I

*(Rezoluții, recomandări, orientări şi avize)*

# REZOLUȚII

# CONSILIU

## REZOLUȚIE A CONSILIULUI

## din 22 martie 2007

## cu privire la o strategie pentru o societate informațională sigură în Europa

(2007/C 68/01)

CONSILIUL UNIUNII EUROPENE,

ADOPTĂ PREZENTA REZOLUȚIE ȘI

APRECIAZĂ

Comunicarea din 31 mai 2006 a Comisiei către Consiliu, Parlamentul European, Comitetul Economic și Social European și Comitetul Regiunilor — O strategie pentru o societate informațională sigură — „Dialog, parteneriat și împuternicire“;

IA NOTĂ DE

Comunicarea din 15 noiembrie 2006 a Comisiei către Consiliu, Parlamentul European, Comitetul Economic și Social European și Comitetul Regiunilor privind lupta împotriva spamului, a softurilor-spion și a softurilor dăunătoare;

REAMINTEȘTE:

(1) Rezoluția Consiliului din 28 ianuarie 2002 privind o abordare comună și acțiuni specifice în domeniul securității rețelelor și informațiilor ([1]);

(2) Rezoluția Consiliului din 18 februarie 2003 privind o abordare europeană a unei culturi a securității rețelelor și informațiilor ([2]);

(3) Concluziile Consiliului din 8-9 martie 2004 privind comunicațiile nesolicitate cu scop de marketing direct sau „spamul“, precum și Concluziile Consiliului din 9-10 decembrie 2004 privind combaterea spam-ului;

(4) Concluziile Consiliului European din martie 2005 de relansare a strategiei de la Lisabona, precum și Concluziile Consiliului European din martie 2006 care invită Comisia și statele membre să pună energic în practică noua Strategie i2010;

(5) Cadrul de reglementare UE pentru comunicațiile electronice ([3]) și în special dispozițiile referitoare la securitatea comunicării, viața privată și confidențialitate, care au contribuit la asigurarea unui înalt nivel de protecție a datelor personale și a vieții personale, precum și a integrității și securității rețelelor de comunicații publice;

(6) Regulamentul (CE) nr. 460/2004 din 10 martie 2004 al Parlamentului European și al Consiliului de instituire a Agenției europene de securitate a rețelelor și a informațiilor (ENISA) ([4]);

(7) Agenda de la Tunis și Angajamentul de la Tunis al Summitului mondial privind societatea informațională (SMSI), care au subliniat necesitatea de a continua lupta împotriva infracționalității în mediul cibernetic și a spam-ului, asigurând în același timp protecția vieții personale și a libertății de expresie, precum și necesitatea de a promova, a dezvolta și a pune în continuare în practică o cultură globală a ciber-securității, în cooperare cu toate părțile interesate;

(8) Concluziile Președinției în urma Conferinței europene anuale privind societatea informațională (27-28 septembrie 2006) „i2010 — Către o societate europeană informațională ubicuă“, de la Espoo, Finlanda;

([1]) JO C 43, 16.2.2002, p. 2.
([2]) JO L 48, 28.2.2003, p. 1.
([3]) Directivele 2002/58/CE (Directivă privind viața privată și comunicațiile electronice), 2002/20/CE (Directivă de autorizare), 2002/22/CE (Directivă privind serviciile universale) (JO L 201, 31.7.2002, p. 37, JO L 108, 24.4.2002, p. 21 și, repectiv, JO L 108, 24.4.2002, p. 51).
([4]) JO L 77, 13.3.2004, p. 1.

ÎN CONSECINȚĂ, SUBLINIAZĂ CĂ:

(1) Societățile noastre trec rapid într-o nouă fază de dezvoltare, pe drumul către o societate informațională ubicuă, în care tot mai multe dintre activitățile de zi cu zi ale cetățenilor se bazează pe utilizarea tehnologiilor informaționale și de comunicații (TIC), precum și pe rețelele de comunicații electronice; securitatea rețelelor și a informațiilor trebuie considerată drept un element-cheie care să înlesnească această dezvoltare și succesul acesteia;

(2) Încrederea reprezintă o componentă vitală a succesului noii societăți informaționale; încrederea se referă de asemenea la experiențele utilizatorilor finali și la necesitatea de a le respecta viața privată; de aceea, securitatea rețelelor și a informațiilor nu trebuie considerată drept o chestiune pur tehnică;

(3) Securitatea rețelelor și a informațiilor este o componentă esențială a creării unui spațiu european al informațiilor în cadrul Inițiativei i2010, contribuind astfel la succesul Strategiei reînnoite de la Lisabona; TIC reprezintă, de asemenea, o componentă fundamentală a inovării, a creșterii economice și a creării de locuri de muncă în întreaga economie;

(4) Noile tehnologii care ne vor conduce spre societatea informațională ubicuă sunt deja în curs de elaborare; apariția tehnologiilor inovatoare (cum ar fi rețelele fără fir de mare viteză, dispozitivele de identificare a frecvenței radio (RFID), rețelele cu senzori) și a serviciilor inovatoare, bogate în conținut (cum ar fi televiziunea pe bază de protocol internet (IPTV), protocolul pe bază de voce pe internet (VoIP), televiziunea mobilă și alte servicii mobile) necesită niveluri adecvate de securitate a rețelei și a informațiilor de la începutul fazei de dezvoltare, în scopul atingerii valorii comerciale reale; adoptarea timpurie a noilor inovații promițătoare este foarte importantă pentru dezvoltarea societății informaționale și pentru competitivitatea Europei; organismele guvernamentale și întreprinderile ar trebui să adopte noile tehnologii și servicii emergente cât mai curând posibil, în scopul de a accelera adoptarea lor generalizată;

(5) Faptul că industria europeană este atât un utilizator exigent, cât și un furnizor competitiv de rețele și de produse și servicii de securitate are o importanță strategică pentru EU; diversitatea, deschiderea și inter-operabilitate ar trebui promovate ca parte integrantă a securității;

(6) Cunoștințele și aptitudinile în domeniul securității rețelelor și a informațiilor trebuie, de asemenea, să devină o parte integrantă a vieții de zi cu zi a tuturor indivizilor și a părților interesate din societate; s-au desfășurat mai multe campanii de sensibilizare a opiniei publice, atât la nivel național, cât și la nivelul UE, dar mai există multe de făcut în acest domeniu, mai ales în ceea ce privește utilizatorii finali și întreprinderile mici și mijlocii (IMM-urile); ar trebui acordată o atenție deosebită utilizatorilor care au nevoi speciale sau care au un nivel scăzut de conștientizare cu privire la aspectele legate de securitatea rețelelor și a informațiilor; toate părțile interesate ar trebui să fie conștiente de faptul că fac parte din lanțul global de securitate și, în consecință, ar trebui împuternicite în această calitate; aspectele legate de securitatea rețelelor și a informațiile ar trebui luate în considerare în toate cursurile de educare și formare profesională referitoare la TIC;

(7) Crearea ENISA a reprezentat un important pas înainte în direcția eforturilor UE de a reacționa la provocările privitoare la securitatea rețelelor și a informațiilor; domeniul de activitate, obiectivele, sarcinile și durata de activitate ale ENISA sunt definite de Regulamentul (CE) nr. 460/2004;

(8) Resursele destinate cercetării și dezvoltării (C&D), precum și inovării, atât la nivel național, cât și la nivelul UE, reprezintă unul dintre elementele-cheie ale consolidării nivelului de informare și securitate a rețelei aferente noilor sisteme, aplicații și servicii; la nivelul UE ar trebui intensificate eforturile depuse în domeniile cercetării și inovării legate de securitate, în special prin intermediul celui de-al șaptelea program-cadru (PC7) și al Programului-cadru privind competitivitatea și inovarea (PCI); de asemenea, ar trebuie ca eforturile să se axeze pe măsurile de difuzare și încurajare a exploatării comerciale a rezultatelor obținute în consecință, inclusiv evaluarea utilității lor în beneficiul comunității în sens larg; acest lucru va spori capacitatea furnizorilor europeni de a oferi soluții de securitate care să satisfacă necesitățile specifice ale pieței europene;

(9) Societatea informațională ubicuă prezintă avantaje deosebite, dar în același timp pune probleme importante, creând astfel o nouă hartă a riscurilor potențiale; amenințările la adresa securității și a vieții private, printre altele prin intermediul interceptării și exploatării ilegale a datelor, devin din ce în ce mai serioase, mai concentrate și mai axate pe beneficiul economic; ar trebui create, de o manieră inovatoare, noi reacții la amenințările emergente, precum și la cele existente, iar aceste reacții ar trebui, de asemenea, să trateze aspectele datorate complexității sistemelor, greșelilor, accidentelor sau neclarității instrucțiunilor; ar trebui încurajate și promovate în continuare crearea și dezvoltarea unor organisme naționale de reacție în cazuri de urgență de natură informatică, axate pe diferiți factori, precum și cooperarea dintre aceste organisme și cea cu alte părți interesate competente;

(10) Standardizarea și certificarea produselor, serviciilor și sistemelor de gestiune, în special furnizate de către instituțiile existente, merită o atenție deosebită în cadrul politicii UE privind rețelele și securitatea informațiilor ca modalitate de difuzare a bunelor practici și a profesionalismului în domeniul rețelelor și al securității informațiilor; în mod special, noile tehnologii emergente, cum sunt identificarea frecvenței radio (RFID) și televiziunea mobilă ar avea de câștigat din posibila adoptare a unor standarde deschise și inter-operabile emergente; ar fi încurajată funcționarea organismelor europene de standardizare în acest domeniu;

(11) Având în vedere faptul că rețelele electronice și sistemele de informații joacă un rol din ce în ce mai important în cadrul funcționării globale a infrastructurilor vitale, disponibilitatea și integritatea acestora devin indispensabile pentru siguranța și calitatea vieții administrațiilor, întreprinderilor și cetățenilor, precum și pentru funcționarea globală a societăților;

(12) Sunt necesare, mai mult ca oricând, cooperarea și abordările practice; diferitele părți interesate ar trebui să își identifice și să își recunoască rolurile, responsabilitățile și drepturile;

ȘI, PRIN URMARE, INVITĂ STATELE MEMBRE:

(1) Să susțină programele de instruire și să sensibilizeze opinia publică în general cu privire la aspectele referitoare la rețele și la securitatea informațiilor, de exemplu prin lansarea de campanii informative cu privire la aspectele legate de rețele și de securitatea informațiilor, adresate tuturor cetățenilor/utilizatorilor și tuturor sectoarelor economiei, mai ales IMM-urilor și utilizatorilor finali cu nevoi speciale sau cu un nivel scăzut de cunoaștere; până în anul 2008 s-ar putea alege o dată comună ca zi a sensibilizării opiniei publice la nivel european (de exemplu „Ziua securității informațiilor și rețelelor"), care să fie găzduită anual și în regim de voluntariat de către fiecare stat membru în parte;

(2) Să consolideze contribuția la cercetarea și dezvoltarea cu privire la securitate și să îmbunătățească caracterul utilizabil și difuzarea rezultatelor obținute; să încurajeze dezvoltarea de parteneriate inovatoare în scopul de a stimula creșterea industriei europene a securității în domeniul TIC și de a spori gradul de utilizare timpurie a noilor tehnologii și servicii de securitate a rețelelor și a informațiilor, pentru a le da un impuls comercial;

(3) Să acorde atenția cuvenită nevoii de a preveni și a combate amenințările la adresa securității, atât pe cele noi, cât și pe cele existente în rețelele de comunicații electronice, printre care intercepția și exploatarea ilegală a datelor, să recunoască și să abordeze riscurile asociate și să încurajeze, în cooperare cu ENISA, după caz, schimburile eficace de informații și cooperarea dintre organizațiile și agențiile relevante la scară națională; să se angajeze în combaterea spam-ului, a spyware și malware, în special prin intermediul unei mai bune cooperări între autoritățile competente la nivel național și internațional;

(4) Să consolideze cooperarea reciprocă dintre ele în cadrul i2010, în scopul de a identifica practicile eficace și inovatoare de îmbunătățire a securității rețelelor și informațiilor și de a difuza cunoștințele cu privire la aceste practici, pe bază de voluntariat, în întreaga Uniune;

(5) Să încurajeze perfecționarea continuă a organismelor naționale de reacție în cazuri de urgență de natură informatică;

(6) Să promoveze un mediu care să încurajeze prestatorii de servicii și operatorii de rețea să ofere servicii robuste clienților lor și să asigure, în structura serviciilor și soluțiilor lor de securitate, rezistența și posibilitatea de a alege, pusă la dispoziția clienților; să încurajeze și să solicite, în situațiile în care este oportun, ca operatorii de rețea și prestatorii de servicii să asigure un nivel adecvat de securitate a rețelei și a informațiilor în beneficiul clienților lor;

(7) Să continue o discuție strategică a Grupului de înalt nivel i2010, ținând seama în același timp de dezvoltarea în curs a societății informaționale, și să asigure o abordare consecventă a dimensiunilor reglementării, a co-reglementării, a cercetării și dezvoltării și a e-guvernării, alături de comunicare și educare;

(8) În conformitate cu Planul de acțiune pentru e-guvernare i2010, să asigure condițiile necesare pentru generalizarea unor servicii de e-guvernare omogene, să promoveze soluții inter-operabile de gestionare a identității și să opereze toate schimbările care se impun în organizarea sectorului public; guvernele și administrațiile publice ar trebui să servească drept exemplu de practici optime prin promovarea de servicii sigure de e-guvernare puse la dispoziția tuturor cetățenilor;

APRECIAZĂ INTENȚIA COMISIEI DE:

(1) A continua dezvoltarea unei strategii cuprinzătoare și dinamice pentru securitatea rețelelor și a informațiilor la nivelul UE. Abordarea holistică propusă de Comisie are o deosebită importanță;

(2) A aborda securitatea rețelelor și a informațiilor drept unul dintre obiectivele analizei Cadrului de reglementare UE pentru comunicații electronice;

(3) A continua să joace un rol menit să sporească nivelul de sensibilizare a opiniei publice cu privire la nevoia unui angajament politic general de a combate spam-ul, spyware și malware; a intensifica dialogul și cooperarea cu țările terțe, în special prin intermediul acordurilor cu țările terțe, care să cuprindă subiectul combaterii spam-ului, a spyware și a malware;

(4) A consolida implicarea ENISA în sprijinirea Strategiei pentru o societate informațională sigură în Europa, astfelcum este stabilită de prezenta rezoluție, în conformitate cu obiectivele și sarcinile stabilite de Regulamentul (CE) nr. 460/2004, precum și în cooperarea mai strânsă și în relațiile de lucru mai apropiate cu statele membre și cu părțile interesate;

(5) A crea, în cadrul inițiativei i2010, în cooperare cu statele membre și cu toate părțile interesate, mai ales cu experții în securitate statistică și informațională ai statelor membre, indicatori corespunzători pentru studiile comunitare privind aspectele legate de securitate și încredere;

(6) A încuraja statele membre să examineze, prin intermediul unui dialog cu mai multe părți interesate, vectorii economici, comerciali și societali în scopul dezvoltării unei politici specifice sectorului tehnologiilor informaționale și comunicaționale, care să sporească securitatea și rezistența rețelelor și ale sistemelor informaționale, ca potențială contribuție la Programul european planificat pentru protecția infrastructurii vitale;

(7) A-și continua eforturile, în coordonare cu statele membre, de a promova dialogul cu partenerii internaționali și cu organizațiile relevante în vederea promovării cooperării globale în domeniul securității rețelelor și a informațiilor, mai ales prin punerea în practică a liniilor de acțiune ale Summitului mondial privind societatea informațională SMSI și prin înaintarea de rapoarte regulate Consiliului;

ȘI CHEAMĂ:

(1) ENISA să lucreze în continuare în strânsă cooperare cu statele membre, cu Comisia și cu alte părțile interesate relevante, în scopul de a realiza acele sarcini și obiective care sunt definite de Regulamentul (CE) nr. 460/2004 și să ofere asistență Comisiei și statelor membre în eforturile acestora de a îndeplini cerințele de securitate a rețelelor și a informațiilor, contribuind astfel la punerea în aplicare și la dezvoltarea în continuare a Strategiei pentru o societate informațională sigură în Europa, astfel cum este stabilită de prezenta rezoluție;

(2) Toate părțile interesate să îmbunătățească securitatea programelor software și securitatea și rezistența rețelelor și a sistemelor informaționale în conformitate cu Strategia pentru o societate informațională sigură în Europa, astfel cum este stabilită de prezenta rezoluție, precum și să se implice într-o dezbatere structurată, care să cuprindă mai multe părți interesate, pe tema modului optim de a utiliza instrumentele tehnice și de reglementare existente;

(3) Întreprinderile să aibă o atitudine pozitivă în raport cu securitatea informațională și a rețelelor în scopul de a crea produse și servicii mai avansate și mai sigure, considerând investiția în astfel de produse și servicii drept un avantaj competitiv;

(4) Producătorii și prestatorii de servicii să înglobeze, în cazurile în care acest lucru este oportun, cerințe de securitate, respectare a vieții private și a confidențialității în proiectarea produselor și serviciilor lor și în desfășurarea infrastructurii lor de rețea, a aplicațiilor și a programelor software, de a pune în practică soluții de securitate și a le monitoriza;

(5) Părțile interesate să coopereze și să lanseze în condiții de siguranță medii experimentale de testare și faze-pilot ale noilor tehnologii și servicii; părțile interesate să adopte la timp noile tehnologii și servicii sigure după lansarea comercială a acestora;

(6) Toate părțile interesate să se implice în noi eforturi de a combate spam-ul și alte practici necorespunzătoare existente pe Internet și să coopereze activ cu autoritățile competente la nivel național și internațional;

(7) Prestatorii de servicii și industria TIC să se concentreze pe sporirea securității, a protecției vieții private și a caracterului utilizabil al produselor, proceselor și serviciilor în vederea fiabilității, a prevenirii și combaterii uzurpării de identitate și a altor atacuri intruzive asupra vieții private;

(8) Operatorii de rețea, prestatorii de servicii și sectorul privat să împărtășească și să aplice bunele practici în domeniul securității, să promoveze o cultură a analizei și a gestionării riscurilor în organizații și întreprinderi, prin sprijinirea unor programe corespunzătoare de instruire și prin elaborarea de planuri pentru situații neprevăzute, precum și să pună soluțiile de securitate la dispoziția clienților lor, ca parte a ofertei lor de servicii.