Dictamen del Comité de las Regiones sobre la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — Seguridad de las redes y de la información: Propuesta para un enfoque político europeo»

(2002/C 107/27)

EL COMITÉ DE LAS REGIONES,

vista la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — Seguridad de las redes y de la información: Propuesta para un enfoque político europeo» (COM(2001) 298 final);

vista la Decisión de la Comisión del 7 de junio de 2001 de consultarle al Comité a ese respecto de conformidad con el primer párrafo del artículo 265 del Tratado constitutivo de la Comunidad Europea;

vista la Decisión de su Presidente del 2 de julio de 2001 de encomendar la elaboración del correspondiente dictamen a la Comisión de Redes Transeuropeas, Transportes y Sociedad de la Información (Comisión 3);

vista la decisión de su Presidente de 26 de octubre de 2001 de nombrar a la Sra. Barrero Flórez ponente general encargada de elaborar un dictamen sobre este asunto, de conformidad con el artículo 40.2 del Reglamento Interno del Comité de las Regiones;

visto su Dictamen sobre la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — Creación de una sociedad de la información más segura mediante la mejora de la seguridad de las infraestructuras de información y la lucha contra los delitos informáticos — eEurope 2002» (COM(2000) 890 final — CDR 88/2001 fin);

vista la «Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social y al Comité de las Regiones — El fomento de la seguridad y la confianza en la comunicación electrónica — Hacia un marco europeo para la firma digital y el cifrado» (COM(1997) 503 final);

vista la «Comunicación de la Comisión al Consejo y al Parlamento Europeo — eEurope 2002: Impacto y prioridades» (COM(2001) 140 final);

visto el Plan de acción eEurope 2002 (COM(2000)330 final);

visto el proyecto de convenio sobre el ciberdelito del Consejo de Europa (COM(2001) 103);

vista la Recomendación del Consejo relativa a los criterios comunes de evaluación de la seguridad en las tecnologías de la información ([1]);

vista la Recomendación del Consejo sobre puntos de contacto accesibles de manera ininterrumpida para la lucha contra la delincuencia de alta tecnología ([2]);

visto el Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos ([3]);

vista la Resolución nº 9194/01 del Consejo de 20 de junio de 2001 sobre las necesidades operativas de las autoridades competentes sobre las redes y servicios públicos de telecomunicaciones;

vistas las conclusiones de la Presidencia del Consejo Europeo de Estocolmo de marzo de 2001;

vista la Directiva 90/388/CE relativa a la competencia en los mercados de servicios de telecomunicaciones;

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

vista la Directiva 95/46/CE relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos;

vista la Directiva 97/33/CE relativa a la interconexión en las telecomunicaciones en lo que respecta a garantizar el servicio universal y la interoperabilidad mediante la aplicación de los principios de la oferta de red abierta (ONP);

vista la Directiva 97/66/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones;

vista la Directiva 98/10/CE sobre la aplicación de la oferta de red abierta (ONP) a la telefonía vocal y sobre el servicio universal de telecomunicaciones en un entorno competitivo;

vista la Directiva 1999/93/CE por la que se establece un marco comunitario para la firma electrónica;

vista la Directiva 2000/31/CE relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico);

vista la Propuesta de Directiva del Parlamento Europeo y del Consejo relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas ([1]);

visto el proyecto de dictamen (CDR 257/2001 rev.), elaborado por la ponente general, Sra. Barrero Flórez (E/PSE); Directora General de Asuntos Europeos, Principado de Asturias;

considerando que las redes y los sistemas de información se han convertido en un factor esencial del desarrollo social y económico de la sociedad actual y que su adecuado funcionamiento es fundamental para infraestructuras vitales como la energética y la viaria entre otras, así como para la gran mayoría de los servicios públicos y privados y la economía en su conjunto;

considerando que la seguridad de las redes y los sistemas de información se está convirtiendo en un requisito previo para futuros progresos en nuevos servicios, en nuevas fuentes de riqueza económica, en innovadoras relaciones comerciales, etc.;

considerando el grave perjuicio que está produciendo en la confianza de los usuarios de las redes de información el creciente número de violaciones de la seguridad de éstas;

considerando que la falta de confianza en las redes y los sistemas de información produce una ralentización en la extensión generalizada de los nuevos servicios relacionados con la Sociedad de la Información y el Conocimiento;

considerando que la seguridad de estas redes y sistemas se ha convertido en un desafío clave para los responsables políticos que necesitan darse cuenta de su importancia, comprender sus aspectos, los problemas de seguridad en juego y la función que pueden desempeñar en su mejora;

considerando que, aunque se ha adoptado un importante conjunto de medidas legislativas como parte del marco de las telecomunicaciones y de las leyes de protección de los datos personales tanto a nivel nacional como de la UE, aún no se han adoptado medidas específicas en el tema de la seguridad;

considerando que muchos son los problemas que siguen sin resolverse en cuanto a la seguridad de las redes y sistemas de información y algunas soluciones tardan en llegar al mercado debido a las imperfecciones de éste;

considerando que las Administraciones públicas tienen una función que desempeñar en la subsanación de carencias o deficiencias de los mercados;

([1]) DO C 365 de 19.12.2000.

considerando que medidas políticas específicas dirigidas a paliar las deficiencias del mercado en cuanto a seguridad de las redes y los sistemas de información podrían reforzar la dinámica del mismo y mejorar el funcionamiento del marco legal;

considerando que tales medidas deberían formar parte de un enfoque europeo de cara a asegurar el desarrollo de la Sociedad de la Información y el Conocimiento en la UE, sacar ventaja de las soluciones comunes y poder actuar de forma eficaz a nivel mundial;

considerando que la complejidad del problema requiere tener en cuenta sus aspectos políticos, económicos, organizativos y técnicos así como su carácter descentralizado y global;

considerando que los efectos de la falta de seguridad en las redes y sistemas de información de regiones europeas menos desarrolladas puede aumentar la fractura digital actualmente existente entre estas regiones y las más desarrolladas y seguras;

considerando que las autoridades regionales y locales pueden y deben jugar un papel esencial en la puesta en práctica de una política europea de seguridad de las redes y los sistemas de información, dado que la proximidad a los ciudadanos, organizaciones y empresas ofrece la necesaria eficacia e idoneidad en la aplicación de las medidas concretas que se decidan,

en su 41º Pleno celebrado los días 14 y 15 de noviembre de 2001 (sesión del 15 de noviembre) ha aprobado por unanimidad el presente Dictamen.

Introducción

El Comité de las Regiones

1. comparte con la Comisión la creciente preocupación que suscita la seguridad de las redes y los sistemas de información y la importancia crítica que ha cobrado, no solo para el desarrollo de la Sociedad de la Información y el Conocimiento, sino también para el actual sistema económico a escala mundial;

2. coincide con la Comunicación en la prioridad política que debe dar la Unión Europea a la seguridad de las redes y los sistemas de información. El mercado no ha sido capaz de dar una respuesta única, por lo que existen muchas tecnologías y estándares de seguridad, pero carece de una norma abierta y común aceptada;

3. está de acuerdo con el objetivo de la Comunicación de determinar en que ámbitos es necesario introducir o reforzar la actuación pública a nivel europeo o nacional con el fin de decidir una política comunitaria sobre seguridad de las redes y los sistemas de información;

4. se muestra preocupado por el respeto a las libertades y derechos civiles reconocidos en la Declaración Universal de Derechos Humanos, en el Pacto Internacional de Derechos Civiles y Políticos y en la Convención Europea de los Derechos Humanos en relación con las medidas a adoptar para aumentar la seguridad de las redes y los sistemas de información. En este sentido, solicita el establecimiento de límites claros para aquellos poderes y capacidades que impliquen situaciones en las que las libertades civiles estén comprometidas. El Comité de las Regiones considera posible el equilibrio entre el respeto a las libertades y derechos civiles y la seguridad de las redes y sistemas de información;

5. cuestiona que esta política concertada a nivel comunitario logre los objetivos de seguridad perseguidos sin el acuerdo con las organizaciones internacionales y con otras potencias mundiales dado el carácter transfronterizo de la problemática;

6. insta a la Comisión a que, de acuerdo con la importancia y la urgencia de proveer de la necesaria seguridad a las redes y a los sistemas de información, agilice y dote de suficientes recursos económicos la puesta en práctica de las medidas concretas que se aprueben.

Análisis de los problemas de seguridad de las redes y de la información

El Comité de las Regiones

7. considera poco clara la definición que de seguridad de las redes y de la información se ofrece en la Comunicación, como «la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionadas que pongan en peligro la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles» cuando se refiere a «un determinado nivel de confianza». El Comité de las Regiones considera que ninguna acción malintencionada o intrusión en una red o sistema de información debe ser aceptada, en absoluto, con ningún «nivel de confianza»;

8. considera muy preocupante que la inversión en seguridad no sea prioritaria, ni proporcional, para la generalidad de los operadores de servicios de telecomunicaciones y proveedores de servicios de acceso que operan en Europa. La existencia además de pequeños operadores regionales cuya prioridad es alcanzar una posición en el mercado que les permita obtener resultados económicos positivos y que les hace descuidar la seguridad añade una dificultad y un factor a tener en consideración;

9. cree que la confianza en los productos de encripción vendrá, en gran medida, de la existencia de estándares y normas internacionales abiertas y estima infructuosas las iniciativas descoordinadas de algunos Estados miembros para apoyar soportes lógicos de fuente abierta para encripción frente a la fuerte e imparable iniciativa de negocio del sector privado;

10. coincide con la Comunicación en que la competencia entre los proveedores de soportes y programas informáticos no se está traduciendo en mayores inversiones en materia de seguridad, por lo que propone el estudio de medidas que favorezcan estas inversiones;

11. considera necesaria la obligatoriedad por parte de los operadores de servicios de telecomunicaciones y proveedores de servicios de acceso de cumplir con unos mínimos de seguridad que han de ser fijados a nivel comunitario.

Un enfoque político europeo

El Comité de las Regiones

12. considera que el desarrollo equilibrado de la Sociedad de la Información y el Conocimiento en la Unión Europea facilitará la cohesión y vertebración de la Europa de las regiones, para lo que es indispensable garantizar la seguridad de las redes y los sistemas de información;

13. coincide con la Comunicación de la Comisión en los beneficios sociales que se generan con toda inversión en la mejora de la seguridad de las redes y los sistemas de información y desea poner de relieve el elevado coste social que la falta de dicha inversión por parte de fabricantes, operadores y proveedores de servicios representa para la sociedad y su bienestar;

14. insta a la Comisión a estudiar la necesidad de establecer unos criterios y normas de seguridad que deban cumplir obligatoriamente todos los sistemas de información considerados básicos (servicios de interés público) que estén conectados a las redes de telecomunicaciones así como las propias redes;

15. es partidario de maximizar la seguridad sin comprometer la facilidad y la calidad del acceso en el que se basa la Sociedad de la Información y el Conocimiento, pero considera indispensable mantener unos niveles mínimos de seguridad aún cuando se penalice la calidad del acceso;

16. coincide con la Comunicación de la Comisión en:

— la necesidad común de comprender los problemas de seguridad latentes y de las medidas específicas a adoptar;

— que las medidas políticas pueden reforzar el proceso del mercado y mejorar al mismo tiempo el funcionamiento del marco legal;

— que es necesario un enfoque europeo para garantizar un mercado único para los servicios de comunicación y de información, el aprovechamiento de las soluciones comunes y la capacidad para actuar de forma eficaz a nivel mundial;

17. es partidario de complementar las acciones de concienciación propuestas en la Comunicación con acciones de apoyo o ayuda a la inversión en medidas de seguridad con el objetivo de que el coste económico no retraiga la adopción de tales medidas que han sido reconocidas como necesarias;

18. resalta la importancia de que, por razones operativas y prácticas, las administraciones regionales y locales tengan un papel relevante en toda campaña de concienciación que en este campo se desarrolle;

19. comparte con la Comunicación la necesidad de fortalecer, urgentemente, el sistema CERT en la Unión Europea y de dotar a los centros existentes de recursos humanos, técnicos y económicos suficientes;

20. recomienda una mayor, directa y ágil relación de los CERT europeos con los potenciales beneficiarios finales;

21. aprueba las acciones propuestas en la Comunicación relativas a un sistema europeo de alarma y de información proponiendo, al mismo tiempo, la adopción de una medida proactiva como es la creación de una Agencia Europea de Seguridad de las Redes y los Sistemas de Información que tenga como función, entre otras, el análisis y testeo de todo software (sistemas operativos, navegadores, gestores de correo electrónico, etc.) que vaya a ser utilizado en redes de información públicas con el objetivo de detectar «agujeros» de seguridad en software que aún no se comercializa en la Unión Europea. El Comité de las Regiones considera que el futuro Instituto de Protección y Seguridad de los Ciudadanos (IPSC) dependiente del Centro Común de Investigación (CCI) no equivale, en su naturaleza y funciones, a la Agencia propuesta;

22. teme que toda investigación sobre seguridad de las redes y de la información financiada por los programas marco de Investigación y Desarrollo de la UE que no sea apoyada por los principales fabricantes de software del mercado no obtenga el resultado práctico deseado. El Comité de las Regiones propone que, independientemente, se realice un esfuerzo por obtener de los principales fabricantes mundiales de software un mayor compromiso con la investigación en seguridad de las redes y de la información y con su aplicación práctica inmediata;

23. manifiesta su preocupación por la actual inexistencia de interoperabilidad entre las distintas soluciones tecnológicas de los fabricantes y por su desinterés por elaborar normas comunes abiertas;

24. recomienda no fomentar el uso de determinadas soluciones o productos de encripción cuando lo que se debe perseguir es que todas las soluciones coincidan en una norma común abierta y aceptada por todos los fabricantes;

25. considera fundamental el establecimiento de acuerdos entre los distintos proveedores de servicios de certificación europeos sobre el mutuo reconocimiento de sus certificados. Sin este acuerdo la utilidad de los certificados electrónicos será muy limitada y, por lo tanto, su utilización alcanzará niveles más bajos de los deseados. Es motivo de preocupación la constitución como proveedores de servicios de certificación de autoridades regionales con soluciones tecnológicas no interoperables lo que complica, sin duda alguna, el objetivo de una Europa de las regiones cohesionada y vertebrada;

26. acoge muy favorablemente las iniciativas europeas para la normalización de firmas electrónicas (EESSI), sobre tarjetas inteligentes del programa *e*Europa y de infraestructura de clave pública (PKI);

27. está de acuerdo en que la armonización de especificaciones favorecerá una mayor interoperabilidad y permitirá la rápida ejecución por parte de los agentes del mercado;

28. se muestra conforme con todas las acciones propuestas de apoyo a la normalización y certificación orientadas al mercado y considera necesaria la adopción de una iniciativa legal sobre el reconocimiento mutuo de los certificados;

29. estima oportuno comprobar periódicamente el grado de cumplimiento por parte de los operadores de servicios de telecomunicaciones en cuanto a las medidas técnicas y organizativas que deben adoptar para salvaguardar la seguridad de sus servicios según lo dispuesto en el artículo 4 de la Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones;

30. desea llamar la atención de la Comisión sobre la gravedad de las consecuencias que puede ocasionar la ciberdelincuencia cometida por grupos terroristas y que no persigue otro objetivo que el máximo daño contra intereses colectivos como forma de chantaje político;

31. se muestra conforme con todas las acciones propuestas en el marco legal y estima necesario aproximar y armonizar las leyes nacionales sobre la ciberdelincuencia para evitar la existencia de Estados europeos desde los que se pueda actuar impunemente o con menores sanciones;

32. propone que se fomente la creación a escala nacional de unidades policiales especializadas en ciberdelincuencia, donde no existan ya, y la coordinación de todas las existentes. Asimismo, considera necesario que se les dote de recursos humanos y técnicos suficientes;

33. aconseja el nombramiento, en todos los países miembros, de fiscales especiales contra el ciberdelito con una amplia formación específica que les permita ejercer la acusación pública con la eficacia debida. La comunicación y coordinación entre estos fiscales especiales deben ser consideradas fundamentales, así como la formación de jueces y magistrados en estos ámbitos con el fin de llevar a cabo una efectiva persecución de los actos que puedan poner en peligro la seguridad de las redes y de quienes accedan a ellas;

34. está completamente de acuerdo con la Comunicación de la Comisión Europea en que el desarrollo de la administración electrónica, por la que muchos entes regionales y locales han apostado con el fin de mejorar sus relaciones con los ciudadanos, la calidad de los servicios que prestan y, en conjunto, su bienestar y su participación democrática, hace de las administraciones públicas ejemplos potenciales de soluciones en materia de seguridad y agentes del mercado con la posibilidad de influir en la oferta a través de sus decisiones de contratación pública. En este sentido, las administraciones públicas tienen el deber de ejercer de motor de empuje en el desarrollo de la Sociedad de la Información y el Conocimiento de acuerdo a sus competencias. Sin seguridad en las redes y los sistemas de información que utilizan las administraciones no habrá confianza por parte de los ciudadanos y el daño que se estará produciendo en el desarrollo de la nueva sociedad será elevado;

35. propone que las acciones relacionadas con las administraciones públicas tengan como destinatarios los tres niveles de la Administración (local, regional y estatal) y que la interoperabilidad de las soluciones aplicadas sea un objetivo irrenunciable;

36. apoya firmemente el reforzamiento del diálogo con las organizaciones internacionales y socios en materia de seguridad de las redes, y en particular sobre el aumento de la seguridad de funcionamiento en las redes electrónicas e insta a la Comisión a valorar la celebración de una cumbre mundial sobre la seguridad de las redes y los sistemas de información con la participación de fabricantes y operadores, así como la creación de un foro europeo para combatir los delitos informáticos. Asimismo, invita a los Estados miembros a ratificar el recientemente aprobado Convenio Internacional sobre la Cibercriminalidad del Consejo de Europa con el fin de que pueda entrar en vigor lo más rápidamente posible y puedan ponerse en marcha los instrumentos normativos que en él se recogen.

Bruselas, 15 de noviembre de 2001.

El Presidente

del Comité de las Regiones

Jos CHABERT