

32005F0222

16.3.2005

JURNALUL OFICIAL AL UNIUNII EUROPENE

L 69/67

**DECIZIA-CADRU 2005/222/JAI A CONSILIULUI
din 24 februarie 2005
privind atacurile împotriva sistemelor informatice**

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană și, în special, articolul 29, articolul 30 alineatul (1) litera (a), articolul 31 alineatul (1) litera (e) și articolul 34 alineatul (2) litera (b) ale acestuia,

având în vedere propunerea Comisiei,

având în vedere avizul Parlamentului European ⁽¹⁾,

întrucât:

- (1) Obiectivul prezentei decizii-cadru constă în îmbunătățirea cooperării între autoritățile judiciare și alte autorități competente, inclusiv poliția și celelalte servicii specializate de aplicare a legii din statele membre, prin apropierea normelor în materie de drept penal din statele membre în ceea ce privește atacurile împotriva sistemelor informatice.
- (2) Există dovezi că s-au produs atacuri împotriva sistemelor informatice, în special din partea criminalității organizate, și se manifestă o îngrijorare crescândă în fața posibilității de atacuri teroriste împotriva sistemelor informatice care fac parte din infrastructura critică a statelor membre. Această situație reprezintă o amenințare la adresa realizării unei societăți informaționale mai sigure și a unui spațiu de libertate, securitate și justiție, necesitând, prin urmare, o reacție la nivelul Uniunii Europene.
- (3) O reacție eficientă la aceste amenințări necesită o abordare de ansamblu în ceea ce privește securitatea rețelelor și a informațiilor, după cum se subliniază în Planul de acțiune eEurope, în comunicarea Comisiei „Securitatea rețelelor și a informațiilor: propunere pentru o abordare politică europeană” și în rezoluția Consiliului din 28 ianuarie 2002 privind o abordare comună și acțiuni specifice în domeniul securității rețelelor și a informațiilor ⁽²⁾.
- (4) Necesitatea de a continua campania de conștientizare a problemelor legate de securitatea informațiilor și de a furniza o asistență practică a fost subliniată și în rezoluția Parlamentului European din 5 septembrie 2001.
- (5) Lacunele și diferențele considerabile existente în legislațiile statelor membre în acest domeniu pot crea obstacole în

calea luptei împotriva criminalității organizate și terorismului și pot îngreuna desfășurarea unei cooperări judiciare și polițienești eficiente în domeniul atacurilor împotriva sistemelor informatice. Dat fiind caracterul transnațional, care nu ține seama de frontiere, al sistemelor informatice moderne, atacurile împotriva acestor sisteme sunt adesea de natură transfrontalieră, subliniind nevoia urgentă de a se face în continuare demersuri pentru apropierea legislațiilor penale în acest domeniu.

- (6) Planul de acțiune al Consiliului și al Comisiei privind modalitățile optime de punere în aplicare a dispozițiilor Tratatului de la Amsterdam privind instituirea unui spațiu de libertate, securitate și justiție ⁽³⁾, Consiliul European de la Tampere din 15-16 octombrie 1999, Consiliul European de la Santa Maria da Feira din 19-20 iunie 2000, Comisia în „tabloul său de bord” și Parlamentul European în rezoluția sa din 19 mai 2000 recomandă sau fac apel la adoptarea unor măsuri legislative contra criminalității care utilizează tehnologiile avansate, inclusiv definiții, incriminări și sancțiuni comune.
- (7) Este necesar să se completeze activitatea desfășurată de organizațiile internaționale, în special cea a Consiliului Europei, în vederea apropierii legislațiilor penale, și lucrările G8 privind cooperarea transnațională în domeniul criminalității care utilizează tehnologiile avansate, prin asigurarea unei abordări comune la nivelul Uniunii Europene în acest domeniu. Acest apel a fost ulterior dezvoltat în comunicarea pe care Comisia a adresat-o Consiliului, Parlamentului European, Comitetului Economic și Social și Comitetului Regiunilor, intitulată „Crearea unei societăți informaționale mai sigure prin întărirea securității infrastructurilor informaționale și combaterea criminalității informatice”.
- (8) Normele de drept penal referitoare la atacurile împotriva sistemelor informatice ar trebui apropiate, pentru a se asigura un grad cât mai ridicat posibil de cooperare judiciară și polițienească în ceea ce privește infracțiunile penale legate de atacurile împotriva sistemelor informatice și pentru a contribui la lupta împotriva criminalității organizate și a terorismului.

⁽¹⁾ JO C 300 E, 11.12.2003, p. 26.

⁽²⁾ JO C 43, 16.2.2002, p. 2.

⁽³⁾ JO C 19, 23.1.1999, p. 1.

- (9) Toate statele membre au ratificat Convenția Consiliului Europei din 28 ianuarie 1981 privind protecția persoanelor față de prelucrarea automatizată a datelor cu caracter personal. Datele cu caracter personal prelucrate în contextul punerii în aplicare a prezentei decizii-cadru ar trebui protejate în conformitate cu principiile enunțate de convenția menționată.
- (10) Existența unor definiții comune în acest domeniu, în special pentru sistemele informatice și datele informatice, este importantă pentru a se asigura aplicarea coerentă a prezentei decizii-cadru în statele membre.
- (11) Este necesar să se adopte o abordare comună față de elementele constitutive ale infracțiunilor penale, definind drept infracțiuni de drept comun accesarea ilegală a unui sistem informatic, afectarea integrității unui sistem și afectarea integrității datelor.
- (12) În scopul combaterii criminalității informatice, fiecare stat membru ar trebui să asigure o cooperare judiciară eficientă în ceea ce privește infracțiunile bazate pe tipurile de comportament menționate la articolele 2, 3, 4 și 5.
- (13) Este necesar să se evite incriminarea excesivă, în special a cazurilor minore, ca de altfel și incriminarea titularilor de drepturi și a persoanelor autorizate.
- (14) Este necesar ca statele membre să prevadă sancțiuni pentru atacurile împotriva sistemelor informatice. Sancțiunile astfel prevăzute trebuie să fie eficiente, proporționale și disuasive.
- (15) Este oportun să se prevadă sancțiuni mai severe atunci când un atac împotriva unui sistem informatic este comis în cadrul unei organizații criminale, astfel cum este definită de Acțiunea comună 98/733/JAI din 21 decembrie 1998 privind incriminarea participării la o organizație criminală într-un stat membru al Uniunii Europene ⁽¹⁾. Este, de asemenea, oportun să se prevadă sancțiuni mai severe atunci când un astfel de atac a cauzat prejudicii grave sau a afectat interese esențiale.
- (16) Ar trebui, de asemenea, prevăzute măsuri de cooperare între statele membre în scopul asigurării unei acțiuni eficiente contra atacurilor împotriva sistemelor informatice. Prin urmare, statele membre ar trebui să facă apel, pentru efectuarea schimburilor de informații, la rețeaua existentă de puncte de contact operaționale menționate de

Recomandarea Consiliului din 25 iunie 2001 privind punctele de contact care asigură un serviciu de 24 de ore din 24 pentru combaterea criminalității care utilizează tehnologiile avansate ⁽²⁾.

- (17) Deoarece obiectivele prezentei decizii-cadru, care asigură sancționarea penală eficientă, proporțională și disuasivă a atacurilor împotriva sistemelor informatice în toate statele membre și îmbunătățesc și încurajează cooperarea judiciară prin eliminarea complicațiilor potențiale, nu pot fi atinse la un nivel satisfăcător de statele membre, întrucât normele trebuie să fie comune și compatibile, și, prin urmare, pot fi mai bine atinse la nivelul Uniunii, aceasta poate adopta măsuri, în conformitate cu principiul subsidiarității menționat la articolul 5 din Tratatul CE. În conformitate cu principiul proporționalității, astfel cum este enunțat în articolul menționat, prezenta decizie-cadru nu depășește ceea ce este necesar pentru atingerea acestor obiective.
- (18) Prezenta decizie-cadru respectă drepturile fundamentale și principiile recunoscute la articolul 6 din Tratatul privind Uniunea Europeană și reflectate în Carta drepturilor fundamentale a Uniunii Europene și, în special, capitolele II și VI ale acesteia,

ADOPTĂ PREZENTA DECIZIE-CADRU:

Articolul 1

Definiții

În sensul prezentei decizii-cadru, se aplică următoarele definiții:

- (a) „sistem informatic” înseamnă orice dispozitiv sau grup de dispozitive interconectate sau omoloage, dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor informatice, precum și datele informatice memorate, prelucrate, recuperate sau transmise de acestea în vederea exploatării, a utilizării, a protecției și a întreținerii lor;
- (b) „date informatice” înseamnă orice reprezentare de fapte, informații sau concepte într-o formă adecvată pentru prelucrare într-un sistem informatic, inclusiv un program care permite unui sistem informatic să execute o funcție;
- (c) „persoană juridică” înseamnă orice entitate care are acest statut în conformitate cu legislația aplicabilă, cu excepția statelor sau a altor organisme publice aflate în exercițiul autorității de stat și a organizațiilor internaționale de drept public;

⁽¹⁾ JO L 351, 29.12.1998, p. 1.

⁽²⁾ JO C 187, 3.7.2001, p. 5.

- (d) „fără a avea dreptul” înseamnă accesare sau afectare a integrității fără autorizarea proprietarului sau a altui titular de drepturi asupra sistemului sau a unei părți a sistemului, sau care nu sunt permise în temeiul legislației naționale.

Articolul 2

Accesarea ilegală a sistemelor informatice

(1) Fiecare stat membru adoptă măsurile necesare pentru a asigura că accesarea intenționată, fără drept, a ansamblului sau a unei părți a sistemului informatic se pedepsește ca infracțiune, cel puțin în cazurile care nu sunt minore.

(2) Fiecare stat membru poate să decidă ca respectivul comportament menționat la alineatul (1) să nu fie incriminat ca infracțiune decât în cazul în care se comite încălcarea unei măsuri de securitate.

Articolul 3

Afectarea integrității unui sistem informatic

Fiecare stat membru adoptă măsurile necesare pentru a asigura că perturbarea gravă sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, eliminarea datelor informatice sau fapta de a le face inaccesibile, atunci când fapta este comisă fără drept, se pedepsește ca infracțiune, cel puțin în cazurile care nu sunt minore.

Articolul 4

Afectarea integrității datelor

Fiecare stat membru adoptă măsurile necesare pentru a asigura că fapta săvârșită intenționat și fără drept de a șterge, periclita, deteriora, modifica, elimina date informatice dintr-un sistem informatic sau de a le face inaccesibile se pedepsește ca infracțiune, cel puțin în cazurile care nu sunt minore.

Articolul 5

Instigarea, complicitatea și tăinuirea și tentativa

(1) Fiecare stat membru asigură că instigarea și complicitatea și tăinuirea la săvârșirea uneia dintre infracțiunile menționate la articolele 2, 3 și 4 se pedepsește ca infracțiune.

(2) Fiecare stat membru asigură că tentativa de săvârșire a infracțiunilor menționate la articolele 2, 3 și 4 se pedepsește ca infracțiune.

- (3) Fiecare stat membru poate decide să nu aplice alineatul (2) în cazul infracțiunilor menționate la articolul 2.

Articolul 6

Sancțiuni

(1) Fiecare stat membru adoptă măsurile necesare pentru ca infracțiunile menționate la articolele 2, 3, 4 și 5 să fie pedepsite cu pedepse eficiente, proporționale și disuasive.

(2) Fiecare stat membru adoptă măsurile necesare pentru ca infracțiunile menționate la articolele 3 și 4 să fie pedepsite cu pedepse al căror maxim special este situat între cel puțin unu și trei ani de închisoare.

Articolul 7

Circumstanțe agravante

(1) Fiecare stat membru adoptă măsurile necesare pentru a asigura că infracțiunea menționată la articolul 2 alineatul (2) și infracțiunea menționată la articolele 3 și 4 se pedepsesc cu pedepse al căror maxim special este situat între cel puțin doi și cinci ani de închisoare atunci când sunt săvârșite în cadrul unei asocieri pentru săvârșirea de infracțiuni, astfel cum este definită în Acțiunea comună 98/733/JAI, independent de nivelul pedepsei prevăzute de aceasta.

(2) Un stat membru poate, de asemenea, adopta măsurile menționate la alineatul (1), atunci când infracțiunea a cauzat un prejudiciu grav sau a afectat interese esențiale.

Articolul 8

Răspunderea persoanelor juridice

(1) Fiecare stat membru adoptă măsurile necesare pentru a asigura că persoanele juridice pot fi trase la răspundere pentru infracțiunile menționate la articolele 2, 3, 4 și 5, săvârșite în folosul lor de către orice persoană, care acționează fie individual, fie în calitate de membru al unui organ al persoanei juridice și care exercită o funcție de conducere în cadrul acesteia, având la bază:

- (a) un mandat de reprezentare a persoanei juridice sau
- (b) autorizația de a lua decizii în numele persoanei juridice sau
- (c) autorizația de a exercita controlul în cadrul persoanei juridice.

(2) În afara cazurilor prevăzute la alineatul (1), statele membre asigură că o persoană juridică poate fi trasă la răspundere atunci când lipsa de supraveghere sau control imputabilă unei persoane menționate la alineatul (1) a făcut posibilă săvârșirea infracțiunilor menționate la articolele 2, 3, 4 și 5 în folosul persoanei juridice respective de către o persoană aflată sub autoritatea acesteia.

(3) Răspunderea unei persoane juridice în temeiul alineatelor (1) și (2) nu exclude urmărirea penală a persoanelor fizice care sunt implicate ca autori, instigatori, tăinuitori sau complici la săvârșirea infracțiunilor menționate la articolele 2, 3, 4 și 5.

Articolul 9

Sancțiuni împotriva persoanelor juridice

(1) Fiecare stat membru adoptă măsurile necesare pentru a asigura că o persoană juridică trasă la răspundere în temeiul articolului 8 alineatul (1) este pedepsită cu pedepse eficiente, proporționale și disuasive, care includ amenzi penale sau fără caracter penal și pot include și alte sancțiuni precum:

- (a) retragerea dreptului de a beneficia de avantaje publice sau de ajutoare de stat;
- (b) interdicție temporară sau definitivă de a desfășura o activitate comercială;
- (c) punerea sub supraveghere judiciară sau
- (d) o măsură judiciară de lichidare.

(2) Fiecare stat membru adoptă măsurile necesare pentru a asigura că o persoană juridică trasă la răspundere în temeiul articolului 8 alineatul (2) este pedepsită cu pedepse sau măsuri eficiente, proporționale și disuasive.

Articolul 10

Competența

(1) Fiecare stat membru adoptă norme care prevăd că este competent cu privire la infracțiunile menționate la articolele 2, 3, 4 și 5 în cazul în care infracțiunea a fost comisă:

- (a) în tot sau în parte pe teritoriul său sau
- (b) de către unul dintre resortisanții săi sau
- (c) în folosul unei persoane juridice care își are sediul pe teritoriul statului membru respectiv.

(2) Atunci când adoptă norme care prevăd că este competent în conformitate cu alineatul (1) litera (a), fiecare stat membru se asigură că aceasta include cazurile în care:

- (a) autorul săvârșește infracțiunea atunci când este prezent fizic pe teritoriul său, indiferent dacă infracțiunea vizează un sistem informatic situat pe teritoriul său sau
- (b) infracțiunea vizează un sistem informatic situat pe teritoriul său, indiferent dacă autorul infracțiunii era sau nu era prezent fizic pe teritoriul său.

(3) Un stat membru care, în temeiul legislației sale, nu procedează încă la extradarea sau predarea propriilor resortisanți, adoptă măsurile necesare pentru stabilirea competenței sale în ceea ce privește infracțiunile prevăzute la articolele 2, 3, 4 și 5 și, după caz, urmărirea penală a acestora, în cazul în care sunt săvârșite de către unul dintre resortisanții săi în afara teritoriului său.

(4) Atunci când o infracțiune intră în competența mai multor state membre și oricare dintre acestea poate urmări penal în mod valabil pe baza aceluiași fapt, statele membre respective cooperează pentru a decide care dintre ele va urmări penal autorii infracțiunii în scopul, dacă este posibil, de a centraliza procedura într-un singur stat membru. În acest scop, statele membre pot apela la orice organ sau mecanism instituit în cadrul Uniunii Europene pentru a facilita cooperarea între autoritățile lor judiciare și coordonarea acțiunilor lor. Se poate ține seama de următorii factori, în această ordine prioritară:

- statul membru este acela pe al cărui teritoriu au fost săvârșite infracțiunile, în conformitate cu alineatul (1) litera (a) și cu alineatul (2);
- statul membru este acela din rândul cărui resortisanți face parte autorul;
- statul membru este acela în care a fost descoperit autorul.

(5) Un stat membru poate decide să nu aplice sau să aplice numai în situații sau circumstanțe speciale normele de competență enunțate la alineatul (1) literele (b) și (c).

(6) Atunci când decid să aplice alineatul (5), statele membre informează Secretariatul General al Consiliului și Comisia precizând, după caz, situațiile sau circumstanțele speciale în care se aplică decizia.

Articolul 11

Schimbul de informații

(1) În scopul efectuării schimbului de informații referitoare la infracțiunile menționate la articolele 2, 3, 4 și 5 și în conformitate cu normele privind protecția datelor, statele membre iau măsuri pentru utilizarea rețelei existente de puncte de contact operaționale disponibile 24 de ore din 24 și șapte zile pe săptămână.

(2) Fiecare stat membru comunică Secretariatului General al Consiliului și Comisiei punctul de contact desemnat în scopul efectuării schimbului de informații cu privire la infracțiunile referitoare la atacuri împotriva sistemelor informatice. Secretariatul General transmite aceste informații celorlalte state membre.

Articolul 12

Punerea în aplicare

(1) Statele membre iau măsurile necesare pentru a se conforma dispozițiilor prezentei decizii-cadru până la 16 martie 2007.

(2) Până la 16 martie 2007, statele membre transmit Secretariatului General al Consiliului și Comisiei textele dispozițiilor care transpun în legislația lor națională obligațiile care le revin în conformitate cu prezenta decizie-cadru. Până la 16 septembrie 2007, pe baza unui raport întocmit pe baza informațiilor și a unui raport scris prezentat de Comisie, Consiliul verifică în ce măsură statele membre au adus la îndeplinire dispozițiile prezentei decizii-cadru.

Articolul 13

Intrarea în vigoare

Prezenta decizie-cadru intră în vigoare la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 24 februarie 2005.

Pentru Consiliu

Președintele

N. SCHMIT