COMISIA EUROPEANĂ

Bruxelles, 30.9.2010
COM(2010) 517 final

2010/0273 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI

privind atacurile împotriva sistemelor informatice și de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

EXPUNERE DE MOTIVE

1. MOTIVELE ŞI OBIECTIVELE PROPUNERII

Scopul propunerii este de a înlocui Decizia-cadru 2005/222/JAI din 24 februarie 2005 privind atacurile împotriva sistemelor informatice[1]. Decizia-cadru a constituit un răspuns, după cum se menționează în considerentele sale, la obiectivul de îmbunătățire a cooperării între autoritățile judiciare și alte autorități competente, inclusiv poliția și alte servicii specializate de aplicare a legii din statele membre, prin alinierea normelor de drept penal în statele membre în ceea ce privește atacurile împotriva sistemelor informatice. Aceasta a introdus legislație la nivelul UE care să permită urmărirea faptelor penale cum ar fi accesul ilegal la sistemele informatice, interferența ilegală în sisteme și interferența ilegală în date, precum și norme specifice privind răspunderea persoanelor juridice, competența și schimbul de informații. Statelor membre li s-a solicitat să ia măsurile necesare pentru a se conforma dispozițiilor deciziei-cadru până la 16 martie 2007.

La 14 iulie 2008, Comisia a publicat un raport privind punerea în aplicare a deciziei-cadru în cauză[2]. În concluziile raportului, s-a menționat că s-au înregistrat progrese semnificative în majoritatea statelor membre și că nivelul de punere în aplicare a fost relativ bun, dar că, în unele state membre, punerea în aplicare nu a fost încă finalizată. În raport s-a mai precizat că „atacurile recente din Europa, care au avut loc după adoptarea deciziei-cadru, au subliniat apariția mai multor amenințări noi, în special, producerea unor atacuri simultane masive împotriva sistemelor informatice și utilizarea infracțională crescută a așa-numitelor «botnets»”. Aceste atacuri nu au fost în centrul atenției atunci când decizia-cadru a fost adoptată. Ca răspuns la aceste evoluții, Comisia va avea în vedere măsuri care vizează găsirea unor răspunsuri mai eficiente la aceste amenințări (a se vedea secțiunea următoare pentru explicații privind botneturile).

Importanța de a se lua măsuri suplimentare pentru intensificarea luptei împotriva criminalității informatice a fost subliniată în Programul de la Haga din 2004 privind consolidarea libertății, securității și justiției în Uniunea Europeană, precum și Programul de la Stockholm din 2009 și planul de acțiune corespunzător acestuia[3]. În plus, Agenda digitală pentru Europa[4], prezentată recent și care reprezintă prima inițiativă emblematică adoptată în cadrul strategiei Europa 2020, a recunoscut necesitatea de a găsi soluții, la nivel european, la apariția unor noi forme de criminalitate, în special criminalitatea informatică. În acest domeniu de acțiune concentrat pe încredere și securitate, Comisia se angajează să adopte măsuri de combatere a atacurilor împotriva sistemelor informatice.

La nivel internațional, Convenția Consiliului Europei privind criminalitatea informatică („Convenția privind criminalitatea informatică”), semnată la 23 noiembrie 2001, este considerată ca fiind standardul internațional cel mai complet până în prezent, deoarece oferă un cadru cuprinzător și coerent, care acoperă diversitatea aspectelor legate de criminalitatea informatică[5]. Până în prezent, Convenția a fost semnată de toate cele 27 de state membre, dar

---

1 JO L 69, 16.3. 2005, p. 68.

2 Raportul Comisiei către Consiliu în temeiul articolului 12 din Decizia-cadru a Consiliului din 24 februarie 2005 privind atacurile împotriva sistemelor informatice, COM(2008) 448.

3 JO C 198, 12.8. 2005, JO C 115, 4.5.2010, COM(2010) 171, 20.4.2010.

4 Comunicarea Comisiei - COM(2010) 245, 19.5.2010.

5 Convenția Consiliului Europei privind criminalitatea informatică, Budapesta, 23.11.2001, STCE nr. 185.

a fost ratificată de numai 15 dintre acestea[6]. Convenția a intrat în vigoare la 1 iulie 2004. UE nu este semnatară a Convenției. Având în vedere importanța acestui instrument, Comisia va încuraja în mod activ restul statelor membre ale UE să ratifice convenția cât mai curând.

- **Contextul general**

În ceea ce privește criminalitatea informatică, principala cauză a acestui fenomen o reprezintă vulnerabilitatea rezultată din diverși factori. Răspunsul insuficient al mecanismelor de punere în aplicare a legii contribuie la răspândirea acestor fenomene, iar dificultățile iau amploare, deoarece anumite forme de fapte penale transcend frontierele naționale. Raportarea acestui tip de criminalitate este adesea necorespunzătoare, pe de o parte deoarece unele infracțiuni trec neobservate, pe de altă parte deoarece victimele (operatorii economici și societățile) nu raportează infracțiunile de teamă să nu le fie compromisă reputația și să nu le fie afectate perspectivele comerciale prin expunerea publică a vulnerabilităților lor.

În plus, variațiile existente la nivel național în ceea ce privește dreptul penal și procedura penală pot determina diferențe în materie de cercetare și urmărire penală, ceea ce duce la tratarea în mod diferit a acestor infracțiuni. Evoluțiile din domeniul tehnologiei informațiilor au exacerbat aceste probleme prin facilitarea producerii și distribuirii instrumentelor („malware” și „botnet”), oferind totodată anonimitate infractorilor și dispersând responsabilitatea între jurisdicții. Dificultățile asociate declanșării anchetelor permit crimei organizate să obțină profituri considerabile, cu risc scăzut.

Prezenta propunere ia în considerare noile metode de comitere a infracțiunilor informatice, în special utilizarea de botneturi. Termenul „botnet” desemnează o rețea de calculatoare care au fost infectate cu programe ostile (viruși informatici). O astfel de rețea de calculatoare virusate („zombie”) poate fi activată pentru a efectua acțiuni specifice, cum ar fi atacarea sistemelor informatice (atacuri informatice). Aceste „zombie” pot fi controlate - adesea fără cunoștința utilizatorilor calculatoarelor virusate - de un alt calculator, cunoscut și sub numele de „centru de comandă și control”. Persoanele care controlează acest centru se numără printre infractori, deoarece utilizează calculatoarele virusate pentru a lansa atacuri împotriva sistemelor informatice. Autorii sunt foarte dificil de identificat, deoarece locația în care se află calculatoarele care alcătuiesc botnetul și lansează atacul poate fi diferită de cea a autorului.

Atacurile lansate de un botnet sunt adesea realizate la scară largă. Atacurile la scară largă sunt fie atacurile care pot fi lansate prin utilizarea de instrumente care afectează un număr semnificativ de sisteme informatice (calculatoare), fie atacurile care produc daune considerabile, de exemplu, în materie de întrerupere a serviciilor aferente sistemului, costuri financiare, pierderi de date cu caracter personal etc. Daunele cauzate de atacurile la scară largă au un impact major asupra funcționării sistemului-țintă și/sau afectează mediul de lucru al acestuia. În acest context, printr-un „botnet mare” se înțelege un botnet care are capacitatea de a produce daune serioase. Botneturile sunt dificil de definit în termeni de dimensiune, dar s-a estimat că cele mai mari botneturi au între 40 000 și 100 000 de conexiuni (și anume calculatoare infectate) pe interval de 24 de ore[7].

---

6 Pentru a cunoaște stadiul în care se află ratificările Convenției (STCE nr. 185), puteți consulta: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

7 Numărul de conexiuni pe interval de 24 de ore este unitatea de măsură utilizată în mod curent pentru estimarea dimensiunii botneturilor.

- **Dispoziții în vigoare în domeniul propunerii**

La nivelul UE, decizia-cadru introduce un nivel minim de armonizare a legislației statelor membre pentru a incrimina o serie de infracțiuni informatice, inclusiv accesul ilegal la sistemele informatice, interferența ilegală în sisteme și interferența ilegală în date, precum și instigarea, complicitatea și încercarea de a comite aceste infracțiuni.

Cu toate că dispozițiile prevăzute în decizia-cadru au fost în general puse în aplicare de către statele membre, decizia prezintă o serie de deficiențe ca urmare a tendinței în materie de dimensiune și număr de fapte penale (atacuri informatice). Aceasta armonizează legislația doar în ceea ce privește un număr limitat de fapte penale, dar nu propune soluții pentru amenințarea potențială pe care o reprezintă atacurile la scară largă pentru societate. De asemenea, aceasta nu ia suficient în considerare gravitatea infracțiunilor și nu prevede sancțiuni împotriva acestora.

Alte inițiative și programe UE, în vigoare sau planificate, încearcă să soluționeze problemele legate de atacurile sau incidentele informatice, cum ar fi securitatea rețelelor și siguranța utilizatorilor de internet. Acestea includ acțiunile sprijinite de programul „Prevenirea și combaterea criminalității”[8], programul „Justiția în materie penală”[9], programul pentru un internet mai sigur („Safer Internet”[10]) și inițiativa privind infrastructurile critice de informații[11]. În plus față de decizia-cadru, alt instrument juridic relevant în vigoare este Decizia-cadru 2004/68/JAI privind combaterea exploatării sexuale a copiilor și a pornografiei infantile.

La nivel administrativ, practica de infectare a calculatoarelor, transformându-le în botneturi, este deja interzisă în temeiul normelor UE în materie de confidențialitate și de protecție a datelor[12]. În special agențiile administrative naționale cooperează deja în cadrul Rețelei europene de contact a autorităților antispam. Conform acestor norme, statele membre sunt obligate să interzică interceptarea comunicațiilor în rețelele publice de comunicații și a serviciilor de comunicații electronice disponibile public, fără acordul utilizatorilor în cauză sau fără autorizație legală.

Prezenta propunere este conformă acestor norme. Statele membre ar trebui să vizeze îmbunătățirea cooperării dintre autoritățile administrative și cele de aplicare a legii pentru cazurile care fac obiectul atât al sancțiunilor administrative, cât și al celor penale.

- **Coerența cu alte politici și obiective ale Uniunii**

Obiectivele sunt compatibile cu politicile UE privind combaterea criminalității organizate, creșterea rezilienței rețelelor de calculatoare, protejarea infrastructurilor critice de informații și protecția datelor. Acestea sunt coerente și cu programul pentru un internet mai sigur, menit să promoveze utilizarea, în condiții de mai mare siguranță, a internetului și a noilor tehnologii online și să combată conținuturile ilegale.

---

8 A se vedea: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 A se vedea: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm

10 A se vedea: http://ec.europa.eu/information_society/activities/sip/index_en.htm

11 A se vedea: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

12 Directiva asupra confidențialității și comunicațiilor electronice (JO L 201, 31.7.2002), modificată prin Directiva 2009/136/CE (JO L 337, 18.12.2009).

Prezenta propunere a făcut obiectul unei examinări aprofundate pentru a se asigura deplina compatibilitate a dispozițiilor sale cu drepturile fundamentale și, în special, cu protecția datelor cu caracter personal, libertatea de exprimare și de informare, dreptul la un proces echitabil, prezumția de nevinovăție și dreptul la apărare, precum și principiile legalității și proporționalității infracțiunilor și sancțiunilor penale.

2. CONSULTAREA PĂRȚILOR INTERESATE ȘI EVALUAREA IMPACTULUI

- **Consultarea părților interesate**

O gamă largă de experți în domeniu au fost consultați în cadrul unei serii de reuniuni diverse care au abordat diferite aspecte ale luptei împotriva criminalității informatice, inclusiv acțiunile judiciare (urmărire penală) ca urmare a acestor infracțiuni. Printre aceștia s-au numărat, în special, reprezentanți ai sectoarelor public și privat ale statelor membre, judecători specializați și procurori, organizații internaționale, agenții europene și grupuri de experți. O serie de experți și organizații au transmis ulterior observații și au furnizat informații.

Principalele concluzii reținute în urma consultărilor sunt:

– necesitatea ca UE să acționeze în acest domeniu;

– necesitatea incriminării unor forme de fapte penale care nu sunt incluse în actuala decizie-cadru, în special noi forme de atacuri informatice (botneturi);

– necesitatea eliminării obstacolelor din calea cercetării și urmăririi penale a cazurilor transfrontaliere.

Contribuțiile primite pe parcursul consultărilor au fost luate în considerare în evaluarea impactului.

Obținerea și utilizarea expertizei

Expertiza externă a fost obținută pe parcursul diferitelor reuniuni cu părțile interesate.

Evaluarea impactului

Au fost examinate diferite opțiuni de politică, ca mijloace de atingere a obiectivului.

- Opțiunea de politică (1): Status quo/nicio acțiune nouă din partea UE

Această opțiune presupune că UE nu va lua nicio măsură suplimentară pentru a combate acest tip specific de criminalitate informatică, și anume atacurile împotriva sistemelor informatice. Acțiunile în curs urmează să fie continuate, în special programele de consolidare a protecției infrastructurilor critice de informații și de îmbunătățire a cooperării dintre sectorul public și cel privat împotriva criminalității informatice.

- Opțiunea de politică (2): elaborarea unui program de consolidare a eforturilor de contracarare a atacurilor împotriva sistemelor informatice prin intermediul unor măsuri fără caracter legislativ

Măsurile fără caracter legislativ, în paralel cu programul de protecție a infrastructurilor critice de informații, s-ar concentra pe cooperarea transfrontalieră în materie de aplicare a legii și de

parteneriate public-privat. Aceste instrumente juridice neobligatorii ar trebui să promoveze continuarea acțiunii coordonate la nivelul UE, inclusiv consolidarea rețelei existente, disponibilă 24 de ore din 24 și 7 zile din 7, de puncte de contact pentru autoritățile de aplicare a legii; instituirea unei rețele europene de puncte de contact public-privat, de experți în domeniul criminalității informatice și de autorități de aplicare a legii; elaborarea unui acord UE standard la nivel de servicii privind cooperarea în domeniul aplicării legii cu operatorii din sectorul privat, precum și sprijinirea organizării de programe de formare pentru autoritățile de aplicare a legii în domeniul investigării criminalității informatice.

- Opțiunea de politică (3): actualizarea selectivă a dispozițiilor deciziei-cadru (noua directivă înlocuind actuala decizie-cadru) în vederea abordării amenințării pe care o reprezintă atacurile la scară largă împotriva sistemelor informatice (botneturi) și, în cazul în care acestea sunt comise prin disimularea identității reale a autorului și provocarea de prejudicii deținătorului de drept al identității, a eficienței punctelor de contact ale autorităților de aplicare a legii din statele membre, precum și a lipsei de date statistice privind atacurile informatice.

Această opțiune prevede introducerea unei legislații specifice selective (adică limitate) pentru a preveni atacurile la scară largă împotriva sistemelor informatice. O astfel de reglementare consolidată ar fi însoțită de măsuri fără caracter legislativ în vederea consolidării cooperării transfrontaliere operaționale împotriva unor astfel de atacuri, ceea ce ar facilita punerea în aplicare a măsurilor legislative. Obiectivul acestor măsuri ar fi îmbunătățirea gradului de pregătire, securitate și reziliență al infrastructurilor critice de informații și schimbul de bune practici.

- Opțiunea de politică (4): introducerea unei legislații UE cuprinzătoare împotriva criminalității informatice

Această opțiune ar implica o nouă legislație UE cuprinzătoare. Pe lângă introducerea unor măsuri legislative neobligatorii prevăzută în cadrul opțiunii de politică 2 și actualizarea prevăzută în cadrul opțiunii de politică 3, această opțiune ar aborda și alte probleme juridice legate de utilizarea internetului. Astfel de măsuri ar acoperi nu numai atacurile împotriva sistemelor informatice, dar și probleme cum ar fi criminalitatea informatică financiară, conținutul ilegal pe internet, colectarea/stocarea/transferul de probe electronice, precum și norme mai detaliate privind competența. Legislația ar funcționa în paralel cu Convenția Consiliului Europei privind criminalitatea informatică și ar include măsurile de însoțire fără caracter legislativ menționate mai sus.

- Opțiunea de politică (5): actualizarea Convenției Consiliului Europei privind criminalitatea informatică

Această opțiune ar presupune renegocierea substanțială a convenției actuale, ceea ce reprezintă un proces îndelungat și nu este compatibil cu termenele pentru acțiunile propuse în evaluarea impactului. Părțile semnatare, la nivel internațional, nu par dispuse să renegocieze convenția. Prin urmare, actualizarea convenției nu poate fi considerată o opțiune fezabilă, deoarece ar depăși termenul prevăzut pentru acțiune.

Opțiunea de politică preferată: măsuri fără caracter legislativ (opțiunea 2) în paralel cu actualizarea selectivă a deciziei-cadru (opțiunea 3)

În urma analizei impactului economic, a impactului social și a impactului asupra drepturilor fundamentale, opțiunile 2 și 3 reprezintă cea mai bună abordare a problemei și permit atingerea obiectivelor propunerii.

În cadrul elaborării prezentei propuneri, Comisia a realizat o evaluare a impactului.

3. ELEMENTELE JURIDICE ALE PROPUNERII

- **Rezumatul acțiunii propuse**

Directiva abrogă Decizia-cadru 2005/222/JAI, dar, în același timp, va prelua dispozițiile actuale și va include următoarele elemente noi:

– în ceea ce privește dreptul penal material în general, directiva:

A. incriminează producerea, vânzarea, achiziționarea în vederea utilizării, importul, distribuirea sau punerea la dispoziție în alt mod a dispozitivelor/instrumentelor utilizate pentru comiterea faptelor penale.

B. prevede circumstanțe agravante:

- marea amploare a atacurilor - botneturile sau instrumentele similare ar putea fi abordate prin introducerea unei noi circumstanțe agravante, în sensul că faptul de a crea un botnet sau un instrument similar ar constitui un factor agravant în cazul în care se comit infracțiunile enumerate în decizia-cadru existentă;

- în cazul în care aceste atacuri sunt comise prin disimularea identității reale a autorului și provocarea de prejudicii deținătorului de drept al identității. Orice astfel de norme ar trebui să respecte principiile legalității și proporționalității infracțiunilor și sancțiunilor penale și să fie în concordanță cu legislația în vigoare privind protecția datelor cu caracter personal[13].

C. introduce „interceptare ilegală” ca infracțiune penală.

D. introduce măsuri de îmbunătățire a cooperării europene în materie de justiție penală prin consolidarea structurii existente care constă în puncte de contact disponibile 24 de ore din 24 și 7 zile din 7[14]:

- se propune obligația de a da curs unei cereri de asistență de către punctele de contact operaționale (prevăzute la articolul 14 din directivă) într-un anumit termen. Convenția privind criminalitatea informatică nu prevede o astfel de dispoziție obligatorie. Obiectivul acestei măsuri este de a asigura că punctele de

[13] Precum Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), JO L 201, 31.7.2002, p. 37 (în curs de revizuire) și precum directiva generală privind protecția datelor (Directiva 95/46/CE).

[14] Create în temeiul convenției și al DC 2005/222/JAI privind atacurile împotriva sistemelor informatice.

contact indică într-un termen determinat dacă sunt în măsură să ofere o soluție la cererea de asistență și care este intervalul de timp în care punctul de contact care a înaintat cererea poate aștepta găsirea unei astfel de soluții. Conținutul efectiv al soluțiilor nu este specificat.

E. răspunde la necesitatea de a furniza date statistice privind infracțiunile informatice, impunând statelor membre obligația de a asigura instituirea unui sistem adecvat pentru înregistrarea, producerea și furnizarea de date statistice cu privire la faptele penale menționate în decizia-cadru existentă și la „interceptarea ilegală", adăugată recent.

În definițiile infracțiunilor enumerate la articolele 3, 4, 5 (accesul ilegal la sistemele informatice, afectarea integrității unui sistem și interceptarea ilegală), directiva conține o dispoziție care permite doar incriminarea „cazurilor care nu sunt minore" în procesul de transpunere a directivei în legislația națională. Acest element de flexibilitate este menit să permită statelor membre să nu acopere cazuri care ar fi *in abstracto* acoperite de definiția de bază, dar care sunt considerate a nu aduce prejudicii interesului juridic, de exemplu în acte specifice comise de tineri care încearcă să își dovedească expertiza în tehnologia informației. Această posibilitate de limitare a domeniului de incriminare nu ar trebui totuși să ducă la introducerea unor elemente constitutive suplimentare de fapte penale pe lângă cele deja incluse în directivă, deoarece aceasta ar determina acoperirea exclusivă a faptelor penale comise în circumstanțe agravante. În procesul de transpunere, statele membre ar trebui să evite în special adăugarea unor elemente constitutive suplimentare la faptele penale de bază, ca de exemplu o intenție specială de a obține câștiguri ilicite din infracțiuni sau prezența unui efect specific, precum cauzarea unui prejudiciu considerabil.

- **Temeiul juridic**

Articolul 83 alineatul (1) din Tratatul privind funcționarea Uniunii Europene[15].

- **Principiul subsidiarității**

Principiul subsidiarității se aplică în cazul acțiunilor Uniunii Europene. Obiectivele propunerii nu pot fi realizate într-o măsură suficientă de statele membre din următoarele motive:

Criminalitatea informatică și, mai precis, atacurile împotriva sistemelor informatice au o dimensiune transfrontalieră considerabilă, ceea ce este valabil în mod foarte clar în cazul atacurilor la scară largă, deoarece elementele de conectare ale unui atac sunt adesea situate în locații și țări diferite. Acest lucru necesită acțiune din partea UE, în special pentru a ține pasul cu tendința actuală de lansare a unor atacuri la scară largă în Europa și în lume. Acțiunea la nivelul UE și actualizarea Deciziei-cadru 2005/222/JAI au fost evocate și în concluziile Consiliului din noiembrie 2008[16], deoarece obiectivul de a proteja în mod eficace cetățenii de infracțiunile informatice nu poate fi realizat în mod satisfăcător doar de statele membre.

Acțiunea la nivelul Uniunii Europene va atinge într-o mai mare măsură obiectivele propunerii, din motivele expuse în continuare:

---

15 JO C 83 din 30.3.2010, p. 49.

16 „ O strategie de lucru concertată și măsuri concrete de combatere a criminalității informatice", Cea de a 2987-a Reuniune a Consiliului JUSTIȚIE și AFACERI INTERNE, 27-28 noiembrie 2008.

Propunerea va armoniza și mai mult dreptul penal material al statelor membre și normele de procedură, fapt ce va avea un impact pozitiv asupra combaterii acestor infracțiuni. În primul rând, este o modalitate de a împiedica instalarea infractorilor în statele membre în care legislația împotriva atacurilor informatice este mai permisivă. În al doilea rând, definițiile comune fac posibil schimbul de informații, precum și culegerea și compararea datelor relevante. În al treilea rând, crește, de asemenea, eficacitatea măsurilor de prevenire la nivelul UE și a cooperării internaționale.

Prin urmare, propunerea respectă principiul subsidiarității.

- **Principiul proporționalității**

Propunerea respectă principiul proporționalității din următorul motiv:

Prezenta decizie-cadru se limitează la minimul necesar pentru atingerea acestor obiective la nivel european, fără a depăși ceea ce este necesar în acest scop, avându-se în vedere

necesitatea acurateței legislației în domeniul penal.

- **Alegerea instrumentelor**

Instrumentul propus: directivă.

Alte mijloace nu ar fi adecvate din următorul motiv:

Temeiul juridic impune o directivă.

Măsurile fără caracter legislativ și autoreglementarea ar îmbunătăți situația în anumite domenii în care punerea în aplicare este crucială. Cu toate acestea, în alte zone în care o nouă legislație este esențială, beneficiile ar fi modeste.

4. IMPLICAȚIILE BUGETARE

Implicațiile propunerii asupra bugetului Uniunii sunt reduse. Peste 90% din cost, estimat la 5 913 000 EUR, va fi suportat de către statele membre și există posibilitatea de a solicita finanțare UE în vederea reducerii costurilor.

5. INFORMAȚII SUPLIMENTARE

- **Abrogarea legislației în vigoare**

Adoptarea propunerii va duce la abrogarea legislației existente.

- **Domeniul teritorial de aplicare**

Prezenta directivă se adresează statelor membre, în conformitate cu tratatele.

2010/0273 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI

privind atacurile împotriva sistemelor informatice şi de abrogare a Deciziei-cadru 2005/222/JAI a Consiliului

PARLAMENTUL EUROPEAN ŞI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcţionarea Uniunii Europene, în special

articolul 83 alineatul (1),

având în vedere propunerea Comisiei Europene[17],

după transmiterea proiectului de act legislativ către parlamentele naţionale,

având în vedere avizul Comitetului Economic şi Social European,

având în vedere avizul Comitetului Regiunilor,

în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Obiectivul prezentei directive constă în armonizarea normelor statelor membre în materie de drept penal în ceea ce priveşte atacurile împotriva sistemelor informatice şi îmbunătăţirea cooperării dintre autorităţile judiciare şi alte autorităţi competente, inclusiv poliţia şi alte servicii specializate de aplicare a legii din statele membre.

(2) Atacurile împotriva sistemelor informatice, în special ca urmare a criminalităţii organizate, constituie o ameninţare din ce în ce mai mare şi se manifestă o îngrijorare crescândă în faţa posibilităţii de atacuri teroriste sau motivate politic împotriva sistemelor informatice care fac parte din infrastructura critică a statelor membre şi a Uniunii. Această situaţie reprezintă o ameninţare la adresa creării unei societăţi informaţionale mai sigure şi a unui spaţiu de libertate, securitate şi justiţie, necesitând, prin urmare, o reacţie la nivelul Uniunii Europene.

(3) Există dovezi în privinţa tendinţei producerii unor atacuri la scară largă tot mai periculoase şi recurente împotriva sistemelor informatice care sunt esenţiale pentru state sau pentru funcţii specifice din sectorul public sau privat. În paralel cu această tendinţă, se dezvoltă instrumente tot mai sofisticate care pot fi utilizate de infractori pentru lansarea de atacuri informatice, de diferite tipuri.

---

17 JO C […][…], […], p. […][…].

(4) 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 directive în statele membre.

(5) Este necesar să se adopte o abordare comună față de elementele constitutive ale infracțiunilor, introducând ca fapte penale de drept comun accesarea ilegală a unui sistem informatic, afectarea integrității unui sistem, afectarea integrității datelor și interceptarea ilegală.

(6) Statele membre ar trebui să prevadă sancțiuni pentru atacurile împotriva sistemelor informatice. Sancțiunile prevăzute în acest scop ar trebui să fie eficace, proporționale și disuasive.

(7) Este necesar să se prevadă sancțiuni mai severe în cazul comiterii unui atac împotriva unui sistem informatic de către o organizație criminală, astfel cum este definită în Decizia-cadru 2008/841/JAI a Consiliului din 24 octombrie 2008 privind lupta împotriva crimei organizate[18], în cazul în care atacul lansat este la scară largă sau fapta este comisă prin disimularea identității reale a autorului și provocarea de prejudicii deținătorului de drept al identității. Este, de asemenea, oportun să se prevadă sancțiuni mai severe atunci când un astfel de atac a cauzat daune grave sau a afectat interese esențiale.

(8) În concluziile sale din 27-28 noiembrie 2008, Consiliul a invitat statele membre și Comisia să elaboreze o nouă strategie, ținând cont de conținutul Convenției Consiliului Europei privind criminalitatea informatică din 2001. Această convenție constituie cadrul juridic de referință în materie de combatere a criminalității informatice, inclusiv a atacurilor împotriva sistemelor informatice. Prezenta directivă se bazează pe convenția menționată anterior.

(9) Având în vedere modurile diferite în care pot fi efectuate atacurile și evoluția rapidă în materie de hardware și software, prezenta directivă face trimitere la „instrumente” care pot fi utilizate în scopul comiterii infracțiunilor prevăzute în prezenta directivă. Instrumentele desemnează, de exemplu, programe ostile, inclusiv botneturi, utilizate pentru a comite atacuri informatice.

(10) Prezenta directivă nu își propune să impună răspundere penală în cazul în care faptele penale sunt comise fără intenția de a săvârși o infracțiune, cum ar fi pentru testarea sau protejarea autorizată a sistemelor informatice.

(11) Prezenta directivă întărește importanța rețelelor, cum ar fi G8 sau rețeaua de puncte de contact, disponibile 24 de ore din 24 și 7 zile din 7, a Consiliul Europei, pentru a face schimb de informații în vederea asigurării acordării de asistență imediată necesară în cercetările sau urmăririle de infracțiuni legate de sisteme și date informatice sau în colectarea de probe în format electronic privind o infracțiune. Având în vedere viteza cu care pot fi realizate atacurile la scară largă, statele membre ar trebui să fie în măsură să răspundă prompt la cererile urgente adresate de această rețea de puncte de contact. Această asistență ar trebui să includă facilitarea sau efectuarea directă a următoarelor măsuri: furnizarea de consultanță tehnică, conservarea datelor, colectarea de probe, furnizarea de informații juridice, precum și localizarea suspecților.

---

[18] JO L 300, 11.11.2008, p. 42.

(12) Este necesar să se culeagă date referitoare la faptele penale care fac obiectul prezentei directive, pentru a se obține o imagine mai completă a problemei la nivelul Uniunii și a se contribui, astfel, la formularea unor răspunsuri mai eficace. În plus, aceste date vor permite agențiilor specializate, precum Europol și Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor să evalueze mai bine amploarea criminalității informatice și gradul de securitate a rețelelor și informațiilor în Europa.

(13) Lacunele și diferențele considerabile existente în legislațiile statelor membre în domeniul atacurilor împotriva sistemelor informatice pot crea obstacole în calea luptei împotriva criminalității organizate și terorismului și pot îngreuna desfășurarea unei cooperări judiciare și polițienești eficace în acest domeniu. Dat fiind caracterul transnațional, care nu ține seama de frontiere, al sistemelor informatice moderne, atacurile împotriva acestor sisteme sunt de natură transfrontalieră, subliniind nevoia urgentă de a se face în continuare demersuri pentru armonizarea legislațiilor penale în acest domeniu. În plus, coordonarea urmăririi penale în cazurile de atacuri împotriva sistemelor informatice ar trebui să fie facilitată de adoptarea Deciziei-cadru 2009/948/JAI a Consiliului privind prevenirea și soluționarea conflictelor de competențe în procedura penală.

(14) Deoarece obiectivele prezentei directive, care asigură sancționarea penală eficace, 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 privind Uniunea Europeană. Prezenta directivă nu depășește ceea ce este necesar pentru a atinge aceste obiective.

(15) Orice date cu caracter personal prelucrate în contextul punerii în aplicare a prezentei directive ar trebui protejate în conformitate cu normele prevăzute de Decizia-cadru 2008/977/JAI a Consiliului din 27 noiembrie 2008 privind protecția datelor cu caracter personal prelucrate în cadrul cooperării polițienești și judiciare în materie penală[19] cu privire la acele activități de prelucrare care intră sub incidența acesteia, precum și de Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date[20].

(16) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute în special de Carta Drepturilor Fundamentale a Uniunii Europene, inclusiv protecția datelor cu caracter personal, libertatea de exprimare și de informare, dreptul la un proces echitabil, prezumția de nevinovăție și drepturile la apărare, precum și principiile legalității și proporționalității infracțiunilor și sancțiunilor. În special, prezenta directivă urmărește să asigure respectarea deplină a acestor drepturi și principii și trebuie transpusă în mod corespunzător.

(17) [În conformitate cu articolele 1, 2, 3 și 4 din Protocolul privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție anexat la Tratatul

---

19 JO L 350, 30.12.2008, p.60.
20 JO L 8, 12.1.2001, p. 1.

privind funcționarea Uniunii Europene, Regatul Unit și Irlanda și-au notificat dorința de a participa la adoptarea și punerea în aplicare a prezentei directive] SAU [Fără a aduce atingere articolului 4 din Protocolul privind poziția Regatului Unit și a Irlandei cu privire la spațiul de libertate, securitate și justiție, Regatul Unit și Irlanda nu vor participa la adoptarea prezentei directive, nu vor avea obligații în temeiul acesteia și nu vor face obiectul aplicării sale].

(18) În conformitate cu articolele 1 și 2 din protocolul referitor la poziția Danemarcei, anexat la Tratatul privind funcționarea Uniunii Europene, Danemarca nu participă la adoptarea prezentei directive și, prin urmare, nu are obligații în temeiul acesteia și nu face obiectul aplicării sale,

ADOPTĂ PREZENTA DIRECTIVĂ:

Articolul 1
Obiect

Prezenta directivă definește infracțiunile în materie de atacuri împotriva sistemelor informatice și instituie norme minime privind sancțiunile pentru aceste fapte. De asemenea, vizează introducerea unor dispoziții comune pentru a preveni astfel de atacuri și a îmbunătăți cooperarea europeană în materie de justiție penală în acest domeniu.

Articolul 2
Definiții

În sensul prezentei Directive, 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 stocate, 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;

(d) „fără a avea dreptul” înseamnă accesare sau afectare a integrității fără autorizarea proprietarului sau a unui alt titular de drepturi asupra sistemului sau a unei părți a acestuia, sau care nu este permisă în temeiul legislației naționale.

Articolul 3

Accesul ilegal la sistemele informatice

Statele membre adoptă măsurile necesare pentru a asigura că accesarea intenționată, fără a avea dreptul, a ansamblului sau a unei părți a unui sistem informatic se pedepsește ca infracțiune, cel puțin în cazurile care nu sunt minore.

Articolul 4

Afectarea integrității unui sistem informatic

Statele membre 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 prin a le face inaccesibile, atunci când fapta este comisă fără a avea dreptul, se pedepsește ca infracțiune, cel puțin în cazurile care nu sunt minore.

Articolul 5

Afectarea integrității datelor

Statele membre adoptă măsurile necesare pentru a asigura că fapta săvârșită intenționat și fără drept, care constă în ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile se pedepsește ca infracțiune, cel puțin în cazurile care nu sunt minore.

Articolul 6

Interceptarea ilegală

Statele membre adoptă măsurile necesare pentru a garanta că interceptarea intenționată, prin mijloace tehnice, de transmisii private de date informatice către un sistem informatic, dinspre acesta sau în interiorul acestuia, inclusiv de emisii electromagnetice provenite de la un sistem informatic care transmit asemenea date informatice, se pedepsește ca infracțiune dacă este comisă fără a avea dreptul.

Articolul 7

Instrumentele utilizate pentru comiterea faptelor penale

Statele membre adoptă măsurile necesare pentru a garanta că se pedepsesc ca infracțiune atunci când sunt comise intenționat și fără a avea dreptul, în vederea comiterii uneia dintre faptele penale menționate la articolele 3-6, producerea, vânzarea, achiziționarea în vederea utilizării, importul, deținerea, distribuirea sau punerea la dispoziție în alt mod a:

(a) unui dispozitiv, inclusiv program de calculator, conceput sau adaptat în principal în scopul comiterii oricăreia dintre faptele menționate la articolele 3-6;

(b) unei parole de calculator, unui cod de acces sau a unor date similare, prin care un întreg sistem informatic sau orice parte a acestuia poate fi accesat(ă),

Articolul 8

Instigarea, participarea, complicitatea și tentativa

1. Statele membre asigură că instigarea, participarea și complicitatea la comiterea uneia dintre infracțiunile menționate la articolele 3- 7 se pedepsește ca infracțiune.

2. Statele membre se asigură că tentativa de comitere a faptelor menționate la articolele 3-6 se pedepsește ca infracțiune.

Articolul 9

Sancțiuni

1. Statele membre iau măsurile necesare pentru a asigura aplicabilitatea unor sancțiuni penale eficace, proporționale și disuasive pentru faptele menționate la articolele 3-8.

2. Statele membre adoptă măsurile necesare pentru a garanta că faptele menționate la articolele 3-7 sunt pasibile de sancțiuni penale privative de libertate având o durată maximă de cel puțin doi ani.

Articolul 10

Circumstanțe agravante

1. Statele membre adoptă măsurile necesare pentru a garanta că faptele menționate la articolele 3-7 sunt pasibile de sancțiuni penale privative de libertate având o durată maximă de cel puțin cinci ani în cazul în care sunt comise în cadrul unei organizații criminale, astfel cum aceasta este definită în Decizia-cadru 2008/841/JAI.

2. Statele membre adoptă măsurile necesare pentru a garanta că faptele menționate la articolele 3-6 sunt pasibile de sancțiuni penale privative de libertate având o durată maximă de cel puțin cinci ani în cazul în care sunt comise prin utilizarea unui instrument conceput pentru a lansa atacuri care afectează o număr semnificativ de sisteme informatice sau atacuri care provoacă pagube considerabile, precum întreruperea serviciilor aferente sistemului, costuri financiare sau pierderi de date cu caracter personal.

3. Statele membre adoptă măsurile necesare pentru a garanta că faptele menționate la articolele 3-6 sunt pasibile de sancțiuni penale privative de libertate având o durată maximă de cel puțin cinci ani în cazul în care sunt comise prin disimularea identității reale a autorului și provocarea de prejudicii deținătorului de drept al identității.

Articolul 11

Răspunderea persoanelor juridice

1. Statele membre adoptă măsurile necesare pentru a se asigura că persoanele juridice pot fi trase la răspundere pentru oricare dintre faptele prevăzute la articolele 3-8, comise spre folosul lor de către orice persoană, acționând fie în nume propriu, fie ca parte a unui organism al persoanei juridice și având o funcție de conducere în cadrul persoanei juridice, în temeiul:

(a) unei împuterniciri din partea persoanei juridice;

(b) unei prerogative de a lua decizii în numele persoanei juridice;

(c) unei prerogative de a exercita controlul în cadrul persoanei juridice.

2. Statele membre adoptă măsurile necesare pentru a garanta că se poate antrena răspunderea juridică a persoanelor juridice în cazul în care, ca urmare a nesupravegherii sau neexercitării controlului, imputabile unei persoane menționate la alineatul (1), a fost posibilă săvârșirea, de către o persoană aflată în subordine, a oricăreia dintre faptele menționate la articolele 3-8, în folosul acelei persoane juridice.

3. Răspunderea persoanelor juridice în temeiul alineatelor (1) și (2) nu exclude procedurile penale îndreptate împotriva persoanelor fizice care sunt autori sau complici la oricare din faptele prevăzute la articolele 3-8.

Articolul 12
Sancțiuni în cazul persoanelor juridice

1. Statele membre iau măsurile necesare pentru a asigura că orice persoană juridică trasă la răspundere în temeiul articolului 11 alineatul (1) este pedepsită prin aplicarea de sancțiuni eficace, proporționale și disuasive, care să includă amenzi penale sau administrative și eventual alte sancțiuni, de exemplu:

(a) excluderea de la dreptul de a primi beneficii publice sau ajutor public;

(b) interdicția temporară sau permanentă de a desfășura activități comerciale;

(c) plasarea sub supraveghere judiciară;

(d) lichidarea judiciară;

(e) închiderea temporară sau permanentă a unităților care au servit la săvârșirea faptei.

2. Statele membre ia măsurile necesare pentru a se asigura că o persoană juridică găsită responsabilă în temeiul articolului 11 alineatul (2) este pedepsită prin aplicarea de sancțiuni sau măsuri eficace, proporționale și disuasive.

Articolul 13
Competența

1. Statele membre adoptă norme care prevăd că sunt competente cu privire la faptele menționate la articolele 3-8 în cazul în care fapta a fost comisă:

(a) integral sau parțial pe teritoriul statului membru respectiv sau

(b) de către resortisanți ai acestora sau o persoană care își are reședința obișnuită pe teritoriul statului membru respectiv sau

(c) în folosul unei persoane juridice care își are sediul pe teritoriul statului membru respectiv.

2. Atunci când adoptă norme care prevăd că sunt competente în conformitate cu alineatul (1) litera (a), statele membre se asigură că acestea includ cazurile în care:

(a) autorul săvârșește fapta atunci când este prezent fizic pe teritoriul statului membru respectiv, indiferent dacă fapta vizează un sistem informatic situat pe teritoriul lor sau

(b) fapta vizează un sistem informatic situat pe teritoriul statului membru respectiv, indiferent dacă autorul faptei era sau nu era prezent fizic pe teritoriul acestuia.

Articolul 14
Schimbul de informații

1. În scopul efectuării schimbului de informații referitoare la faptele menționate la articolele 3-8 și în conformitate cu normele privind protecția datelor, statele membre utilizează rețeaua existentă de puncte de contact operaționale disponibile 24 de ore din 24 și șapte zile pe săptămână. Statele membre se asigură, de asemenea, că dispun de procedurile necesare astfel încât să poată răspunde, în termen de cel mult opt ore, la cererile urgente. Un astfel de răspuns indică, cel puțin, dacă se va răspunde cererii de ajutor, sub ce formă și când.

2. Statele membre informează Comisia cu privire la punctul lor de contact desemnat în scopul efectuării schimbului de informații privind faptele menționate la articolele 3-8. Comisia comunică aceste informații celorlalte state membre.

Articolul 15
Monitorizarea și statisticile

1. Statele membre se asigură că dispun de un sistem adecvat pentru înregistrarea, producerea și furnizarea de date statistice cu privire la faptele menționate la articolele 3-8.

2. Datele statistice menționate la alineatul (1) acoperă, cel puțin, numărul de fapte menționate la articolele 3-8 raportate statelor membre și urmările acestor raportări și indică anual numărul cazurilor raportate care au fost investigate, numărul persoanelor urmărite penal, precum și numărul persoanelor condamnate pentru faptele menționate la articolele 3-8.

3. Statele membre transmit Comisiei datele culese în conformitate cu prezentul articol. De asemenea, statele membre se asigură de publicarea unei revizuiri consolidate a acestor rapoarte statistice.

Articolul 16

Abrogarea Deciziei-cadru 2005/222/JAI

Decizia-cadru 2005/222/CEE se abrogă, fără a se aduce atingere obligațiilor statelor membre privind termenele pentru transpunerea în dreptul intern.

Trimiterile la decizia-cadru abrogată se interpretează ca trimiteri la prezenta directivă.

Articolul 17

Transpunerea

1. Statele membre pun în aplicare actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive în cel târziu [doi ani de la adoptare]. Statele membre comunică de îndată Comisiei textele acelor dispoziții, precum și un tabel de corespondență între dispozițiile respective și prezenta directivă. Atunci când statele membre adoptă dispozițiile respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o asemenea trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

2. Comisiei îi sunt comunicate de către statele membre textele principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 18

Raportarea

1. În [PATRU ANI DE LA ADOPTARE] și la fiecare trei ani după aceea, Comisia prezintă un raport Parlamentului European și Consiliului, care conține propunerile necesare, privind aplicarea prezentei directive în statele membre.

2. Statele membre transmit Comisiei toate informațiile utile pentru întocmirea raportului menționat la alineatul (1). Informațiile includ o descriere detaliată a măsurilor legislative și fără caracter legislativ adoptate pentru aplicarea prezentei directive.

Articolul 19

Intrarea în vigoare

Prezenta directivă intră în vigoare în a douăzecea a zi de la data publicării în *Jurnalul Oficial al Uniunii Europene*.

Articolul 20

Destinatarii

Prezenta directivă se adresează statelor membre, în conformitate cu tratatele.

Adoptată la Bruxelles,

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*