK är oroad över att investering i nätsäkerhet inte prioriteras, eller är proportionerlig, bland majoriteten av de teleoperatörer och Internetleverantörer som verkar inom unionen. Ytterligare ett problem som bör tas med i beräkningen är förekomsten av mindre lokala operatörer, vars främsta mål är att skaffa sig en marknadsposition som kan ge ekonomisk utdelning, och som därför inte månar om säkerheten.

9. Enligt ReK:s uppfattning kommer förtroendet för krypteringsprodukter att växa framför allt genom inrättandet av öppna internationella regler och normer. Vidare menar kommittén att de icke sammanordnade initiativ som vissa medlemsstater har valt för att stödja programvara som bygger på öppen källkod för kryptering i stället för att stödja den privata sektorns starka marknadsinitiativ inte leder någon vart.

10. Kommittén håller med kommissionen om att konkurrensen mellan olika hårdvaru- och programvaruförsäljare inte leder till större investeringar i säkerhet, och föreslår därför att man skall undersöka åtgärder som gynnar sådana investeringar.

11. Vidare menar ReK att teleoperatörer och Internetleverantörer skall tvingas uppfylla en lägsta säkerhetsnivå, som skall fastställas på gemenskapsnivå.

En europeisk strategi

12. Kommittén menar att en välavvägd utveckling av informations- och kunskapssamhället inom Europeiska Unionen kommer att underlätta sammanhållningen och strukturering av unionens regioner, varför nät- och informationssäkerheten måste säkerställas.

13. Kommittén håller med kommissionen om att samtliga investeringar i nät- och informationssäkerhet kommer att få sociala fördelar, och vill poängtera den höga kostnad som avsaknaden av investeringar från operatörer, försäljare och tjänsteföretag för närvarande innebär för samhället och vår ekonomiska välfärd.

14. ReK uppmanar kommissionen att undersöka behovet av kriterier och normer som rör säkerhet, och som bör uppfyllas av samtliga grundläggande informationssystem (allmännyttiga tjänster) som är uppkopplade såväl till telenätet som till Internet.

15. Kommittén håller med om att säkerheten bör ökas utan att man för den skull äventyrar vare sig tillträdesmöjligheten eller dess kvalitet, vilka utgör grunden för informations- och kunskapssamhället. Samtidigt anser kommittén att det krävs en lägsta nivå för säkerhet även om det påverkar kvaliteten på tillträdet.

16. ReK instämmer i

— att det finns ett gemensamt behov av att förstå vilka säkerhetsfrågor som måste bearbetas ochvilka åtgärder som skall vidtas,

— att politiska åtgärder kan påverka marknaden och samtidigt göra lagstiftningen effektivare,

— att en europeisk strategi är oundgänglig för att den inre marknaden för kommunikations- och informationstjänster skall kunna fungera, för att man skall kunna dra nytta av gemensamma lösningar och för att gemenskapen skall kunna agera effektivt på det globala planet.

17. ReK stöder förslaget om att upplysningskampanjerna bör kompletteras med stödkampanjer för investeringar i säkerhet, med målet att genomförandet av nödvändiga åtgärder inte skall hindras av ekonomiska skäl.

18. ReK vill understryka vikten av att lokala och regionala myndigheter av praktiska skäl ges en viktig roll i den upplysningskampanj som utformas på området.

19. Kommittén delar kommissionens uppfattning att man snarast bör stärka CERT-systemet i Europeiska unionen och förse existerande CERT-grupper med tillräckligt med personal samt tekniska och ekonomiska resurser.

20. Kommittén föreslår att de europeiska CERT-grupperna skall ha tätare, mer direkt och mer flexibla relationer till de slutliga stödmottagarna.

21. ReK ställer sig positiv till de åtgärder som föreslås i meddelandet beträffande ett europeiskt varnings- och informationssystem, samt antagandet av förutseende åtgärder som inrättandet av en europeisk byrå för nät- och informationssäkerhet, som bl.a. skall ha till uppgift att analysera och testa mjukvara (operativsystem, webbläsare, e-postsystem etc.) och som skall användas i de allmänna informationsnäten i syfte att upptäcka ”säkerhetsbrister” i mjukvara som ännu inte finns på den europeiska marknaden. Regionkommittén menar att det planerade Institutet för medborgarnas skydd och säkerhet (IPSC) som skall underordnas Gemensamma forskningscentret (GFC), till sin uppbyggnad och sina befogenheter inte överensstämmer med den byrå som tidigare föreslagits.

22. Regionkommittén befarar att all forskning rörande nät- och informationssäkerhet som finansieras genom ramprogrammen för forskning och utveckling i EU, men som inte får stöd från de främsta programvarutillverkarna, inte kommer att uppnå önskade resultat. Kommittén föreslår därför att man skall göra ett försök att förmå världens främsta programvarutillverkare att ingå ett avtal om forskning i nät- och informationssäkerhet, och om hur det omgående skall genomföras i praktiken.

23. ReK ser med oro på att operatörernas olika lösningar inte är kompatibla, samt att det inte finns något intresse av att utarbeta öppna gemensamma normer.

24. Kommittén rekommenderar att man inte skall öka bruket av vissa lösningar eller krypteringsprodukter utan i stället kämpa för att samtliga lösningar skall överensstämma med en gemensam öppen norm som godkänns av samtliga producenter.

25. ReK anser att det måste upprättas avtal mellan olika europeiska tillhandahållare av certifikattjänster när det gäller ett ömsesidigt erkännande av certifikat. Utan ett sådant avtal begränsas de elektroniska certifikatens användbarhet, och följaktligen kommer deras användbarhet att bli lägre än förväntat. Det är oroande att regionala myndigheter skall tillhandahålla certifikattjänster till tekniska lösningar som inte är kompatibla, vilket även undergräver ett sammanhängande och strukturerat regionernas Europa.

26. ReK ställer sig positiv till de europeiska initiativen om att inrätta gemensamma normer för elektroniska signaturer när det gäller åtgärderna i *e*Europa om smarta kort och om Public Key Infrastructure-initiativet (PKI).

27. Kommittén håller med om att harmoniserade specifikationer kommer att öka kompatibiliteten och göra det lättare för aktörerna att snabbt börja tillämpa specifikationerna.

28. Kommittén ställer sig positiv till samtliga föreslagna åtgärder om stöd för marknadsorienterad standardisering och certifiering, och menar att det är nödvändigt att ta itu med de rättsliga aspekterna på ömsesidigt erkännande av certifikat.

29. Vidare menar kommittén att man med jämna mellanrum bör kontrollera i vilken utsträckning teleoperatörerna genomför de tekniska och organisatoriska åtgärder som de bör vidta för att deras tjänster skall uppfylla säkerhetskraven, i enlighet med artikel 4 i direktivet för behandling av personuppgifter och skydd för privatlivet inom telekommunikationsområdet.

30. ReK vill uppmärksamma kommissionen på de allvarliga följderna av terroristgruppers datorrelaterade brottslighet, där det enda målet är att, i form av politisk utpressning, tillföra kollektiva intressen så allvarliga skador som möjligt.

31. Kommittén ger sitt stöd till samtliga föreslagna lagstiftningåtgärder och menar att medlemsstaternas lagstiftning som rör datorrelaterad brottslighet måste harmoniseras och närma sig varandra, för att på så sätt undvika att det finns medlemsstater inom unionen varifrån man kan agera ostraffat eller med lägre straff.

32. Vidare föreslår kommittén att man på nationell nivå skall gynna inrättandet av polisenheter som är specialiserade på datorrelaterad brottslighet, samt att man i de länder där sådana enheter redan finns skall samordna deras verksamhet med andra enheter. Kommittén anser även att enheterna måste få tillräckligt med personal och tekniska resurser.

33. Kommittén anser att man i samtliga medlemsstater bör utnämna särskilda åklagare med ansvar för datorrelaterad brottslighet som besitter omfattande specialkunskaper och har möjlighet att väcka offentligt åtal i den utsträckning som krävs. Man bör lägga särskilt stor vikt vid såväl kontakterna och samarbetet mellan dessa åklagare som vid utbildning av domare på området, i syfte att så effektivt som möjligt få bukt med de gärningar som kan äventyra säkerheten för nätet och dess användare.

34. Kommittén stöder helt och hållet kommissionens åsikt att myndigheternas allt större utbud av elektroniska tjänster gör dem mycket lämpliga för att visa upp goda säkerhetslösningar. Många regionala och lokala myndigheter har satsat på just elektroniska tjänster för att förbättra dels kontakten med medborgarna, dels kvaliteten på sitt utbud av tjänster, men på det hela taget också för att göra det enklare för medborgarna och öka deras demokratiska deltagande. De är också marknadsaktörer som kan påverka utvecklingen via sina upphandlingar. Av den anledningen bör myndigheterna, i enlighet med sina befogenheter, fungera som drivkraft när det gäller utvecklingen av informations- och kunskapssamhället. Om inte de områden som används av myndigheterna uppvisar en fungerande nät- och informationssäkerhet kommer de inte att få medborgarnas förtroende, vilket i sin tur kommer att få allvarliga följder för utvecklingen av det nya samhället.

35. Kommittén föreslår att åtgärder som berör myndigheter skall rikta sig till samtliga tre plan inom administrationen (lokal, regional och statlig nivå), och att de lösningar som tillämpas måste vara kompatibla.

36. Slutligen ger kommittén sitt fulla stöd för ett ökat samarbete med internationella organisationer och partner när det gäller nätsäkerhet, och framför allt de elektroniska nätens driftssäkerhet. Vidare uppmanar ReK kommissionen att överväga dels tanken på ett internationellt toppmöte om nät- och informationssäkerhet där producenter och operatörer deltar, dels att skapa ett europeiskt forum för att bekämpa datorrelaterad brottslighet. Kommittén vill samtidigt uppmana samtliga medlemsstater att ratificera det internationella avtal om datorrelaterad brottslighet som nyligen antagits av Europarådet för att det snarast möjligt skall kunna träda i kraft och de regleringsinstrument som tas upp i avtalet skall kunna tillämpas.

Bryssel den 15 november 2001.

Regionkommitténs

ordförande

Jos CHABERT