Aviz al Comitetului Economic și Social European privind Comunicarea Comisiei adresată Consiliului, Parlamentului European, Comitetului Economic și Social European și Comitetului Regiunilor — O strategie pentru o societate informațională sigură — Dialog, parteneriat și responsabilizare

COM(2006) 251 final

(2007/C 97/09)

La 31 mai 2006, Comisia Europeană, în conformitate cu articolul 262 din Tratatul de instituire a Comunității Europene, a hotărât să consulte Comitetul Economic și Social European cu privire la propunerea sus-menționată.

Secțiunea pentru transporturi, energie, infrastructură și societatea informațională însărcinată cu pregătirea lucrărilor Comitetului pe această temă, și-a adoptat avizul la 11 ianuarie 2007. Raportor: dl PEZZINI.

La cea de-a 433-a sesiune plenară din 16 februarie 2007, Comitetul Economic și Social European a adoptat prezentul aviz cu 132 voturi pentru și 2 abțineri.

1. **Concluzii și recomandări**

1.1 Comitetul este convins că problema securității informatice reprezintă una din preocupările crescânde pentru întreprinderi, administrații, organismele publice și private și utilizatorii individuali.

1.2 În general, Comitetul aprobă analizele și argumentele invocate pentru punerea în aplicare a unei noi strategii care să ducă la creșterea securității rețelelor și a informației împotriva atacurilor și intruziunilor pentru care nu există limite geografice.

1.3 Comitetul consideră că Comisia ar trebui să facă mai multe eforturi pentru aplicarea unei strategii inovatoare și structurate, date fiind amploarea fenomenului și efectele sale în domeniul economic și asupra vieții private.

1.3.1 Comitetul atrage atenția și asupra faptului că, recent, Comisia a adoptat o nouă comunicare privind securitatea informatică și că, în curând, va apărea un alt document pe această temă. Comitetul își rezervă dreptul de a emite ulterior un aviz mai detaliat care va lua în considerare toate aceste comunicări.

1.4 Comitetul insistă asupra faptului că securitatea informatică nu poate în nici un caz să fie disociată de necesitatea de a îmbunătăți protecția datelor personale și a libertăților garantate prin Convenția europeană a drepturilor omului.

1.5 CESE se întreabă care este, la ora actuală, valoarea adăugată a acestei propuneri în raport cu cea adoptată în 2001, al cărei scop era același cu cel menționat în această comunicare ([1]).

1.5.1 Raportul de analiză de impact (*Impact Assessment*) ([2]) anexat la această propunere conține câteva actualizări interesante față de poziția din 2001, dar cum a fost publicat într-o singură limbă, este inaccesibil multor cetățeni europeni care își formulează o părere personală pe baza documentului oficial publicat în toate limbile comunitare.

1.6 Comitetul reamintește concluziile summit-ului mondial de la Tunis din 2005 privind societatea informațională, ratificate de Adunarea ONU din 27 martie 2006, care propuneau:

— principii de acces nediscriminatoriu;

— promovarea TIC (tehnologia informației și comunicației) utilizate în scopuri pașnice;

— definirea instrumentelor destinate consolidării democrației, coeziunii și bunei guvernanțe;

— prevenirea abuzurilor și respectarea drepturilor omului ([3]).

1.7 Comitetul subliniază că o strategie comunitară dinamică și integrată ar trebui să prevadă, pe lângă dialog, parteneriat și responsabilizare prin:

— acțiuni de prevenire;

— trecerea de la securitatea informatică la asigurarea informatică ([4]);

— crearea unui cadru comunitar sigur și recunoscut la nivel juridic, de reglementare și de aplicare de sancțiuni;

— consolidarea standardizării tehnice;

([1]) Cf. Avizului CESE privind „Comunicarea Comisiei adresată Consiliului, Parlamentului, Comitetul Economic și Social European și Comitetului Regiunilor — Securitatea rețelelor și a informației: propunere pentru o abordare strategică europeană", JO C 48 din 21.2.2002, p. 33.

([2]) Un „raport de impact" nu are aceeași semnificație ca un „document de strategie".

([3]) ONU 27.3.2006. Recomandările nr. 57 și 58. Documentul final de la Tunis nr. 15.

([4]) „Noile tehnologii în contextul securității", CCR — Institutul pentru protecția și securitatea cetățeanului, caiet de cercetare strategică, septembrie 2005, Comisia Europeană, http://serac.jrc.it

— identificarea digitală a utilizatorilor;

— lansarea de exerciții europene de analiză și de prospectivă (*Foresight*) cu privire la securitatea informatică într-un context de convergență a tehnologiilor multimodale;

— dezvoltarea mecanismelor europene și naționale de evaluare a riscurilor;

— măsuri pentru evitarea apariției de monoculturi informatice;

— îmbunătățirea coordonării comunitare la nivel european și internațional;

— crearea pentru mai multe direcții generale a unui punct comun „Securitatea TIC" („ICT Security Focal Point");

— crearea unei rețele europene pentru securitatea rețelelor și a informației („European Network and Information Security Network");

— optimizarea rolului cercetării europene în domeniul securității informatice;

— lansarea unei „Zile europene a securității informatice";

— acțiuni-pilot comunitare despre securitatea informatică, organizate în școli de tipuri și niveluri diferite.

1.8 Comitetul estimează că, pentru a pune în aplicare o strategie comunitară dinamică și integrată, este necesar să se prevadă bugete adecvate, însoțite de inițiative și de măsuri pentru întărirea coordonării la nivel comunitar, astfel încât Europa să se poată exprima cu o singură voce în contextul mondial.

2. **Expunere de motive**

2.1 Securitatea societății informaționale este un aspect fundamental în ce privește încrederea în rețelele și serviciile de comunicații și fiabilitatea acestora, factori esențiali pentru dezvoltarea economiei și a societății.

2.2 Rețelele și sistemele informatice trebuie protejate, dacă se dorește menținerea capacităților competitive și comerciale, garantarea integrității și continuității comunicațiilor electronice, prevenirea fraudelor și asigurarea protecției legale a vieții private.

2.3 Comunicațiile electronice și serviciile legate de acestea reprezintă segmentul cel mai important din întreg sectorul telecomunicațiilor: în 2004, aproximativ 90 % din întreprinderile europene au utilizat activ Internetul, 65 % din acestea și-au creat propriul site Internet, în timp ce, conform estimărilor, aproximativ jumătate din populația europeană utilizează periodic Internetul, iar 25 % dintre familii utilizează în permanență conexiunea de tip broadband ([5]).

2.4 Deși există o dezvoltare accelerată a investițiilor, volumul cheltuielilor destinate securității nu reprezintă decât între 5 și 13 % din totalul investițiilor în informație. Aceste procentaje sunt prea mici. Studii recente au arătat că „în medie, din 30 de protocoale care folosesc în comun aceleași structuri-cheie, 23 sunt vulnerabile la atacuri de tip multi-protocol" ([6]) în timp ce se apreciază că zilnic se transmit în medie 25 milioane de mesaje electronice *spam* ([7]): Comitetul apreciază deci propunerea prezentată recent de Comisie pe această temă.

2.5 În domeniul virușilor informatici ([8]) evoluția rapidă pe scară largă a „viermilor informatici" ([9]) și a programelor-spion (*spyware*) ([10]) a avut loc în paralel cu dezvoltarea crescândă a sistemelor și a rețelelor de comunicație electronică. Acestea au devenit din ce în ce mai complexe și, în același timp, din ce în ce mai vulnerabile, în special din cauza convergenței dintre multimedia, telefonia mobilă și sistemele *GRID infoware* ([11]): cazurile de extorsiune, de DdoS (*Distributed denials of service*, adică o întrerupere a serviciului cu origine din mai multe surse), furtul de identitate în linie, de *phishing* ([12]), de *piraterie* ([13]) și așa mai departe, reprezintă tot atâtea provocări lansate securității societății informaționale. Această temă a fost abordată de Comunitatea Europeană într-o Comunicare din 2001 ([14]) despre care Comitetul și-a exprimat deja poziția într-un aviz ([15]). În acea Comunicare Comisia propunea o strategie bazată pe trei tipuri de intervenții:

— măsuri specifice de securitate;

([5]) *i2010: O strategie pentru o societate informațională sigură* — DG Societatea informațională și mass-media, „Fișa de informare 8" (iunie 2006), http://ec.europa.eu/information_society/doc/factsheets/001-dg-glance-it.pdf

([6]) Lucrările primei Conferințe internaționale asupra disponibilității, fiabilității și securității (ARES'06) — Volumul 00 ARES 2006 Editore: IEEE Computer Society.

([7]) Spam = mesaje nedorite în mesageria electronică cu caracter comercial. La origine, spam înseamnă „spiced pork and ham" (carne de porc și șuncă condimentată), carne în conserve foarte populară în timpul celui de-al doilea război mondial, când a devenit principala sursă de alimentație atât pentru trupele americane, cât și pentru populația engleză. După ani de zile de asemenea regim termenul a dobândit un semnificat negativ.

([8]) Virus informatic: un tip special de software care aparține categoriei malware (programe răuvoitoare) și care, odată activat, poate să infecteze fișiere pentru a se reproduce prin duplicare, de obicei fără a fi detectat de către utilizator. Viruşii pot să fie mai mult sau mai puțin nocivi pentru sistemul de operare gazdă, dar chiar şi, în cel mai bun caz, provoacă o risipă de resurse RAM, CPU şi de spațiu pe discul dur (www.wikipedia.org/wiki/Virus_informatico).

([9]) Vierme (Worm)= software răuvoitor capabil să se reproducă: un „e-mail worm" este un atac perturbator contra unei rețele care culege toate adresele electronice conținute într-un program local (de exemplu, MS Outlook), pentru a trimite după aceea sute de emailuri la aceste adrese care conțin programul virus de tipul „vierme" ca anexă invizibilă.

([10]) Programe-spion = programe care înregistrează navigarea pe Internet a utilizatorului şi care se auto-instalează fără ca utilizatorul să fie informat sau conştient de aceasta, fără aprobarea sau controlul său.

([11]) *GRID infoware* = permite utilizarea în comun, selectarea şi regruparea unei largi game de resurse de elaborare electronică delocalizate (de tipul supercalculatoare, „computer clusters", sisteme de stocare date, surse de date, instrumente, resurse umane), pe care le prezintă ca o sursă unică şi autosuficientă, capabilă să efectueze calcule extrem de complexe şi să elaboreze date mari consumatoare de resurse.

([12]) Phishing= se defineşte „phishing" în informatică o tehnică de cracking utilizată pentru a avea acces la informațiile personale şi confidențiale pentru a uzurpa identitatea prin intermediul unor e-mailuri false concepute astfel încât să pară autentice.

([13]) Pirateria („piracy") = termen utilizat de către „piraţii" în informatică pentru a descrie un program al cărui protecție anti-copiere a fost dezactivat şi care este disponibil şi poate fi descărcat de pe Internet.

([14]) COM(2001) 298 final.

([15]) A se vedea nota de subsol 1.

— un cadru de reglementare care include și protecția datelor și a vieții private;

— lupta împotriva infracționalității informatice.

2.6 Înregistrarea atacurilor informatice, identificarea și prevenirea acestora în cadrul unui sistem în rețea constituie o provocare pentru găsirea soluțiilor adecvate, având în vedere modificările continue de configurație, diversitatea protocoalelor de rețea și a serviciilor oferite și dezvoltate și extrema complexitate a modurilor de atac asincron ([16]).

2.7 Cu toate acestea, perspectivele vagi de beneficiu în urma investițiilor în domeniul securității și lipsa de responsabilizare a utilizatorilor au dus, din păcate, la subestimarea riscurilor și la diminuarea eforturilor făcute pentru a dezvolta o cultură a securității informatice.

3. **Propunerea Comisiei**

3.1 Prin comunicarea sa privind o Strategie pentru o societate informațională sigură ([17]), Comisia dorește îmbunătățirea securității informatice printr-o strategie dinamică și integrată bazată pe:

a) îmbunătățirea dialogului dintre autoritățile publice și Comisie, printr-o evaluare comparativă a politicilor naționale și prin identificarea celor mai bune practici de comunicare electronică în regim de siguranță;

b) o mai bună sensibilizare a cetățenilor și a IMM-urilor față de sistemele de securitate eficiente, datorită rolului stimulator al Comisiei și participării mai intense a Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (AESRI/ENISA);

c) un dialog privind mijloacele și instrumentele regulamentare utilizate pentru a ajunge la un raport echilibrat între securitate și drepturile fundamentale, inclusiv protecția vieții private.

3.2 Comunicarea prevede, de asemenea, prin intermediul unui cadru adecvat pentru colectarea datelor privind încălcarea securității, nivelul de încredere al utilizatorilor și evoluțiile din industria securității, instituirea de către ENISA a unui parteneriat de încredere

a) cu statele membre;

b) cu consumatorii și utilizatorii;

c) cu industria securității informatice;

d) cu sectorul privat.

prin crearea unui portal european multilingv de informare și de alertă, pentru un parteneriat strategic între sectorul privat, statele membre și cercetători.

3.2.1 Comunicarea prevede, de asemenea, o responsabilizare crescută a participanților față de necesitățile și riscurile în materie de securitate.

3.2.2 În ceea ce privește cooperarea internațională și cu țările terțe, „dimensiunea globală a rețelelor și a informației impune Comisiei să își multiplice eforturile, atât la nivel internațional cât și în coordonare cu statele membre, pentru a promova o cooperare globală în materie de securitatea rețelelor informatice” ([18]): această indicație nu este reluată însă în acțiunile bazate pe dialog, parteneriat și responsabilizare.

4. **Observații**

4.1 Comitetul își exprimă acordul cu analizele și argumentele în favoarea unei strategii europene integrate și dinamice pentru securitatea rețelelor și a informației. Comitetul consideră că problema securității este esențială dacă se dorește promovarea unei atitudini mai favorabile față de punerea în aplicarea a tehnologiei informației (IT) și creșterea încrederii în acestea. CESE și-a exprimat poziția în numeroase avize ([19]).

4.1.1 Comitetul reafirmă din nou ([20]) că „rețeaua Internet și noile tehnologii de comunicații on-line (de exemplu, telefonia mobilă sau calculatoarele palmtop cu funcții multimedia capabile de a se conecta în rețea, în plină dezvoltare) constituie instrumente fundamentale pentru dezvoltarea economiei cunoașterii, a e-economiei și a e-administrației”.

([16]) Multivariate Statistical Analysis for Network Attacks Detection (Analiza statistică multidimensională pentru detectarea atacurilor asupra rețelei). Guangzhi Qu, Salim Hariri* — 2005, SUA, Arizona. Laboratorul de tehnologie Internet, Departmentul ECE, Universitatea din Arizona, http://www.ece.arizona.edu/~hpdc
Mazin Yousif, Intel Corporation, SUA — Lucrare finanțată parțial printr-o bursă a Consiliului de cercetare-dezvoltare IT al Intel Corporation.

([17]) COM(2006) 251, final din 31.5.2006.

([18]) COM(2006) 251, final, penultimul paragraf, cap. 3.

([19]) Cf. documentelor următoare:
— Avizul CESE referitor la „Propunerea de directivă a Parlamentului European și a Consiliului privind păstrarea datelor tratate în cadrul furnizării de servicii publici de comunicații electronice și care modifică Directiva 2002/58/CE” — JO C 69, 21.3.2006 p. 16;
— Avizul CESE referitor la „Comunicarea Comisiei adresată Consiliului, Parlamentului European, Comitetul Economic și Social European și Comitetului Regiunilor — i2010 — O societate europeană informațională pentru dezvoltarea și ocuparea forței de muncă” — JO C 110, 9.5.2006, p. 83.
— Avizul CESE referitor la „Propunerea de decizie a Parlamentului European și a Consiliului privind elaborarea unui program comunitar multianual pentru promovarea unei utilizări mai sigure a Internetului și a noilor tehnologii on-line” — JO C 157, 28.6.2005 p. 136.
— Avizul CESE privind „Comunicarea Comisiei adresată Consiliului, Parlamentului, Comitetul Economic și Social European și Comitetului Regiunilor — Securitatea rețelelor și a informației: propunere pentru o abordare strategică europeană”, JO C 48 din 21.2.2002, p. 33.

([20]) A se vedea nota de subsol 19, a treia liniuță.

4.2 *Pentru adoptarea de către Comisie de propuneri mai energice*

4.2.1 Cu toate acestea, Comitetul consideră că abordarea propusă de către Comisie de a fundamenta această strategie integrată și dinamică atât pe un dialog deschis și inclusiv, cât și pe un parteneriat și o responsabilizare mai mare a tuturor participanților, în special a utilizatorilor, poate fi extinsă și mai mult.

4.2.2 Această poziție a fost deja evidentă în avizele precedente „această luptă trebuie să implice direct, pentru a fi eficace, toți utilizatorii de Internet, care trebuie formați și informați despre măsurile de precauție și mijloacele necesare pentru a se proteja contra primirii de asemenea conținuturi periculoase sau nedorite sau pentru a nu fi utilizați ca transmițători de asemenea conținuturi. Partea de informare și formare din planul de acțiune trebuie, în opinia Comitetului, să acorde prioritate mobilizării utilizatorilor" ([21]).

4.2.3 Cu toate acestea, Comitetul consideră că participarea utilizatorilor și a cetățenilor trebuie să se efectueze astfel încât să concilieze protecția necesară a informației și a rețelelor cu libertățile individuale și dreptul utilizatorilor la conectări sigure și la un preț redus.

4.2.4 Trebuie avut în vedere că securitatea informatică reprezintă un cost pentru consumator, mai ales din punct de vedere al timpului destinat eliminării și ocolirii obstacolelor. Comitetul consideră că este necesar să se impună instalarea sistematică de sisteme de protecție antivirus pe toate calculatoarele, sisteme pe care utilizatorul ar putea să le activeze sau nu, dar care ar fi prezente „din fabrică" în produs.

4.3 *Pentru o strategie comunitară mai dinamică și inovatoare*

4.3.1 Independent de aceste măsuri, Uniunea Europeană ar trebui, în opinia Comitetului, să își fixeze obiective mai ambițioase și să lanseze o strategie inovatoare, integrată și dinamică, bazată pe inițiative noi:

— sisteme care să permită identificarea digitală a utilizatorilor, cărora li se cere prea des să se identifice ei înșiși;

— acțiuni, puse în aplicare cu ajutorul ETSI ([22]), necesare pentru o utilizare sigură a TIC, care oferă soluții ad-hoc și rapide, asigurând un prag comun de securitate pentru întreaga Uniune Europeană;

— acțiuni de prevenire prin integrarea de cerințe minime de securitate în sistemele informatice și de rețea și lansarea de acțiuni pilot prin organizarea în școlile de toate tipurile și de toate nivelurile de cursuri despre securitatea informatică;

— crearea la nivel european a unui cadru juridic-normativ sigur și recunoscut. Un asemenea cadru, aplicat la informatică și la rețele, ar permite să se treacă de la securitatea informatică la asigurarea informatică;

— întărirea sistemelor europene și naționale de evaluare a riscurilor și o mai bună capacitate de aplicare a actelor cu putere de lege cu scopul de a sancționa delictele informatice care cauzează prejudicii vieții private și fișierelor informatice;

— acțiuni pentru a evita apariția de monoculturi informatice care utilizează produse și soluții care vulnerabile; sprijinirea inovațiilor multiculturale diversificate pentru realizarea unui Spațiu unic european al informației (SEIS — Single European Information Space).

4.3.2 Comitetul apreciază că este oportun să se creeze un punct de contact „Securitatea TIC" inter DG ([23]). Acest punct de contact ar permite intervenția:

— la nivelul serviciilor interne ale Comisiei;

— la nivelul statelor, prin elaborarea de soluții orizontale pentru aspectele legate de inter-operativitate, de gestionarea identității, de protecția vieții private, de accesarea liberă a informațiilor și serviciilor, de cerințele minime de securitate;

— la nivel internațional, pentru ca Europa să se poată exprima cu o singură voce în diferitele organizații de tipul ONU, G8, OCDE, ISO.

4.4 *Pentru întărirea acțiunilor UE în domeniul coordonării responsabile*

4.4.1 Comitetul acordă, de asemenea, mare importanță creării unei rețele europene pentru securitatea rețelelor și a informației (*European Network and Information Security Network*) care ar permite finanțarea anchetelor, a studiilor și a atelierelor pe tema mecanismelor de securitate și a interoperabilității lor, a criptografiei avansate și a protecției vieții private.

4.4.2 Comitetul consideră că ar fi necesar, în acest sector sensibil, să se optimizeze rolul cercetării europene printr-o sinteză utilă a conținutului:

— programului european de cercetare a securității informatice (PERS) ([24]) inclus în al 7-lea program-cadru RDT,

([21]) A se vedea nota de subsol 19, a treia liniuță.

([22]) ETSI (Institutul european de standardizare pentru telecomunicații), mai ales Atelierul din 16 și 17 ianuarie 2006. ETSI a elaborat, între altele, standarde pentru interceptările ilegale (TS 102 232; 102 233; 102 234), pentru accesul la Internet Lan Wireless (TR 102 519) și pentru semnăturile electronice, și a dezvoltat algoritmi de securitate pentru GSM GPRS și UMTS.

([23]) Acest punct de contact inter DG-uri ar putea fi finanțat în cadrul priorităților TSI ale programului specific de cooperare al celui de al 7-lea program-cadru al RDT sau ale programului european de cercetare privind securitatea PERS.

([24]) Al șaptelea program cadru de RST & D — program specific Cooperare — prioritate tematică „Securitatea", dotată cu un buget de 1,35 miliarde euro pentru perioada 2007-2013.

— programului Safer Internet Plus și

— programului european de protecție a infrastructurilor critice (PEPIC) ([25]).

4.4.3 S-ar putea adăuga la aceste propuneri instituirea unei „Zile europene a securității informatice", susținută prin campanii naționale de educație în școli și campanii de informare adresate utilizatorilor privind procedurile informatice de protecție a informațiilor, plus informațiile despre noile tehnologii realizate în domeniul vast și în plină evoluție al calculatoarelor.

4.4.4 Comitetul a subliniat de mai multe ori că „rapiditatea cu care întreprinderile sunt dispuse să introducă TIC în activitățile comerciale depinde de felul în care este percepută și de încrederea care există în securitatea tranzacțiilor on-line. În funcție de încrederea pe care o au consumatorii în securitatea tranzacțiilor, aceștia sunt sau nu dispuși să-și indice numărul cărții de credit pe un site internet" ([26]).

4.4.5 Comitetul este convins că, dat fiind enormul potențial de dezvoltare a sectorului, este necesar să se pună în aplicare politici specifice și să se adapteze politicile actuale la noile evoluții. Este necesar să existe o strategie integrată care să coordoneze inițiativele europene în materie de securitate informatică, indiferent de sector, și care să garanteze o difuzare omogenă și sigură a TIC în societate.

4.4.6 Comitetul consideră că strategiile importante, cum este cea în discuție, se dezvoltă cu o lentoare excesivă din cauza dificultăților birocratice și culturale create de către statele membre atunci când trebuie luate decizii indispensabile la nivel comunitar.

4.4.7 Comitetul consideră, de asemenea, că resursele comunitare sunt insuficiente pentru a permite punerea în aplicare a multiplelor proiecte prioritare care ar putea aduce rezolvări concrete la noile probleme create de globalizare, cu condiția de a fi duse la bun sfârșit la nivel comunitar.

4.5 *Pentru garanții comunitare îmbunătățite privind protecția consumatorilor*

4.5.1 Comitetul este conștient de faptul că statele membre au pus la punct măsuri tehnologice de securitate și proceduri de gestionare a securității adaptate propriilor lor nevoi și care tratează aspecte diferite de la un stat la altul. Acesta este unul dintre motivele care fac dificilă găsirea unei soluții unice și eficiente pentru problemele de securitate. Cu excepția anumitor rețele administrative, nu există cooperare transfrontalieră sistematică între statele membre, în ciuda faptului că problemele de securitate nu pot fi tratate separat de fiecare țară.

4.5.2 Comitetul observă, de altfel, că, prin intermediul deciziei-cadru 2005/222/JAI, Consiliul a lansat un cadru de cooperare între autoritățile judiciare și celelalte autorități competente pentru a garanta, prin intermediul unei apropieri a normelor penale naționale care pedepsesc atacurile împotriva sistemelor informatice, o abordare coerentă a statelor membre în ceea ce privește:

— accesul ilicit la sistemele informatice;

— interferențele ilicite care au ca scop provocarea unei perturbări grave sau întreruperea funcționării unui sistem informatic;

— interferențele ilicite care vizează datele și care au drept scop să șteargă, să avarieze, să deterioreze, să modifice, să elimine sau să facă inaccesibile datele informatice ale unui sistem informatic;

— incitarea, asistența și complicitatea la delictele care au fost menționate mai sus.

4.5.3 Decizia-cadru precizează, de asemenea, criteriile care permit stabilirea răspunderii persoanelor juridice și eventualele sancțiuni care trebuie aplicate atunci când această răspundere este dovedită.

4.5.4 Fiind vorba de dialogul cu autoritățile publice din statele membre, Comitetul sprijină propunerea Comisiei ca aceste autorități să efectueze o evaluare comparativă a politicilor naționale privind securitatea rețelelor și a sistemelor informatice, inclusiv a celor care sunt destinate numai sectorului public. Această propunere figura deja într-un aviz CESE din 2001 ([27]).

4.6 *Pentru o generalizare a culturii securității*

4.6.1 În ceea ce privește implicarea industriei securității informatice, pentru a proteja dreptul la protecția vieții private și la confidențialitate clienților săi, aceasta trebuie să garanteze efectiv utilizarea de sisteme de supraveghere materială a instalațiilor sale și de criptare a comunicațiilor, în funcție de evoluția în domeniul tehnicii ([28]).

([25]) COM(2005) 576, final din 17.11.2005.
([26]) A se vedea nota de subsol 19, a doua liniuță.
([27]) A se vedea nota de subsol 19, a patra liniuță.
([28]) Cf. Directiva 97/66/CE privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul telecomunicațiilor (JO L 24, 30.1.1998).

4.6.2 În ceea ce privește acțiunea de sensibilizare, Comitetul consideră că este fundamental să se creeze o veritabilă „cultură a securității" care să fie pe deplin compatibilă cu libertatea informației, a comunicării și a expresiei. De altfel, numeroși utilizatori nu sunt conștienți de toate riscurile legate de pirateria informatică, în timp ce numeroși operatori, vânzători sau furnizori de servicii nu reușesc să evalueze existența și amplitudinea aspectelor vulnerabile.

4.6.3 În cazul în care protecția vieții private și a datelor personale sunt obiective prioritare, consumatorii au, de asemenea, dreptul de a fi protejați în mod eficient împotriva profilării nominative abuzive făcute prin intermediul unor programe-spion de tipul „spyware" și „web bugs" sau prin alte mijloace. Ar trebui împiedicat spamming-ul ([29]) (trimiterea masivă de mesaje nesolicitate) care este adesea o consecință a acestor abuzuri. Aceste intruziuni produc prejudicii victimelor ([30]).

4.7 *Pentru o agenție europeană mai puternică și mai activă*

4.7.1 Comitetul este favorabil unui rol mai eficient și mai puternic al Agenției Europene pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) în ceea ce privește acțiunea de sensibilizare, dar și, mai ales, acțiunile de informare și de formare a operatorilor și a utilizatorilor, astfel cum a indicat deja într-un alt aviz recent ([31]) privind furnizarea de servicii de comunicare electronică accesibile publicului.

4.7.2 Fiind vorba de acțiuni prevăzute pentru responsabilizarea fiecărui grup de participanți, acestea par să țină de respectarea foarte strictă a principiului subsidiarității. Într-adevăr, statelor membre și sectorului privat le revine sarcina de a le pune în aplicare, în funcție de responsabilitățile lor specifice.

4.7.3 Agenția ar putea utiliza contribuțiile aduse de rețeaua europeană pentru securitatea rețelelor și a informației (European Network and Information Security Network) pentru a organiza activități comune; aceasta ar trebui de asemenea să utilizeze portalul comunitar plurilingv de alertă contra riscurilor informatice pentru a putea furniza informații personalizate și interactive, cu limbaje ușor de utilizat, mai ales de către IMM-uri și utilizatorii individuali de orice vârstă.

Bruxelles, 16 februarie 2007.

Președintele
Comitetului Economic și Social European
Dimitris DIMITRIADIS

([29]) „Pollupostage" în franceză.
([30]) Cf. Avizul CESE privind „rețelele de comunicații electronice" (JO C 123, 25.4.2001, p. 50), privind „comerțul electronic" (JO C 169, 16.6.1999, p. 36) și privind „impactul comerțului electronic asupra pieței unice" (JO C 123, 25.4.2001, p. 1).

([31]) A se vedea nota de subsol 19, prima liniuță.