COMISIA EUROPEANĂ

Bruxelles, 30.9.2010
COM(2010) 521 final

2010/0275 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

privind Agenția europeană pentru securitatea rețelelor și a informațiilor (ENISA)

{SEC(2010) 1126}
{SEC(2010) 1127}

EXPUNERE DE MOTIVE

1. CONTEXTUL PROPUNERII

1.1. Context strategic

Agenția europeană pentru securitatea rețelelor și a informațiilor („The European Network and Information Security Agency", denumită în continuare „ENISA") a fost instituită în martie 2004, pentru o perioadă inițială de cinci ani, prin Regulamentul (CE) nr. 460/2004[1], având ca scop principal asigurarea *„[...] unui nivel ridicat și eficient al securității rețelelor informatice și a datelor în [Uniune]*" și dezvoltarea „*[...] unei culturi a securității rețelelor informatice și a datelor în beneficiul cetățenilor, consumatorilor, întreprinderilor și organizațiilor din sectorul public al Uniunii Europene, contribuind astfel la funcționarea normală a pieței interne*." Regulamentul (CE) nr. 1007/2008[2] a prelungit mandatul ENISA până în martie 2012.

Prelungirea mandatului ENISA în 2008 a ocazionat, de asemenea, lansarea unei dezbateri cu privire la direcția generală a eforturilor europene pentru realizarea securității rețelelor și a informațiilor („network and information security" – NIS), la care Comisia a contribuit prin lansarea unei consultări publice privind obiectivele posibile ale unei politici consolidate în materie de NIS la nivelul Uniunii. Această consultare publică s-a derulat din noiembrie 2008 până în ianuarie 2009 şi a adunat aproape 600 de contribuții[3].

La 30 martie 2009, Comisia a adoptat o comunicare privind protecția infrastructurilor critice de informații („Communication on Critical Information Infrastructure Protection" – CIIP)[4], care pune accentul pe protejarea Europei împotriva atacurilor cibernetice şi a perturbărilor sistemelor informatice prin mărirea gradului de pregătire, securitate şi reziliență, cu un plan de acțiune care invită ENISA să joace un rol, în principal de sprijinire a statelor membre. Planul de acțiune a fost aprobat în linii mari în cadrul discuțiilor purtate la Conferința ministerială privind protecția infrastructurilor critice de informații (CIIP) care a avut loc la Tallinn, în Estonia, pe 27 şi 28 aprilie 2009[5]. Concluziile preşedinției Uniunii Europene privind conferința subliniază importanța *„de a profita de sprijinul operațional"* al ENISA; în ele se afirmă că ENISA *„reprezintă un instrument valoros de sprijinire a eforturilor de cooperare în acest domeniu la nivelul Uniunii"* şi se indică necesitatea de a regândi şi de a reformula mandatul agenției *„pentru a pune mai mult accent pe prioritățile şi necesitățile UE; pentru a obține o capacitate de reacție mai flexibilă; pentru a dezvolta aptitudini și competențe,*

---

1 Regulamentul (CE) nr. 460/2004 al Parlamentului European şi al Consiliului din 10 martie 2004 privind instituirea Agenției europene pentru securitatea rețelelor informatice și a datelor (JO L 77, 13.3.2004, p. 1).

2 Regulamentul (CE) nr. 1007/2008 al Parlamentului European şi al Consiliului din 24 septembrie 2008 de modificare a Regulamentului (CE) nr. 460/2004 al Parlamentului European și al Consiliului din 10 martie 2004 privind instituirea Agenției europene pentru securitatea rețelelor informatice și a datelor, în ceea ce privește durata de funcționare a acesteia (JO L 293, 31.10.2008, p. 1.).

3 Raportul de sinteză privind rezultatele consultării publice „Towards a Strengthened Network and Information Security Policy in Europe"" se ataşează sub forma anexei 11 la evaluarea impactului care însoțeşte prezenta propunere.

4 COM(2009) 149, 30.3.2009.

5 Documentul de dezbatere: http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf
Concluziile preşedinției: http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf.

precum şi pentru a consolida eficienţa operaţională a agenţiei şi impactul său general" cu scopul de a face astfel încât agenţia să devină *„un activ permanent pentru fiecare stat membru şi pentru Uniunea Europeană în general."*"

În urma discuţiilor purtate cu ocazia Consiliului Telecomunicaţii din 11 iunie 2009, în cadrul cărora statele membre şi-au exprimat sprijinul în favoarea extinderii mandatului ENISA şi a sporirii resurselor agenţiei în lumina importanţei NIS şi a evoluţiei continue a provocărilor din acest domeniu, dezbaterea a fost finalizată sub preşedinţia suedeză a Uniunii. Rezoluţia Consiliului din 18 decembrie 2009 privind o abordare europeană a securităţii reţelelor şi a informaţiilor (NIS) bazată pe colaborare[6] recunoaşte rolul şi potenţialul ENISA şi *„necesitatea de a continua dezvoltarea acesteia, astfel încât să devină un organism eficient"*. Rezoluţia subliniază, de asemenea, necesitatea de a moderniza şi a consolida agenţia pentru a sprijini Comisia şi statele membre în reducerea decalajului dintre tehnologie şi politică, îndeplinind rolul de centru de expertiză al Uniunii în materie de NIS.

1.2. Contextul general

Tehnologiile informaţiei şi comunicaţiilor (TIC) au devenit axul central al economiei şi societăţii europene în ansamblul său. TIC sunt vulnerabile la ameninţări care nu mai respectă graniţele naţionale şi care au luat noi forme odată cu evoluţia tehnologiei şi a pieţei. Deoarece TIC au caracter mondial, sunt interconectate şi interdependente cu alte infrastructuri, securitatea şi reziliența acestora nu pot fi asigurate prin abordări strict naţionale şi necoordonate. În acelaşi timp, provocările legate de NIS evoluează rapid. Reţelele şi sistemele informatice trebuie protejate eficient împotriva tuturor tipurilor de perturbări şi disfuncţionalităţi, inclusiv împotriva atacurilor omului.

Politicile privind securitatea reţelelor şi a informaţiilor (NIS) joacă un rol central în Agenda digitală pentru Europa[7] (ADE), iniţiativă emblematică în cadrul strategiei UE 2020, având drept obiectiv exploatarea şi mărirea potenţialului TIC şi transformarea acestui potenţial în creştere durabilă şi inovare. Încurajarea adoptării TIC şi sporirea încrederii în societatea informaţională sunt priorităţi absolute ale ADE.

ENISA a fost iniţial creată pentru a asigura un nivel ridicat şi eficace al securităţii reţelelor şi a informaţiilor în interiorul Uniunii. Ţinând cont de experienţa dobândită de agenţie, precum şi de provocările şi de ameninţările actuale, se impune modernizarea mandatul agenţiei pentru ca acesta să răspundă mai bine necesităţilor Uniunii Europene care decurg din:

- fragmentarea abordărilor naţionale în ceea ce priveşte reacţia la noile provocări;
- absenţa unor modele bazate pe colaborare în ceea ce priveşte implementarea politicilor NIS;
- nivelul insuficient de pregătire, datorat de asemenea capacităţii limitate de alertă rapidă şi de reacţie la nivel european;
- lipsa de date fiabile la nivel european şi cunoaşterea limitată a problemelor evolutive;

---

[6] Rezoluţia Consiliului din 18 decembrie 2009 privind o abordare europeană a securităţii reţelelor şi a informaţiilor bazată pe colaborare (JO C 321, 29.12.2009, p. 1). http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

[7] COM(2010) 245, 19.5.2010.

- nivelul redus de conştientizare a riscurilor şi provocărilor în materie de NIS;

- provocarea reprezentată de integrarea aspectelor NIS în politici de combatere mai eficace a criminalității cibernetice.

1.3. Obiectivele de politică

Obiectivul general al propunerii de regulament este de a permite UE, statelor membre şi părților interesate să dezvolte un grad înalt de pregătire şi capacitate de a preveni, detecta şi a răspunde mai bine la problemele din sfera NIS. Aceasta va ajuta la consolidarea încrederii, care stă la baza dezvoltării societății informaționale, la ameliorarea competitivității întreprinderilor europene și la garantarea unei funcționări eficace a pieței interne.

1.4. Dispoziții în vigoare în domeniul propunerii

Prezenta propunere completează inițiative de politică, cu sau fără caracter de reglementare, privind securitatea rețelelor și a informațiilor, luate la nivelul Uniunii în vederea sporirii securității şi a rezilienței TIC:

- Planul de acțiune lansat de comunicarea privind CIIP prevedea crearea a două entități:

    (1) Un forum european al statelor membre, care vizează promovarea discuțiilor şi schimbului de informații privind bunele practici, cu scopul de a stabili obiective de politică şi priorități comune privind securitatea şi reziliența infrastructurii TIC, beneficiind de asemenea în mod direct de pe urma activității şi a sprijinului agenției.

    (2) Un parteneriat european public-privat pentru reziliență (EP3R), care constituie cadrul european flexibil de guvernanță pentru reziliența infrastructurilor TIC şi care operează prin promovarea cooperării între sectorul public şi sectorul privat în ceea ce privește obiectivele de securitate şi reziliență, cerințele de bază, precum și măsurile și bunele practici de politică.

- Programul de la Stockholm, adoptat de Consiliul European la 11 decembrie 2009, promovează politici de asigurare a securității rețelelor, care să permită o reacție mai rapidă în caz de atacuri cibernetice în cadrul Uniunii.

- Aceste inițiative contribuie la punerea în aplicare a Agendei digitale pentru Europa. Politicile privind NIS joacă un rol central în această parte a strategiei care se concentrează pe sporirea încrederii şi a securității în societatea informațională. Ele susțin, de asemenea, măsurile Comisiei de sprijinire şi politica acesteia privind protejarea vieții private (în special „protejarea vieții private din momentul proiectării") şi a datelor cu caracter personal (revizuirea cadrului), rețeaua CPC, gestionarea identității și programul „Safer Internet".

1.5. Evoluții ale politicii NIS actuale în raport cu propunerea

Multe dintre evoluțiile actuale ale politicii NIS, în special cele anunțate în cadrul Agendei digitale pentru Europa, profită de pe urma sprijinului și a expertizei ENISA. Printre acestea se numără:

- Consolidarea cooperării politice în materie de NIS prin intensificarea activităților în cadrul **Forumului european al statelor membre**, care, cu sprijinul direct al ENISA, va contribui la:

  – definirea unor modalități de creare a unei rețele europene eficiente prin intermediul cooperării transfrontaliere între echipele naționale/guvernamentale de intervenție în caz de urgențe informatice („Computer Emergency Response Teams” – CERT);

  – identificarea obiectivelor şi a priorităților pe termen lung pentru exerciții paneuropene la scară largă având ca temă incidente din sfera NIS;

  – promovarea unor cerințe minime referitor la achizițiile publice, pentru consolidarea securității și a rezilienței sistemelor și a rețelelor publice;

  – identificarea unor stimulente de natură economică şi reglementară în favoarea securității și a rezilienței;

  – evaluarea situației din punctul de vedere al NIS în Europa.

- Consolidarea cooperării şi a parteneriatului dintre sectorul public şi cel privat, prin sprijinirea **Parteneriatului public-privat european pentru reziliență (EP3R).** ENISA joacă un rol tot mai mare în facilitarea reuniunilor şi a activităților EP3R. Următoarele activități ale EP3R vor include:

  – Discutarea unor măsuri şi instrumente inovatoare de îmbunătățire a securității şi rezilienței, cum ar fi:

  (1) cerințe de bază în ceea ce privește securitatea şi reziliența, în special în domeniul achizițiilor publice de produse sau servicii TIC, pentru a uniformiza regulile jocului, asigurând în acelaşi timp un nivel adecvat de pregătire şi prevenire;

  (2) explorarea aspectelor legate de răspunderea operatorilor economici, de exemplu atunci când aceştia implementează cerințe minime de securitate;

  (3) stimulente economice în favoarea dezvoltării şi adoptări de practici de gestionare a riscului, de procese şi produse în materie de securitate;

  (4) sisteme de evaluare şi gestionare a riscului, în vederea evaluării şi gestionării incidentelor majore pe o bază comună de înțelegere;

  (5) cooperarea între sectorul privat şi cel public în cazul unor incidente de mare amploare;

  (6) organizarea unui **summit economic** având ca temă factorii economici favorabili și nefavorabili securității și rezilienței.

- Punerea în practică a cerințelor de securitate din pachetul de reglementare privind comunicațiile electronice, domeniu în care expertiza şi asistența ENISA sunt necesare pentru:

– a sprijini statele membre şi Comisia, luând în considerare punctele de vedere ale sectorului privat, după caz, la stabilirea unui cadru de norme şi proceduri de implementare a prevederilor referitoare la notificarea violării securităţii [prevăzută la articolul 13 alineatul (a) din directiva-cadru revizuită].

– a înfiinţa un forum anual al organismelor naţionale competente/autorităţilor naţionale de reglementare pe probleme de NIS şi al părţilor interesate din sectorul privat, pentru a discuta pe marginea lecţiilor învăţate şi a schimba bune practici în ceea ce priveşte aplicarea de măsuri de reglementare în domeniul NIS.

- Facilitarea **exerciţiilor de pregătire în materie de securitate cibernetică la nivelul UE**, cu sprijinul Comisiei şi cu contribuţia ENISA, cu scopul de a extinde astfel de exerciţii la nivel internaţional, într-o etapă ulterioară.

- **Instituirea unei CERT (*Computer Emergency Response Team* – echipă de intervenţie în caz de urgenţe informatice) pentru instituţiile UE**. Acţiunea cheie 6 din Agenda digitală pentru Europa prevede prezentarea de către Comisie „a unor măsuri în vederea instituirii unei politici în domeniul securităţii reţelelor şi informaţiilor consolidate şi de nivel înalt, inclusiv a unor [...] măsuri care să permită o reacţie mai rapidă în caz de atacuri cibernetice, inclusiv a unei echipe CERT pentru instituţiile UE”[8]. Comisia şi celelalte instituţii ale Uniunii Europene vor trebui prin urmare să analizeze şi să înfiinţeze o echipă CERT căreia ENISA îi poate oferi asistenţă tehnică şi expertiză.

- Mobilizarea şi sprijinirea statelor membre pentru completarea şi, dacă este necesar, crearea de echipe **CERT naţionale/guvernamentale, în vederea stabilirii unei reţele performante de echipe CERT care să acopere întreaga Europă**. Această activitate va juca de asemenea un rol esenţial în dezvoltarea în continuare a unui Sistem european de alertă şi schimb de informaţii („European Information Sharing and Alert System” – EISAS) pentru cetăţeni şi IMM-uri, care urmează să fie construit cu resurse şi capacităţi naţionale până la sfârşitul anului 2012.

- **Sensibilizarea** faţă de provocările NIS, care va include:

  – colaborarea Comisiei cu ENISA la elaborarea proiectului de orientări cu privire la promovarea standardelor, a bunelor practici şi a unei culturi de gestionare a riscului în domeniul NIS. Va fi prezentată o primă serie de orientări.

  – organizarea de către ENISA, în colaborare cu statele membre, a **„lunii europene a securităţii reţelelor şi a informaţiilor pentru toţi”**, printre ale cărei manifestări se vor număra concursuri de securitate informatică la nivel naţional/european.

1.6. Coerenţa cu alte politici şi obiective ale Uniunii

Propunerea este în concordanţă cu politicile şi obiectivele existente ale Uniunii Europene şi este în deplină conformitate cu obiectivul de a contribui la buna funcţionare a pieţei interne,

---

[8] Rezoluţia Consiliului din 18 decembrie 2009 privind o abordare europeană a securităţii reţelelor şi a informaţiilor bazată pe colaborare prevedea de asemenea că: *„Consiliul [...] recunoaşte [...] importanţa explorării efectelor strategice, a riscurilor şi a perspectivelor legate de înfiinţarea CERT pentru instituţiile UE şi luarea în calcul a posibilului rol al ENISA în viitor sub acest aspect”.*

prin consolidarea nivelului de pregătire şi reacţie la provocările din sfera securităţii reţelelor şi informaţiilor.

2. REZULTATELE CONSULTĂRILOR ŞI EVALUAREA IMPACTULUI

2.1. Consultarea părţilor interesate

Această iniţiativă politică este rezultatul unor ample discuţii purtate în urma unei abordări incluzive şi cu respectarea principiilor de participare, deschidere, responsabilitate, eficacitate şi coerenţă. Vastul proces care a avut loc a inclus o evaluare a agenţiei în 2006/2007, urmată de recomandările consiliului de administraţie al ENISA, două consultări publice (în 2007 şi în 2008-2009) şi o serie de ateliere de lucru pe probleme legate de NIS.

Prima consultare publică a fost lansată în legătură cu comunicarea Comisiei privind evaluarea intermediară a ENISA. Aceasta s-a axat pe viitorul agenţiei, s-a derulat în perioada 13 iunie - 7 septembrie 2007 şi a adunat un total de 44 de contribuţii on-line, plus alte două prezentate în scris. Răspunsurile au venit din partea mai multor părţi interesate şi implicate, inclusiv din partea ministerelor statelor membre, a organismelor de reglementare, a industriei şi a asociaţiilor de consumatori, a instituţiilor academice, companiilor şi cetăţenilor.

Răspunsurile au evidenţiat o serie de aspecte interesante privind evoluţia scenariului de ameninţare; necesitatea de a clarifica şi de a ameliora flexibilitatea regulamentului pentru a permite ENISA să se adapteze la provocări; importanţa asigurării unei interacţiuni eficiente cu părţile interesate; precum şi posibilitatea unei creşteri limitate a resurselor sale.

Cea de-a doua consultare publică, care s-a derulat din 7 noiembrie 2008 până în 9 ianuarie 2009, a avut ca scop identificarea obiectivelor prioritare ale unei politici consolidate în materie de NIS la nivel european, precum şi a mijloacelor de realizare a acestor obiective. Au fost primite aproape 600 de contribuţii de la autorităţile statelor membre, instituţii academice/de cercetare, asociaţii industriale, companii private şi alte părţi interesate, cum ar fi organizaţii de protecţie a datelor şi de consultanţă, şi de la cetăţeni.

O mare majoritate a respondenţilor[9] a sprijinit prelungirea mandatului agenţiei şi a pledat pentru un rol extins în coordonarea activităţilor NIS la nivel european şi o creştere a resurselor sale. Priorităţile cheie au fost necesitatea unei abordări mai coordonate a ameninţărilor cibernetice în întreaga Europă, cooperarea transnaţională pentru a răspunde la atacuri cibernetice de amploare, construirea încrederii şi îmbunătăţirea schimbului de informaţii între părţile interesate.

S-a efectuat o evaluare a impactului propunerii, începând din septembrie 2009, pe baza unui studiu pregătitor efectuat de un contractant extern. A fost implicat un mare număr de părţi interesate şi experţi. Printre participanţi s-au numărat organisme NIS ale statelor membre, autorităţi naţionale de reglementare, operatori de telecomunicaţii şi furnizori de servicii de internet şi asociaţii profesionale din domeniu, asociaţii ale consumatorilor, producători TIC, echipe CERT, cadre universitare şi întreprinderi utilizatoare. Pentru a sprijini procesul de evaluare a impactului, s-a creat un grup de coordonare la nivel de servicii, alcătuit din direcţiile generale relevante ale Comisiei.

---

[9] A se vedea anexa XI la evaluarea impactului.

2.2. Evaluarea impactului

Menținerea agenției a fost identificată ca fiind soluția adecvată pentru atingerea obiectivelor de politică europene[10]. În urma unui proces de examinare prealabilă, au fost selectate cinci opțiuni de politică în vederea unei analize ulterioare:

- Opțiunea 1 – Nicio politică;
- Opțiunea 2 – Statu-quo, cu alte cuvinte funcționarea în temeiul unui mandat asemănător și dispunând de același nivel al resurselor;
- Opțiunea 3 – Extinderea funcțiilor atribuite ENISA, prin adăugarea de agenții responsabile cu aplicarea legii și protejarea vieții private, cu titlul de părți interesate cu drepturi depline;
- Opțiunea 4 – Adăugarea funcțiilor de combatere a atacurilor cibernetice și de reacție la incidentele informatice;
- Opțiunea 5 – Adăugarea funcțiilor de sprijinire a autorităților judiciare și a autorităților responsabile cu aplicarea legii în combaterea criminalității cibernetice.

În urma unei analize comparative cost-beneficiu, opțiunea 3 a fost identificată ca fiind modalitatea cea mai rentabilă și eficace de realizare a obiectivelor de politică.

Opțiunea 3 prevede extinderea rolului ENISA, punând accentul pe:

- construirea și menținerea unei rețele de legătură între părțile interesate și a unei rețele de cunoștințe pentru a se asigura că ENISA este informată în amănunțime cu privire la peisajul european al NIS;
- funcționarea ca centru de suport NIS pentru dezvoltarea și implementarea politicilor [în special cu privire la protecția vieții private în mediul electronic (e-privacy), semnătura electronică (e-sign), cartea de identitate electronică (e-ID) și standardele privind achizițiile pentru NIS];
- sprijinirea politicii UE referitoare la CIIP și reziliență (de exemplu prin exerciții, EP3R, Sistemul european de alertă și schimb de informații etc.);
- crearea unui cadru UE pentru colectarea datelor NIS, inclusiv dezvoltarea de metode și practici de raportare juridică și de partajare;
- studierea aspectelor economice legate de NIS;
- stimularea cooperării cu țări terțe și cu organizații internaționale pentru a promova o abordare globală comună a NIS și pentru a asigura impactul inițiativelor internaționale de înalt nivel în Europa;
- desfășurarea de activități neoperaționale legate de aspectele NIS din sfera aplicării legii în domeniul criminalității cibernetice și al cooperării judiciare.

[10] A se vedea anexa IV la evaluarea impactului.

3. ELEMENTELE JURIDICE ALE PROPUNERII

3.1. Rezumatul acțiunii propuse

Regulamentul propus vizează consolidarea şi modernizarea Agenției europene pentru securitatea rețelelor și a informațiilor („European Network and Information Security Agency" - ENISA) şi stabilirea unui nou mandat pentru o perioadă de cinci ani.

Propunerea include anumite modificări importante față de regulamentul inițial:

(1) **Mai multă flexibilitate, adaptabilitate şi capacitate de concentrare**. Sarcinile sunt actualizate şi reformulate în linii mari, în scopul de a oferi un domeniu mai larg de aplicare activităților agenției; ele sunt suficient de precise pentru a descrie mijloacele prin care trebuie atinse obiectivele. Acest fapt delimitează mai bine misiunea agenției, îmbunătățește capacitatea sa de a își atinge obiectivele şi consolidează sarcinile sale de sprijinire a implementării politicilor Uniunii.

(2) **O aliniere mai bună a agenției la procesul politic și de reglementare al Uniunii**. Instituțiile şi organismele europene se pot adresa agenției pentru asistență şi consultanță. Acest lucru este în concordanță cu evoluțiile politice şi de reglementare: Consiliul a început să se adreseze direct agenției în rezoluții, iar Parlamentul European şi Consiliul au alocat agenției sarcini legate de securitatea rețelelor și a informațiilor în contextul cadrului de reglementare privind comunicațiile electronice.

(3) **Interfața cu lupta împotriva criminalității cibernetice**. La realizarea obiectivelor sale, Agenția ține cont de lupta împotriva criminalității cibernetice. Autoritățile responsabile cu aplicarea legii şi cu protejarea vieții private devin părți interesate cu drepturi depline ale agenției, în special în cadrul Grupului permanent al părților interesate.

(4) **O structură de guvernanță consolidată**. Propunerea consolidează rolul de supraveghere al consiliului de administrație al agenției, în cadrul căruia sunt reprezentate statele membre şi Comisia. De exemplu, consiliul de administrație este capabil să adreseze orientări generale cu privire la chestiuni legate de personal, anterior responsabilitatea exclusivă a directorului executiv. El poate de asemenea institui organisme de lucru care să îl asiste la îndeplinirea sarcinilor sale, inclusiv la monitorizarea implementării deciziilor sale.

(5) **Eficientizarea procedurilor.** Procedurile care s-au dovedit a fi inutil de împovărătoare sunt simplificate. Exemple: a) simplificarea procedurii privind regulile interne ale consiliului de administrație, (b) avizul privind programul de activitate al ENISA este emis de serviciile Comisiei, și nu printr-o decizie a Comisiei. Consiliul de administrație primește, de asemenea, resursele adecvate, în cazul în care acesta trebuie să ia decizii executive şi apoi să le implementeze (de exemplu, în cazul în care un membru al personalului depune o plângere împotriva directorului executiv sau a consiliului însuși).

(6) **Mărirea treptată a resurselor**. În scopul de a face față priorităților consolidate ale Europei şi provocărilor tot mai mari, fără a aduce atingere propunerii Comisiei privind următorul cadru financiar multianual, se prevede creşterea treptată a resurselor financiare şi umane ale agenției între 2012 şi 2016. Pe baza propunerii Comisiei privind regulamentul de stabilire a cadrului financiar multianual după anul 2013 şi

ținând cont de concluziile evaluării impactului, Comisia va prezenta fişa financiară legislativă modificată.

(7) **Opțiunea de prelungire a mandatului directorului executiv**. Consiliul de administrație poate prelungi durata mandatului directorului executiv cu trei ani

3.2. Temeiul juridic

Temeiul juridic al prezentei propuneri este articolul 114 din Tratatul privind funcționarea Uniunii Europene[11] (TFUE).

În conformitate cu hotărârea Curții Europene de Justiție[12], înainte de intrarea în vigoare a Tratatului de la Lisabona **articolul 95 din Tratatul CE** trebuia considerat temeiul juridic adecvat pentru crearea unui organism în scopul asigurării unui nivel ridicat şi eficient al NIS în cadrul Uniunii. Prin utilizarea expresiei „măsurile privind apropierea" în articolul 95, autorii tratatului au dorit să confere legiuitorului Uniunii o marjă de libertate în ceea ce privește alegerea măsurilor adecvate pentru atingerea rezultatului dorit. Întărirea securității şi a rezilienței infrastructurilor TIC este prin urmare un element important care contribuie la buna funcționare a pieței interne.

În temeiul Tratatului de la Lisabona, **articolul 114 din TFUE[13]** descrie – în termeni aproape identici - responsabilitatea cu privire la piața internă. Din motivele expuse mai sus, acesta va continua să reprezinte temeiul juridic aplicabil pentru adoptarea de măsuri de îmbunătățire a NIS. Responsabilitatea pieței interne este acum o competență partajată între Uniune şi statele membre [articolul 4 alineatul (2) litera (a) din TFUE]. Acest lucru înseamnă că Uniunea şi statele membre pot adopta măsuri (obligatorii) şi că statele membre vor acționa în cazul în care Uniunea nu şi-a exercitat competența sau a hotărât să nu mai acționeze [articolul 2 alineatul (2) din TFUE].

Măsurile luate în temeiul responsabilității pieței interne vor necesita procedura legislativă ordinară (articolele 289 şi 294 din TFUE), care este similară[14] cu vechea procedură de codecizie (articolul 251 din Tratatul CE).

Odată cu Tratatul de la Lisabona, fosta distincție între piloni a dispărut. Prevenirea şi combaterea criminalității a devenit o competență partajată a Uniunii. Acest lucru a creat pentru ENISA oportunitatea de a juca rolul de platformă în ceea ce privește aspectele NIS ale luptei împotriva criminalității cibernetice şi de a face schimb de opinii şi de bune practici cu autoritățile de apărare împotriva atacurilor cibernetice, autoritățile responsabile cu aplicarea legii şi cu cele responsabile cu protejarea vieții private.

3.3. Principiul subsidiarității

Propunerea respectă principiul subsidiarității: politica în domeniul NIS necesită o abordare bazată pe colaborare, iar obiectivele propunerii nu pot fi realizate de către statele membre în mod individual.

---

11 JO C 115, 9.5.2008, p. 94.

12 CEJ 2.5.2006, C-217/04, Regatul Unit al Marii Britanii şi al Irlandei de Nord / Parlamentul European şi Consiliul Uniunii Europene.

13 Cf. mențiunea de mai sus.

14 Procedura legislativă ordinară diferă în special în ceea ce privește cerințele de întrunire a majorității în Consiliu şi PE.

O strategie de completă neintervenție a Uniunii în politicile naționale din domeniul NIS ar lăsa sarcina la latitudinea statelor membre, fără a ține cont de interdependența clară dintre sistemele informatice existente. O măsură de asigurare a unui grad adecvat de coordonare între statele membre care să garanteze că riscurile din sfera NIS pot fi gestionate corespunzător în contextul transfrontalier în care apar acestea respectă, prin urmare, principiul subsidiarității. În plus, acțiunea la nivel european ar îmbunătăți eficacitatea politicilor existente la nivel național, conferind astfel valoare adăugată.

În plus, instituirea unei politici NIS concertate şi de colaborare va avea un impact benefic asupra protecției drepturilor fundamentale şi în special a dreptului la protecția datelor cu caracter personal şi a vieții private. Necesitatea de a proteja datele este esențială în prezent, dat fiind că cetățenii europeni își încredințează din ce în ce mai des datele personale unor sisteme informatice complexe, fie din proprie inițiativă, fie din necesitate, fără a avea neapărat capacitatea de a evalua corect riscurile aferente legate de protecția datelor. Prin urmare, când vor avea loc incidente, aceştia nu vor fi probabil capabili să ia măsuri adecvate, după cum nu există certitudinea că statele membre vor putea soluționa cu eficacitate vreun incident internațional în absența unei coordonări în materie de NIS la nivel european.

3.4. Principiul proporționalității

Prezenta propunere respectă principiul proporționalității, deoarece nu depăşeşte ceea ce este necesar pentru atingerea obiectivului său.

3.5. Alegerea instrumentelor

Instrumentul propus: un regulament care se aplică direct în toate statele membre.

4. IMPLICAȚIILE BUGETARE

Propunerea va avea implicații asupra bugetului Uniunii.

Deoarece sarcinile care urmează să fie incluse în noul mandat al ENISA sunt stabilite, se anticipează că agenția va primi resursele necesare pentru a își desfăşura activitățile în mod satisfăcător. Evaluarea agenției, amplul proces de consultare cu părțile interesate la toate nivelurile şi evaluarea impactului arată un acord general cu privire la faptul că dimensiunea agenției se află sub masa critică şi că este necesară o creştere a resurselor. Consecințele şi efectele unei creşteri a personalului şi a bugetului agenției sunt analizate în evaluarea impactului care însoțeşte propunerea.

Finanțarea UE după 2013 va fi examinată în cadrul unei dezbateri la nivelul Comisiei privind toate propunerile pentru perioada de după 2013.

5. OBSERVAȚII SUPLIMENTARE

5.1. Durată

Regulamentul va acoperi o perioadă de cinci ani.

5.2. Clauza de reexaminare

Regulamentul prevede o evaluare a agenției, care acoperă intervalul de timp scurs de la evaluarea anterioară din 2007. Aceasta va evalua eficacitatea agenției în îndeplinirea obiectivelor sale conform prevederilor regulamentului, măsura în care agenția reprezintă încă un instrument eficace şi dacă durata de funcționare a agenției trebuie prelungită din nou. Pe baza constatărilor, consiliul de administrație va face recomandări Comisiei cu privire la modificarea prezentului regulament, a agenției şi a metodelor sale de lucru. Pentru a permite Comisiei să elaboreze o propunere de prelungire a mandatului în timp util, evaluarea va trebui să se facă până la sfârşitul celui de-al doilea an al mandatului prevăzut de regulament.

5.3. Măsuri provizorii

Comisia este conştientă de faptul că procedura legislativă din cadrul Parlamentului European şi al Consiliului poate necesita un timp îndelungat pentru dezbaterea chestiunilor legate de propunere şi că există riscul unui vid legislativ în cazul în care noul mandat al Agenției nu este adoptat în timp util, înainte de expirarea actualului mandat. Prin urmare, Comisia propune, pe lângă prezenta propunere, un regulament de prelungire a mandatului actual al agenției cu 18 luni pentru a acorda suficient timp pentru dezbateri şi derularea procedurilor.

2010/0275 (COD)

Propunere de

REGULAMENT AL PARLAMENTULUI EUROPEAN ŞI AL CONSILIULUI

privind Agenția europeană pentru securitatea rețelelor și a informațiilor (ENISA)

PARLAMENTUL EUROPEAN ŞI CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind funcționarea Uniunii Europene, în special articolul 114,

având în vedere propunerea Comisiei Europene,

având în vedere avizul Comitetului Economic şi Social European[15],

având în vedere avizul Comitetului Regiunilor[16],

după transmiterea propunerii către parlamentele naționale,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Comunicațiile, infrastructurile și serviciile electronice au devenit un factor esențial în dezvoltarea economică și socială. Ele joacă un rol vital pentru societate şi au devenit elemente la fel de indispensabile ca aprovizionarea cu energie electrică sau cu apă. Perturbarea lor are potențialul de a provoca daune economice considerabile, subliniind importanța măsurilor de creştere a protecției și a rezilienței menite să asigure continuitatea serviciilor critice. Securitatea comunicațiilor, a infrastructurii şi a serviciilor electronice, în special integritatea şi disponibilitatea lor, se confruntă cu provocări din ce în ce mai mari. Acest lucru reprezintă o preocupare crescândă pentru societate, nu în ultimul rând din cauza unor posibile probleme cauzate de complexitatea sistemelor, accidente, erori şi atacuri care pot avea consecințe pentru infrastructura fizică care furnizează servicii esențiale pentru bunăstarea cetățenilor europeni.

(2) Peisajul amenințărilor este în continuă schimbare, iar incidentele de securitate pot pune în pericol încrederea utilizatorilor. Perturbările grave ale comunicațiilor, infrastructurii şi serviciilor electronice pot avea un impact economic şi social major, însă și încălcările și problemele de securitate şi neplăcerile de zi cu zi au de asemenea potențialul de a eroda încrederea publicului în tehnologie, rețele şi servicii.

---

15 OJ C , , p. .

16 OJ C , , p. .

(3) Evaluarea periodică a securității rețelelor şi informațiilor în Europa, pornind de la date la nivel european fiabile, este prin urmare importantă pentru factorii de decizie politică, industrie şi utilizatori.

(4) Reprezentanții statelor membre, reuniți în cadrul Consiliului European din 13 decembrie 2003, au decis ca Agenția europeană pentru securitatea rețelelor și a informațiilor („European Network and Information Security Agency" – ENISA), care urma să fie instituită pe baza propunerii prezentate de Comisie, să aibă sediul într-un oraş din Grecia care urmează să fie stabilit de guvernul elen.

(5) În 2004, Parlamentul European şi Consiliul au adoptat Regulamentul (CE) nr. 460/2004[17] privind instituirea Agenției europene pentru securitatea rețelelor informatice și a datelor, cu scopul de a contribui la obiectivele de asigurare a unui nivel ridicat al securității rețelelor şi a informațiilor în cadrul Uniunii şi la dezvoltarea unei culturi a securității rețelelor şi a informațiilor în beneficiul cetățenilor, al consumatorilor, al întreprinderilor şi al administrațiilor publice. În 2008, Parlamentul European şi Consiliul au adoptat Regulamentul (CE) nr. 1007/2008[18], prelungind mandatul agenției până în martie 2012.

(6) În intervalul de timp scurs de la înființarea agenției, provocările legate de securitatea rețelelor şi a informațiilor s-au schimbat, odată cu evoluția tehnologiei, a pieței şi cu schimbările de natură socio-economică; ele au făcut obiectul unor reflecții şi dezbateri continue. Ca reacție la noile provocări, Uniunea şi-a actualizat prioritățile în ceea ce privește politica de securitate a rețelelor și a informațiilor printr-o serie de documente, între care Comunicarea Comisiei din 2006 intitulată „O strategie pentru o societate informațională sigură - Dialog, parteneriat şi responsabilizare"[19], Rezoluția Consiliului din 2007 privind o strategie pentru o societate informațională sigură în Europa[20], comunicarea din 2009 privind protecția infrastructurilor critice de informație - „Protejarea Europei de atacuri cibernetice şi perturbații de amploare: ameliorarea gradului de pregătire, a securității şi a rezilienței"[21], Concluziile președinției conferinței ministeriale privind protecția infrastructurilor critice de informație („Critical Information Infrastructure Protection" – CIIP), Rezoluția Consiliului din 2009 privind o abordare europeană a securității rețelelor şi a informațiilor bazată pe colaborare[22]. A fost recunoscută necesitatea de a moderniza şi a consolida agenția, pentru a contribui cu succes la eforturile depuse de instituțiile europene şi de statele membre pentru dezvoltarea unei capacități europene de a face față provocărilor legate de securitatea rețelelor şi a informațiilor. Mai recent, Comisia a adoptat Agenda digitală pentru Europa[23], cu titlul de inițiativă emblematică în cadrul strategiei Europa 2020. Această agendă cuprinzătoare vizează exploatarea şi promovarea potențialului TIC în scopul de a transforma acest potențial în creştere durabilă şi inovare. Sporirea încrederii în societatea informațională este unul dintre obiectivele cheie ale acestui

---

17 JO L 77, 13.3.2004, p. 1.

18 JO L 293, 31.10.2008, p. 1.

19 COM(2006) 251, 31.5.2006.

20 Rezoluția Consiliului din 22 martie 2007 cu privire la o strategie pentru o societate informațională sigură în Europa (JO C 68, 24.3.2007, p. 1).

21 COM(2009) 149, 30.3.2009.

22 Rezoluția Consiliului din 18 decembrie 2009 privind o abordare europeană a securității rețelelor și a informațiilor bazată pe colaborare (JO C 321, 29.12.2009, p. 1).

23 COM(2010) 245, 19.5.2010

program cuprinzător, care a anunțat o serie de acțiuni ce trebuie întreprinse de Comisie în acest domeniu, inclusiv prezenta propunere.

(7) Măsurile referitoare la piața internă luate în domeniul securității comunicațiilor electronice şi, în mod mai general, al securității rețelelor şi a informațiilor, necesită adoptarea unor tipuri diferite de aplicații tehnice şi organizatorice de către statele membre şi de Comisie. Aplicarea eterogenă a acestor cerințe poate dăuna eficienței şi poate crea obstacole pentru piața internă. Din acest motiv este necesar un centru de expertiză la nivel european care să furnizeze orientări, consiliere şi, atunci când este solicitat, asistență pe probleme legate de securitatea rețelelor şi a informațiilor, pe care statele membre şi instituțiile europene să se poată baza. Agenția poate răspunde acestor nevoi prin dezvoltarea şi menținerea unui nivel ridicat de expertiză şi prin asistența oferită statelor membre, Comisiei şi, în consecință, comunității de afaceri, în scopul de a le ajuta să îndeplinească cerințele legale şi de reglementare legate de securitatea rețelelor şi a informațiilor, contribuind astfel la buna funcționare a pieței interne.

(8) Agenția trebuie să ducă la îndeplinire sarcinile care îi sunt conferite de legislația actuală a Uniunii din domeniul comunicațiilor electronice şi să contribuie, în general, la un nivel sporit de securitate a comunicațiilor electronice, între altele prin furnizarea de expertiză şi consiliere, precum şi prin promovarea schimbului de bune practici.

(9) Directiva 2002/21/CE a Parlamentului European şi a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele şi serviciile de comunicații electronice (directivă-cadru)[24] prevede, de asemenea, că furnizorii de rețele publice de comunicații electronice accesibile publicului sau de servicii de comunicații electronice destinate publicului trebuie să ia măsurile corespunzătoare menite să garanteze integritatea şi securitatea acestora şi introduce cerințe privind notificarea încălcării securității şi a pierderii integrității. Atunci când este cazul, agenția trebuie de asemenea notificată de către autoritățile naționale de reglementare, care trebuie totodată să prezinte Comisiei şi agenției un raport anual de sinteză privind notificările primite şi măsurile întreprinse. Directiva 2002/21/CE invită în același timp agenția să contribuie la armonizarea măsurilor de securitate de natură tehnică şi organizațională adecvate, prin emiterea de avize.

(10) Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității şi comunicațiilor electronice)[25] impune furnizorilor de servicii de comunicații electronice accesibile publicului să ia măsurile tehnice şi organizatorice corespunzătoare pentru a proteja securitatea serviciilor oferite şi impune de asemenea confidențialitatea comunicațiilor şi a datelor de trafic aferente. Directiva 2002/58/CE introduce cerințe referitoare la notificarea și furnizarea de informații cu privire la violarea datelor cu caracter personal pentru furnizorii de servicii de comunicații electronice. De asemenea, ea invită Comisia să consulte agenția cu privire la orice măsuri tehnice de implementare care urmează să fie adoptate în ceea ce priveşte circumstanțele sau formatul cerințelor de informare şi notificare, precum şi procedurile aplicabile acestora. Conform Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995

[24] JO L 108, 24.4.2002, p. 33.
[25] JO L 201, 31.7.2002, p. 37.

privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[26] , statele membre trebuie să stabilească obligația organismului de control de a implementa măsuri tehnice și organizatorice corespunzătoare pentru protecția datelor cu caracter personal împotriva distrugerii accidentale sau ilegale ori a pierderii accidentale, modificării sau divulgării neautorizate ori a accesului neautorizat la acestea, în special în situațiile în care prelucrarea implică transmiterea datelor printr-o rețea, precum și împotriva tuturor celorlalte forme ilegale de prelucrare.

(11) Agenția trebuie să contribuie la un nivel ridicat de securitate a rețelelor și a informațiilor în interiorul Uniunii și la dezvoltarea unei culturi a securității rețelelor și a informațiilor în beneficiul cetățenilor, al consumatorilor, al întreprinderilor și al organizațiilor din sectorul public al Uniunii Europene, contribuind astfel la buna funcționare a pieței interne.

(12) Este necesar să se indice printr-un set de sarcini modul în care agenția trebuie să își realizeze obiectivele, permițându-i în același timp să opereze cu flexibilitate. Sarcinile îndeplinite de agenție trebuie să includă colectarea de informații și date adecvate, necesare pentru efectuarea analizei riscurilor la adresa securității și rezilienței comunicațiilor, infrastructurii și serviciilor electronice și pentru evaluarea, în cooperare cu statele membre, a situației securității rețelelor și a informațiilor în Europa. Agenția trebuie să asigure coordonarea cu statele membre și sporirea cooperării între părțile interesate din Europa, în special prin implicarea în activitățile sale a organismelor naționale competente și a experților în domeniul securității rețelelor și informațiilor din sectorul privat. Agenția trebuie să ofere asistență Comisiei și statelor membre în dialogul lor cu industria, pentru a aborda probleme legate de securitatea produselor hardware și software, contribuind astfel la o abordare bazată pe colaborare a chestiunii securității rețelelor și a informațiilor.

(13) Agenția trebuie să funcționeze ca punct de referință și să instaureze încredere grație independenței sale, calității serviciilor de consultanță acordate și informațiilor diseminate, transparenței procedurilor și metodelor sale de operare, precum și eforturilor depuse în îndeplinirea sarcinilor care îi sunt alocate. Agenția trebuie să se sprijine pe eforturile naționale și ale UE și, prin urmare, să își îndeplinească sarcinile în deplină cooperare cu statele membre și să fie deschisă la contactele cu întreprinderile din sector și cu alte părți interesate relevante. În plus, agenția trebuie să se bazeze pe informațiile primite de la sectorul privat și pe cooperarea cu acesta; ele joacă un rol important în asigurarea securității comunicațiilor, infrastructurilor și serviciilor electronice.

(14) Comisia a lansat Parteneriatul european public-privat pentru reziliență, cu rolul de cadru flexibil de guvernanță la nivel european în favoarea rezilienței infrastructurilor TIC, în care agenția trebui să joace un rol de facilitator, care să reunească părțile interesate din sectorul public și privat pentru a discuta prioritățile de politică publică, dimensiunea economică și de piață a provocărilor și măsurile în favoarea rezilienței infrastructurilor TIC și pentru a identifica responsabilitatea părților interesate.

---

[26] JO L 281, 23.11.1995, p. 31.

(15) Agenția trebuie să ofere consultanță Comisiei prin intermediul avizelor şi al analizelor tehnice şi socio-economice, la cererea Comisiei sau din proprie inițiativă, pentru a contribui la elaborarea politicii în domeniul securității rețelelor şi a informațiilor. Agenția trebuie de asemenea să sprijine statele membre, instituțiile şi organismele europene, la cererea acestora, în eforturile lor de dezvoltare a politicii şi capacității în materie de securitate a rețelelor și a informațiilor.

(16) Agenția trebuie să asiste statele membre şi instituțiile europene în eforturile lor de construire şi sporire a capacității şi pregătirii transfrontaliere de a preveni, detecta, atenua şi răspunde la problemele şi incidentele în materie de securitate a rețelelor şi a informațiilor; în acest sens, agenția trebuie să faciliteze cooperarea între statele membre, precum şi între statele membre şi Comisie. În acest scop, agenția trebuie să joace un rol activ în sprijinirea statelor membre în eforturile lor continue de îmbunătățire a propriei capacități de reacție şi de organizare şi executare de exerciții la nivel național şi european având ca temă incidentele de securitate.

(17) Directiva 95/46/CE reglementează prelucrarea datelor cu caracter personal efectuată în temeiul prezentului regulament.

(18) Pentru a înțelege mai bine provocările din domeniul securității rețelelor şi a informațiilor, agenția trebuie să analizeze riscurile actuale şi pe cele emergente. În acest scop, în cooperare cu statele membre şi, după caz, cu organismele de statistică, agenția trebuie să colecteze informațiile relevante. În plus, agenția trebui să asiste statele membre şi instituțiile şi organismele europene în eforturile lor de a colecta, analiza şi disemina informații referitoare la securitatea rețelelor și a informațiilor.

(19) În desfăşurarea activităților de monitorizare în interiorul Uniunii, agenția trebuie să faciliteze cooperarea dintre Uniune şi statele membre cu privire la evaluarea securității rețelelor şi a informațiilor în Europa şi să contribuie la activitățile de evaluare, în cooperare cu statele membre.

(20) Agenția trebuie să faciliteze cooperarea dintre organismele publice competente ale statelor membre, în special prin sprijinirea dezvoltării şi schimbului de bune practici şi standarde pentru programele de educație şi cele de sensibilizare. Intensificarea schimbului de informații între statele membre va facilita această acțiune. Agenția trebuie de asemenea să sprijine cooperarea între părțile interesate din sectorul public şi privat la nivelul Uniunii, în parte prin promovarea schimbului de informații, a campaniilor de sensibilizare şi a programelor de educație şi formare profesională.

(21) Politicile de securitate eficiente trebuie să se bazeze pe metode de evaluare a riscurilor bine puse la punct, atât în sectorul public cât şi în sectorul privat. Metode şi proceduri de evaluare a riscurilor sunt utilizate la diferite niveluri, fără a exista o practică comună în ceea ce privește aplicarea lor eficientă. Promovarea şi dezvoltarea de bune practici pentru evaluarea riscurilor şi pentru soluții interoperabile de gestionare a riscurilor în cadrul organizațiilor din sectoarele public şi privat vor spori nivelul de securitate al rețelelor şi sistemelor informatice din Europa. În acest scop, agenția trebuie să sprijine cooperarea între părțile interesate din sectorul public şi privat la nivelul Uniunii, facilitând eforturile acestora referitoare la dezvoltarea şi adoptarea de standarde în ceea ce privește gestionarea riscurilor şi securitatea măsurabilă a produselor, sistemelor, rețelelor şi serviciilor electronice.

(22) În activitatea sa, agenția trebuie să înglobeze activități permanente de cercetare, dezvoltare și evaluare tehnică, în special acele activități desfășurate în cadrul diferitelor inițiative de cercetare ale UE.

(23) Atunci când este adecvat și util pentru acoperirea domeniului de competență și îndeplinirea obiectivelor și sarcinilor sale, agenția trebuie să își împărtășească experiența și informațiile cu caracter general cu organismele și agențiile create în temeiul legislației Uniunii Europene, care se ocupă de problema securității rețelelor și a informațiilor.

(24) În activitatea sa de menținere a legăturii cu organismele responsabile cu aplicarea legii, cu privire la aspectele de securitate ale criminalității cibernetice, agenția respectă canalele de informații şi rețelele existente, cum ar fi punctele de contact menționate în Propunerea de directivă a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice și de abrogare a Deciziei-cadru 2005/222/JAI, sau echipa Europol compusă din șefii unităților responsabile cu combaterea criminalității bazate pe tehnologii avansate („Europol Heads of High Tech Crime Units Task Force”).

(25) Pentru a asigura realizarea deplină a obiectivelor sale, agenția trebuie să colaboreze cu autoritățile responsabile cu aplicare legii şi cu cele responsabile cu protejarea vieții private pentru a evidenția şi aborda corect acele aspecte ale combaterii criminalității cibernetice legate de securitatea rețelelor şi a informațiilor. Reprezentanții acestor autorități trebuie să devină părți interesate cu drepturi depline ale agenției şi trebuie să fie reprezentate în cadrul Grupului permanent al părților interesate al agenției.

(26) Problemele de securitate a rețelelor și a informațiilor sunt probleme de dimensiune mondială. Este nevoie de întărirea cooperării internaționale pentru îmbunătățirea standardelor de securitate şi a schimbului de informații şi pentru promovarea unei abordări comune la nivel mondial a problemelor de securitate a rețelelor şi a informațiilor. În acest scop, agenția trebuie să sprijine cooperarea cu țări terțe şi cu organizații internaționale, în cooperare, după caz, cu SEAE.

(27) Îndeplinirea sarcinilor agenției nu trebuie să interfereze, să împiedice sau să se suprapună competențelor conferite următoarelor entități, sau să prevaleze asupra atribuțiilor și sarcinilor acestora: autoritățile naționale de reglementare, conform prevederilor directivelor cu privire la rețelele şi serviciile de comunicații electronice, precum şi Organismul autorităților europene de reglementare în domeniul comunicațiilor electronice (OAREC) instituit prin Regulamentul 1211/2009[27] al Parlamentului European şi al Consiliului şi Comitetului pentru comunicații menționat în Directiva 2002/21/CE, organismele europene de standardizare, organismele naționale de standardizare şi Comitetul permanent instituit prin Directiva 98/34/CE a Parlamentului European şi a Consiliului din 22 iunie 1998 de stabilire a unei proceduri pentru furnizarea de informații în domeniul standardelor, reglementărilor tehnice şi al normelor privind serviciile societății informaționale[28] şi autoritățile de supraveghere ale statelor membre în probleme legate de protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal şi libera circulație a acestor date.

---

27 JO L 337, 18.12.2009, p. 1.

28 JO L 204, 21.7.1998, p. 37.

(28) Pentru a asigura eficacitatea agenției, statele membre și Comisia trebuie să fie reprezentate într-un consiliu de administrație, care trebuie să definească direcția generală a activităților agenției și să se asigure că aceasta își îndeplinește sarcinile în conformitate cu prezentul regulament. Consiliului de administrație trebuie să i se încredințeze competențele necesare pentru stabilirea bugetului, verificarea execuției acestuia, adoptarea normelor financiare adecvate, stabilirea unor proceduri de lucru transparente pentru luarea deciziilor de către agenție, adoptarea programului de activitate al agenției, adoptarea propriilor reguli de procedură și a normele interne de funcționare a agenției, precum și pentru numirea directorului executiv și pentru a decide cu privire la prelungirea sau încetarea mandatului acestuia. Consiliul de administrație trebuie să poată să înființeze organisme de lucru care să îi ofere asistență la îndeplinirea sarcinilor sale; aceste organisme ar putea, de exemplu, să redacteze deciziile consiliului sau să monitorizeze implementarea acestora.

(29) Pentru buna funcționare a agenției este necesar ca numirea directorului executiv să fie făcută pe baza meritelor și aptitudinilor administrative și manageriale atestate, precum și a competenței și experienței relevante în domeniul securității rețelelor și a informațiilor și, de asemenea, este necesar ca directorul executiv să își ducă la îndeplinire atribuțiile în deplină independență în ceea ce privește organizarea funcționării interne a agenției. În acest scop, directorul executiv trebuie să elaboreze o propunere privind programul de activitate al agenției, după consultări prealabile cu serviciile Comisiei, și să ia toate măsurile necesare pentru a asigura îndeplinirea corespunzătoare a programului de activitate al agenției. Directorul executiv trebuie să întocmească în fiecare an un proiect de raport general spre a fi prezentat consiliului de administrație, să elaboreze un proiect de declarație de venituri și cheltuieli estimate ale agenției și să execute bugetul.

(30) Directorul executiv trebuie să aibă opțiunea de a înființa grupuri de lucru ad-hoc pentru a aborda aspecte specifice, în special de natură științifică, tehnică, juridică sau socio-economică. La înființarea grupurilor de lucru ad-hoc, directorul executiv trebuie să solicite și să țină cont de expertiza externă relevantă necesară pentru a permite agenției să aibă acces la informațiile cele mai actualizate disponibile cu privire la provocările în materie de securitate generate de dezvoltarea societății informaționale. Agenția trebuie să garanteze că selecționarea membrilor grupurilor de lucru ad-hoc se realizează în conformitate cu cele mai înalte standarde de competență, ținând cont în mod corespunzător de un echilibru reprezentant – după caz, în funcție de problemele specifice – între administrațiile publice ale statelor membre, sectorul privat, inclusiv industria, utilizatorii, și experții universitari în domeniul securității rețelelor și a informațiilor. De la caz la caz, agenția poate invita să participe la activitățile grupurilor de lucru, dacă este necesar, experți individuali recunoscuți ca fiind competenți în domeniul relevant. Cheltuielile acestora trebuie suportate de agenție, în conformitate cu normele sale interne și cu regulamentele financiare existente.

(31) Agenția trebuie să includă, cu titlul de organism consultativ, un Grup permanent al părților interesate, pentru a asigura un dialog regulat cu sectorul privat, organizațiile de consumatori și alte părți interesate relevante. Grupul permanent al părților interesate, instituit de consiliul de administrație la propunerea directorului executiv, trebuie să se concentreze pe probleme relevante pentru toate părțile interesate și să le aducă în atenția agenției. Atunci când este oportun și în conformitate cu ordinea de zi a ședințelor, directorul executiv poate invita reprezentanți ai Parlamentului European și ai altor organisme pertinente să ia parte la reuniunile grupului.

(32) Agenția funcționează în conformitate cu, respectiv, (i) principiul subsidiarității, asigurând un grad adecvat de coordonare între statele membre pe probleme legate de NIS şi îmbunătățind eficacitatea politicilor naționale, adăugând astfel valoare acestora și (ii) principiul proporționalității, nemergând dincolo de ceea ce este necesar în vederea atingerii obiectivelor stabilite prin prezentul regulament.

(33) Agenția trebuie să aplice legislația relevantă a UE privind accesul public la documente, conform Regulamentului (CE) nr. 1049/2001 al Parlamentului European și al Consiliului[29], și privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, conform Regulamentului (CE) nr. 45/2001 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[30].

(34) În limitele domeniului său de competență, în cadrul obiectivelor și la îndeplinirea sarcinilor sale, agenția trebuie să se conformeze în special dispozițiilor aplicabile instituțiilor europene, precum și dispozițiilor legislațiilor naționale privind tratamentul aplicat documentelor sensibile. Consiliul de administrație trebuie să aibă puterea de a lua o decizie care să permită agenției să trateze informații clasificate.

(35) Pentru a garanta autonomia și independența deplină a agenției, se consideră necesară alocarea unui buget autonom, ale cărui venituri provin în principal din contribuția Uniunii și din contribuții ale țărilor terțe care iau parte la activitățile agenției. Statul membru gazdă sau oricare alt stat membru trebuie să fie autorizat să contribuie în mod voluntar la veniturile agenției. Procedura bugetară a UE rămâne aplicabilă în ceea ce privește toate subvențiile plătibile din bugetul general al Uniunii Europene. De asemenea, Curtea de Conturi trebuie să îndeplinească sarcina de auditare a conturilor.

(36) Agenția trebuie să succeadă ENISA, astfel cum este instituită prin Regulamentul nr. 460/2004. În conformitate cu decizia reprezentanților statelor membre, reuniți sub egida Consiliului European din 13 decembrie 2003, statul membru gazdă trebuie să mențină și să dezvolte măsurile practice actuale pentru a asigura funcționarea neîntreruptă și eficientă a agenției, ținând cont în special de cooperarea și de asistența acordată de agenție Comisiei, statelor membre și organismelor competente ale acestora, altor instituții și organisme ale Uniunii și părților interesate din sectorul public și privat din întreaga Europă.

(37) Agenția trebuie instituită pentru o perioadă limitată de timp. Operațiunile sale trebuie să fie evaluate din perspectiva eficacității în realizarea obiectivelor și a practicilor sale de lucru, pentru a determina în ce măsură obiectivele agenției sunt sau nu valabile în continuare și, pe această bază, dacă durata sa de funcționare trebuie prelungită,

---

[29] Regulamentul (CE) nr. 1049/2001 al Parlamentului European și al Consiliului din 30 mai 2001 privind accesul public la documentele Parlamentului European, ale Consiliului și ale Comisiei (JO L 145, 31.5.2001, p. 43).

[30] Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date (JO L 8, 12.1.2001, p. 1).

ADOPTĂ PREZENTUL REGULAMENT:

SECȚIUNEA 1 DOMENIU DE APLICARE, OBIECTIVE ȘI SARCINI

Articolul 1
Obiect și domeniu de aplicare

1. Prezentul regulament instituie Agenția europeană pentru securitatea rețelelor și a informațiilor („European Network and Information Security Agency” – ENISA, denumită în continuare „agenția”) cu scopul de a contribui la un nivel ridicat de securitate a rețelelor și a informațiilor în cadrul Uniunii, pentru a sensibiliza societatea și a dezvolta o cultură a securității rețelelor și a informațiilor în beneficiul cetățenilor, al consumatorilor, al întreprinderilor și al organizațiilor din sectorul public al Uniunii, contribuind astfel la buna funcționare a pieței interne.

2. Obiectivele și sarcinile agenției nu aduc atingere competențelor statelor membre în domeniul securității rețelelor și a informațiilor și, în orice caz, nu aduc atingere activităților privind securitatea publică, apărarea, securitatea statului (inclusiv bunăstarea economică a statului atunci când sunt în cauză subiecte legate de securitatea statului) și nici activităților statului în domeniul dreptului penal.

3. În sensul prezentului regulament, prin „securitatea rețelelor și a informațiilor” se înțelege capacitatea unei rețele sau a unui sistem informatic de a rezista, la un nivel de încredere dat, la evenimente accidentale sau la acțiuni ilegale sau răuvoitoare care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor stocate sau transmise și a serviciilor conexe oferite sau accesibile prin aceste rețele și sisteme.

Articolul 2
Obiective

1. Agenția asistă Comisia și statele membre la îndeplinirea cerințelor legale și de reglementare referitoare la securitatea rețelelor și a informațiilor din legislația actuală și viitoare a Uniunii, contribuind astfel la buna funcționare a pieței interne.

2. Agenția consolidează pregătirea și capacitatea Uniunii și a statelor membre de a preveni, detecta și a răspunde la problemele și incidentele în materie de securitate a rețelelor și a informațiilor.

3. Agenția dezvoltă și menține un nivel ridicat de expertiză și folosește această expertiză pentru a stimula o cooperare extinsă între actorii din sectorul public și din cel privat.

Articolul 3
Sarcini

1. În sensul dispozițiilor articolului 1, agenția va îndeplini următoarele sarcini:

(a) sprijină Comisia, la cererea acesteia sau din proprie inițiativă, la dezvoltarea politicii în domeniul securității rețelelor și a informațiilor, furnizând(u-i) opinii și avize și realizând analize tehnice și socio-economice, precum și activități pregătitoare pentru elaborarea și actualizarea legislației Uniunii în domeniul securității rețelelor și a informațiilor;

(b) facilitează cooperarea între statele membre, precum şi între statele membre şi Comisie în privința eforturilor transfrontaliere ale acestora de prevenire, detectare şi reacție la incidentele NIS;

(c) asistă statele membre şi instituțiile şi organismele europene în eforturile lor de a colecta, analiza şi disemina date privind securitatea rețelelor şi a informațiilor;

(d) evaluează în mod regulat, în cooperare cu statele membre şi instituțiile europene, situația securității rețelelor şi a informațiilor în Europa;

(e) sprijină cooperarea între organismele publice competente din Europa, în special eforturile acestora de a dezvolta şi face schimb de bune practici şi standarde;

(f) asistă Uniunea Europeană şi statele membre în promovarea utilizării bunelor practici şi standardelor în materie de gestionare a riscului şi securitate pentru produse, sisteme şi servicii electronice;

(g) sprijină cooperarea între părțile interesate din sectorul public şi privat la nivelul Uniunii prin promovarea, printre altele, a schimbului de informații şi a sensibilizării, şi prin facilitarea eforturilor lor de a dezvolta şi adopta standarde în materie de gestionare a riscului şi de securitate a produselor, rețelelor şi serviciilor electronice.

(h) facilitează dialogul şi schimbul de bune practici între părțile interesate din sectorul public şi privat cu privire la probleme legate de securitatea rețelelor şi a informațiilor, inclusiv aspecte ale luptei împotriva criminalității cibernetice; sprijină Comisia la elaborarea de politici care să ia în considerare aspecte legate de securitatea rețelelor şi a informațiilor din cadrul luptei împotriva criminalității cibernetice.

(i) asistă statele membre şi instituțiile şi organismele europene, la cererea acestora, în eforturile lor de a dezvolta capacitatea de reacție, detectare și analiză a problemelor din sfera securității rețelelor şi a informațiilor.

(j) sprijină dialogul şi cooperarea Uniunii Europene cu țările terțe şi cu organizațiile internaționale, în cooperare, după caz, cu SEAE, pentru a promova cooperarea internațională şi o abordare comună la nivel mondial a problemelor de securitate a rețelelor şi a informațiilor.

(k) îndeplinește sarcinile conferite agenției prin acte legislative ale Uniunii.

SECȚIUNEA 2 ORGANIZARE

Articolul 4
Organisme ale agenției

Agenția este compusă din:

(a) un consiliu de administrație;

(b) un director executiv şi personalul agenției; şi

(c) un Grup permanent al părților interesate.

Articolul 5
Consiliul de administrație

1. Consiliul de administrație definește direcția generală de funcționare a agenției și garantează că agenția operează în conformitate cu normele și principiile stabilite în prezentul regulament. De asemenea, consiliul de administrație asigură compatibilitatea activității agenției cu activitățile desfășurate de statele membre și la nivelul UE.

2. Consiliul de administrație adoptă propriul regulament de procedură, în acord cu serviciile competente ale Comisiei.

3. Consiliul de administrație adoptă regulamentul intern de funcționare al agenției, în acord cu serviciile competente ale Comisiei. Aceste norme sunt făcute publice.

4. Consiliul de administrație numește directorul executiv în conformitate cu articolul 10 alineatul (2) și poate revoca directorul executiv. Consiliul de administrație exercită autoritate disciplinară asupra directorului executiv.

5. Consiliul de administrație adoptă programul de activitate al agenției, în conformitate cu articolul 13 alineatul (3) și cu raportul general privind activitățile agenției pentru/în anul precedent, în conformitate cu articolul 14 alineatul (2).

6. Consiliul de administrație adoptă normele financiare aplicabile agenției. Acestea nu se pot abate de la dispozițiile Regulamentului (CE, Euratom) nr. 2343/2002 al Comisiei din 19 noiembrie 2002 privind regulamentul financiar cadru pentru organismele menționate la articolul 185 din Regulamentul (CE, Euratom) nr. 1605/2002 al Consiliului privind regulamentul financiar aplicabil bugetului general al Comunităților Europene[31], cu excepția cazului în care funcționarea agenției impune în mod specific acest lucru, iar Comisia și-a dat acordul în prealabil.

7. Consiliul de administrație, de comun acord cu Comisia, adoptă normele relevante de implementare, în conformitate cu articolul 110 din statutul funcționarilor.

8. Consiliul de administrație poate înființa grupuri de lucru compuse din membri ai săi, care să îl asiste la îndeplinirea funcțiilor, inclusiv la elaborarea deciziilor și la monitorizarea implementării acestora.

9. Consiliul de administrație poate adopta planul multianual de politică a personalului după consultarea serviciilor Comisiei și după ce a informat în mod corespunzător autoritatea bugetară.

Articolul 6
Componența consiliului de administrație

1. Consiliul de administrație este compus dintr-un reprezentant al fiecărui stat membru, din trei reprezentanți numiți de Comisie, precum și din trei reprezentanți fără drept de vot numiți de Comisie, fiecare dintre aceștia reprezentând unul dintre următoarele grupuri:

(a) industria tehnologiei informației și a comunicațiilor;

[31] JO L 357, 31.12.2002, p. 72.

(b) grupuri de consumatori;

(c) experți universitari în domeniul securității rețelelor și a informațiilor.

2. Membrii consiliului și supleanții acestora sunt numiți pe baza nivelului de experiență și expertiză corespunzător în domeniul securității rețelelor și a informațiilor.

3. Durata mandatului reprezentanților grupurilor menționate la alineatul 1 literele (a), (b) și (c) este de patru ani. Acest mandat se poate reînnoi o dată. În cazul în care un reprezentant încetează să mai facă parte din respectivul grup de interes, Comisia numeşte un înlocuitor.

Articolul 7
Președintele consiliului de administrație

Consiliul de administrație alege un președinte și un vicepreședinte dintre membrii săi, pentru o perioadă de trei ani, care poate fi reînnoită. Vicepreședintele îl înlocuiește din oficiu pe președinte în cazul în care acesta din urmă nu își poate exercita prerogativele.

Articolul 8
Reuniuni

1. Reuniunile consiliului de administrație se convoacă de către președinte.

2. Consiliul de administrație se reunește în ședință ordinară de două ori pe an. De asemenea, consiliul se reunește în ședință extraordinară la cererea președintelui sau la cererea a cel puțin o treime din membrii cu drept de vot.

3. Directorul executiv ia parte la ședințele consiliului de administrație fără a avea drept de vot.

Articolul 9
Votul

1. Consiliului de administrație decide printr-o majoritate a membrilor cu drept de vot.

2. Este necesară o majoritate de două treimi din numărul total al membrilor cu drept de vot pentru adoptarea regulamentului de procedură al consiliului de administrație, a regulamentului intern de funcționare al agenției, a bugetului agenției, a programului anual de activitate al agenției, precum și pentru numirea și revocarea directorului executiv.

Articolul 10
Directorul executiv

1. Agenția este condusă de un director executiv care trebuie să fie independent în exercitarea prerogativelor sale.

2. Directorul executiv este numit și eliberat din funcție de către consiliul de administrație. Numirea se efectuează dintr-o listă de candidați propusă de Comisie, pentru o perioadă de cinci ani, pe baza meritelor și a aptitudinilor administrative și de gestionare demonstrate, precum și a competențelor și experienței specifice. Înainte de a fi numit în funcție, candidatul

selecționat de către consiliul de administrație poate primi invitația de a se adresa comisiei competente a Parlamentului European și de a răspunde întrebărilor puse de membrii acesteia.

3. Pe parcursul ultimelor nouă luni dinaintea încetării acestei perioade, Comisia efectuează o evaluare. În cadrul evaluării, Comisia analizează în special:

– rezultatele obținute de directorul executiv;

– îndatoririle și obligațiile agenției în anii următori.

4. Consiliul de administrație, hotărând la propunerea Comisiei, având în vedere raportul de evaluare și numai în acele cazuri în care decizia poate fi justificată de sarcinile și obligațiile agenției, poate să prelungească durata mandatului directorului executiv cu o perioadă care nu depășește trei ani.

5. Consiliul de administrație informează Parlamentul European în legătură cu intenția sa de a prelungi mandatul directorului executiv. În luna care precede prelungirea mandatului său, directorul executiv poate primi invitația de a se adresa comisiei competente a Parlamentului European și de a răspunde întrebărilor puse de membrii acesteia.

6. Dacă mandatul nu este prelungit, directorul executiv rămâne în funcție până la numirea succesorului său.

7. Directorul executiv este responsabil cu:

(a) administrarea curentă a Agenției;

(b) implementarea programului de activitate și a deciziilor adoptate de consiliul de administrație;

(c) asigurarea îndeplinirii sarcinilor agenției în conformitate cu cerințele celor care utilizează serviciile acesteia, în special în ceea ce privește caracterul adecvat al serviciilor furnizate;

(d) toate chestiunile specifice legate de personal, asigurarea respectării orientărilor generale și a deciziilor cu caracter general ale consiliului de administrație;

(e) stabilirea și menținerea contactului cu instituțiile și organismele europene;

(f) stabilirea și menținerea contactului cu comunitatea de afaceri și cu organizațiile consumatorilor, în vederea asigurării unui dialog periodic cu părțile interesate pertinente;

(g) alte sarcini care îi sunt încredințate în virtutea prezentului regulament.

8. După caz și în limita obiectivelor și sarcinilor agenției, directorul executiv poate înființa grupuri de lucru ad-hoc, compuse din experți. Consiliul de administrație trebuie informat în prealabil. Procedurile referitoare în special la componență, la numirea experților de către directorul executiv și la funcționarea grupurilor de lucru ad-hoc se specifică în regulamentul intern de funcționare al agenției.

9. Directorul executiv pune la dispoziția consiliului de administrație personal administrativ de sprijin și alte resurse, ori de câte ori este necesar.

Articolul 11

Grupul permanent al părților interesate

1. Consiliul de administrație instituie un Grup permanent al părților interesate, la propunerea directorului executiv, alcătuit din experți reprezentând părțile interesate relevante, cum ar fi industria tehnologiei informației și a comunicațiilor, grupurile de consumatori, experții universitari în domeniul securității rețelelor și a informațiilor, precum și autoritățile responsabile cu aplicarea legii și autoritățile responsabile cu protejarea vieții private.

2. Procedurile referitoare în special la numărul, componența și numirea membrilor de către consiliul de administrație, la propunerea directorului executiv și la funcționarea grupului se specifică în regulamentul intern de funcționare al agenției și se fac publice.

3. Grupul este prezidat de directorul executiv.

4. Mandatul membrilor grupului este de doi ani și jumătate. Membrii consiliului de administrație nu pot fi membri ai grupului. Personalul Comisiei are dreptul de a participa la reuniunile și activitățile grupului.

5. Grupul acordă consultanță agenției în exercitarea activităților sale. Grupul acordă consultanță în special directorului executiv, în ceea ce privește elaborarea unei propuneri de program de activitate al agenției și asigurarea comunicării cu părțile interesate relevante, referitor la programul de activitate.

SECȚIUNEA 3 FUNCȚIONARE

Articolul 12

Programul de activitate

1. Agenția își desfășoară activitatea în conformitate cu programul său de lucru, care trebuie să conțină toate activitățile sale planificate. Programul de activitate nu împiedică agenția să preia activități neprevăzute care sunt conforme cu obiectivele și sarcinile sale și care se încadrează în limitele bugetului său. Directorul executiv informează consiliul de administrație cu privire la activitățile agenției care nu sunt prevăzute în programul de activitate.

2. Directorul executiv este responsabil cu elaborarea proiectului de program de activitate al agenției, în urma consultării prealabile a serviciilor Comisiei. Înainte de data de 15 martie a fiecărui an, directorul executiv prezintă proiectul programului de activitate pentru anul următor consiliului de administrație.

3. Până la data de 30 noiembrie a fiecărui an, consiliul de administrație adoptă programul de activitate al agenției pentru anul următor, în urma consultării cu serviciile Comisiei. Programul de activitate include o perspectivă multianuală. Consiliul de administrație se asigură că programul de activitate este compatibil cu obiectivele agenției și cu prioritățile legislative și politice ale Uniunii în domeniul securității rețelelor și a informațiilor.

4. Programul de activitate se organizează în conformitate cu principiul gestionării pe activități („Activity-Based Management” – ABM) . Programul de activitate trebuie să conform cu declarația estimativă de venituri și cheltuieli a agenției și cu bugetul agenției pentru același exercițiu financiar.

5. După adoptarea de către consiliul de administrație, directorul executiv trimite programul de activitate Parlamentului European, Consiliului, Comisiei și statelor membre și dispune publicarea acestuia.

Articolul 13
Raportul general

1. În fiecare an, directorul executiv supune consiliului de administrație un proiect de raport general care acoperă toate activitățile agenției din anul precedent.

2. Până la data de 31 martie a fiecărui an, consiliul de administrație adoptă raportul general privind activitățile agenției din anul precedent.

3. După adoptarea de către consiliul de administrație, directorul executiv transmite raportul general al agenției Parlamentului European, Consiliului, Comisiei, Curții de Conturi, Comitetului Economic și Social European și Comitetului Regiunilor și dispune publicarea acestuia.

Articolul 14
Solicitări adresate agenției

1. Solicitările privind consultanța și asistența care se încadrează în obiectivele și sarcinile agenției se adresează directorului executiv și sunt însoțite de referințe care explică chestiunea ce trebuie examinată. Directorul executiv informează consiliul de administrație în legătură cu cererile primite și, la timpul potrivit, cu acțiunile întreprinse ca urmare a cererilor. În cazul în care refuză o solicitare, agenția prezintă justificări.

2. Solicitările menționate la alineatul (1) pot fi adresate de:

(a) Parlamentul European;

(b) Consiliu;

(c) Comisie;

(d) orice organism competent desemnat de un stat membru, cum ar fi o autoritate națională de reglementare, conform definiției de la articolul 2 din Directiva 2002/21/CE.

3. Modalitățile practice de aplicare a alineatelor (1) și (2) – privind în special transmiterea solicitărilor adresate agenției, stabilirea priorităților, urmărirea solicitărilor și informarea consiliului de administrație în legătură cu acestea – se prevăd de către consiliul de administrație în regulamentul intern de funcționare al agenției.

Articolul 15
Declarația de interes

1. Directorul executiv și funcționarii detașați temporar din partea statelor membre întocmesc o declarație scrisă de angajamente și o declarație scrisă indicând absența oricăror interese directe sau indirecte care ar putea aduce atingere independenței lor.

2. Experții externi care participă la grupurile de lucru ad-hoc declară, cu ocazia fiecărei reuniuni, toate interesele care ar putea aduce atingere independenței lor în ceea ce privește punctele înscrise pe ordinea de zi și se abțin de la participarea la dezbaterile referitoare la punctele respective.

Articolul 16
Transparență

1. Agenția se asigură că își desfășoară activitățile la un nivel ridicat de transparență și în conformitate cu articolele 13 și 14.

2. Agenția se asigură că publicului și tuturor părților interesate li se furnizează informații obiective, fiabile și ușor accesibile, în special în ceea ce privește rezultatele activității sale, după caz. De asemenea, agenția face publice declarațiile de interese întocmite de directorul executiv și de funcționarii detașați temporar din partea statelor membre, împreună cu declarațiile de interese ale experților referitoare la punctele înscrise pe ordinea de zi a reuniunilor grupurilor de lucru ad-hoc.

3. Consiliul de administrație, pe baza unei propuneri din partea directorului executiv, poate autoriza părțile interesate să participe ca observatori la unele dintre activitățile agenției.

4. În regulamentul intern de funcționare, agenția stabilește modalitățile practice de implementare a normelor privind transparența menționate la alineatele (1) și (2).

Articolul 17
Confidențialitate

1. Fără să aducă atingere articolului 14, agenția nu divulgă terților informațiile pe care le prelucrează sau pe care le primește și pentru care s-a cerut/solicitat un tratament confidențial.

2. Membrii consiliului de administrație, directorul executiv, membrii Grupului permanent al părților interesate, experții externi care participă la grupurile de lucru ad-hoc și membrii personalului agenției, inclusiv funcționarii detașați temporar din partea statelor membre, intră sub incidența cerințelor de confidențialitate în temeiul articolului 339 din tratat, (chiar și)/inclusiv după încetarea atribuțiilor lor.

3. În regulamentul intern de funcționare, agenția stabilește modalitățile practice de implementare a normelor de confidențialitate menționate la alineatele (1) și (2).

4. Consiliul de administrație poate decide să acorde agenției permisiunea de a trata/lucra cu informații clasificate. În acest caz, consiliul de administrație – în acord cu serviciile competente ale Comisiei – adoptă un regulament intern de funcționare care să aplice principiile de securitate cuprinse în Decizia 2001/844/CE a Comisiei, CECO, Euratom din 29 noiembrie 2001 de modificare a regulamentului său (intern) de procedură[32]. Sunt vizate, între altele, dispozițiile privind schimbul, prelucrarea și stocarea informațiilor/de informații clasificate.

[32] JO L 317, 3.12.2001, p. 1.

Articolul 18
Accesul la documente

1. Regulamentul (CE) nr. 1049/2001 se aplică documentelor deținute de agenție.

2. Consiliul de administrație adoptă modalitățile de implementare a Regulamentului (CE) nr. 1049/2001 în termen de șase luni de la instituirea agenției.

3. Deciziile adoptate de agenție în temeiul articolului 8 din Regulamentul (CE) nr. 1049/2001 pot face obiectul unei plângeri adresate Ombudsmanului sau al unei acțiuni înaintate Curții de Justiție a Uniunii Europene, conform articolelor 228, respectiv 263 din tratat.

SECȚIUNEA 4 DISPOZIȚII FINANCIARE

Articolul 19
Adoptarea bugetului

1. Veniturile agenției constau în contribuția primită de la bugetul UE, contribuții primite de la țările terțe care participă la activitățile agenției în conformitate cu dispozițiile articolului 29 și contribuții primite de la statele membre.

2. Cheltuielile agenției cuprind cheltuielile cu personalul, cheltuieli administrative și de suport tehnic, cheltuieli de infrastructură și operaționale/de exploatare, precum și cheltuielile rezultând din contracte încheiate cu părți terțe.

3. În fiecare an, până cel târziu la data de 1 martie, directorul executiv elaborează un proiect de declarație de venituri și cheltuieli estimate ale agenției pentru următorul an financiar și îl înaintează consiliului de administrație, împreună cu un proiect al schemei de personal.

4. Veniturile și cheltuielile trebuie să fie în echilibru.

5. În fiecare an, pe baza proiectului declarației de venituri și cheltuieli estimate elaborat de directorul executiv, consiliul de administrație adoptă declarația de venituri și cheltuieli estimate ale agenției pentru următorul an financiar.

6. Până cel târziu la data de 31 martie, consiliul de administrație transmite această declarație estimativă, care cuprinde un proiect al schemei de personal, împreună cu proiectul programului de activitate, Comisiei și statelor cu care Uniunea Europeană a încheiat acorduri în conformitate cu articolul 24.

7. Declarația estimativă este înaintată de Comisie Parlamentului European și Consiliului (amândouă denumite în continuare „autoritatea bugetară”), împreună cu proiectul de buget general al Uniunii Europene.

8. Pe baza declarației estimative, Comisia înscrie în proiectul de buget general al Uniunii Europene estimările pe care le consideră necesare în privința schemei de personal și a valorii subvențiilor care urmează să fie acordate de la bugetul general, pe care le prezintă autorității bugetare în conformitate cu articolul 314 din tratat.

9. Autoritatea bugetară autorizează creditarea cu titlu de subvenție acordată agenției.

10. Autoritatea bugetară adoptă schema de personal a agenției.

11. Consiliul de administrație adoptă bugetul agenției și programul de activitate al acesteia. Bugetul agenției devine definitiv după adoptarea definitivă a bugetului general al Uniunii Europene. Dacă este cazul, consiliul de administrație ajustează bugetul agenției şi programul de activitate al acesteia în conformitate cu bugetul general al Uniunii Europene. Consiliul de administrație înaintează bugetul fără întârziere Comisiei și autorității bugetare.

Articolul 20
Combaterea fraudei

1. În lupta împotriva fraudei, corupției și altor activități ilegale se aplică fără restricție dispozițiile Regulamentului (CE) nr. 1073/1999 al Parlamentului European și al Consiliului din 25 mai 1999 privind investigațiile efectuate de Oficiul European de Luptă Antifraudă (OLAF)[33] .

2. Agenția subscrie/aderă la Acordul interinstituțional din 25 mai 1999 dintre Parlamentul European, Consiliul Uniunii Europene şi Comisia Comunităților Europene privind investigațiile interne desfășurate de Oficiul European de Luptă Antifraudă (OLAF)[34] și emite, fără întârziere, dispozițiile corespunzătoare care se aplică tuturor angajaților agenției.

Articolul 21
Execuția bugetului

1. Directorul executiv execută bugetul agenției.

2. Auditorul intern al Comisiei exercită asupra agenției aceleași prerogative ca și asupra serviciilor Comisiei.

3. Până la data de 1 martie a anului următor exercițiului financiar, contabilul agenției transmite contabilului Comisiei conturile provizorii însoțite de raportul privind gestiunea bugetară și financiară a exercițiului financiar. Contabilul Comisiei consolidează conturile provizorii ale instituțiilor și ale organismelor descentralizate în conformitate cu articolul 128 din Regulamentul (CE, Euratom) nr. 1605/2002 al Consiliului din 25 iunie 2002 privind regulamentul financiar aplicabil bugetului general al Comunităților Europene[35] (denumit în continuare „regulamentul financiar general”).

4. După fiecare exercițiu financiar, până cel târziu la data de 31 martie, contabilul Comisiei transmite Curții de Conturi conturile provizorii ale agenției, însoțite de un raport privind gestiunea bugetară și financiară pentru exercițiul financiar în cauză. Raportul privind gestiunea bugetară și financiară pentru exercițiul financiar respectiv este transmis, de asemenea, și autorității bugetare.

5. La primirea observațiilor Curții de Conturi cu privire la conturile provizorii ale agenției, în temeiul articolului 129 din regulamentul financiar general, directorul executiv întocmește

---

33 JO L 136, 31.5.1999, p. 1.
34 JO L 136, 31.5.1999, p. 15.
35 JO L 248, 16.9.2002, p. 1.

conturile definitive ale agenției pe propria sa răspundere și le transmite consiliului de administrație spre avizare.

6. Consiliul de administrație emite un aviz cu privire la conturile definitive ale agenției.

7. Directorul executiv transmite Parlamentului European, Consiliului, Comisiei și Curții de Conturi situația definitivă a conturilor, împreună cu avizul consiliului de administrație, până cel târziu la data de 1 iulie a anului ulterior încheierii fiecărui exercițiu financiar.

8. Directorul executiv publică conturile definitive.

9. Până cel târziu la data de 30 septembrie, directorul executiv transmite Curții de Conturi un răspuns cu privire la observațiile acesteia. Directorul executiv transmite acest răspuns și consiliului de administrație.

10. Directorul executiv prezintă Parlamentului European, la solicitarea acestuia, toate informațiile necesare pentru buna desfășurare a descărcării de gestiune pentru exercițiul financiar în cauză, în conformitate cu dispozițiile articolului 146 alineatul (3) din regulamentul financiar general.

11. La recomandarea Consiliului, Parlamentul European acordă, înaintea datei de 30 aprilie a anului N+2, descărcarea de gestiune directorului executiv în ceea ce privește executarea bugetului pentru anul N.

SECȚIUNEA 5 DISPOZIȚII GENERALE

Articolul 22
Statutul juridic

1. Agenția este un organism al Uniunii. Ea are personalitate juridică.

2. În fiecare stat membru, agenția dispune de cea mai extinsă capacitate juridică acordată persoanelor juridice conform legislației statului membru respectiv. Agenția poate, în special, să achiziționeze sau să înstrăineze bunuri mobile și imobile și să se constituie parte în proceduri judiciare.

3. Agenția este reprezentată de directorul său executiv.

Articolul 23
Personalul

1. Normele şi reglementările aplicabile funcționarilor şi altor categorii de personal al Uniunii Europene se aplică personalului agenției, inclusiv directorului său executiv.

2. În ceea ce privește directorul executiv, consiliul de administrație exercită atribuțiile conferite autorității de desemnare prin statutul funcționarilor, precum cele conferite și autorității împuternicite să încheie contracte prin regimul aplicabil.

3. În ceea ce privește personalul agenției, directorul executiv exercită atribuțiile conferite autorității de desemnare prin statutul funcționarilor, precum și cele conferite autorității împuternicite să încheie contracte conform prin regimul aplicabil.

4. Agenția poate angaja experți naționali detașați de statele membre. Agenția stabilește în regulamentul său intern de funcționare modalitățile practice de implementare a prezentei dispoziții.

Articolul 24
Privilegii și imunități

Protocolul privind privilegiile și imunitățile Comunităților Europene se aplică agenției și personalului acesteia.

Articolul 25
Răspundere

1. Răspunderea contractuală a agenției este reglementată de legislația aplicabilă contractului în cauză.

Curtea de Justiție a Uniunii Europene este competentă să se pronunțe în temeiul oricărei clauze compromisorii cuprinse într-un contract încheiat de agenție.

2. În cazul unei răspunderi necontractuale, agenția, în conformitate cu principiile generale comune legislațiilor statelor membre, acordă reparații pentru toate prejudiciile cauzate de serviciile sau de angajații proprii în timpul/cursul exercitării prerogativelor lor.

Curtea de Justiție este competentă în ceea ce privește toate litigiile privind repararea unor astfel de prejudicii.

3. Responsabilitatea personală a angajaților față de agenție este reglementată de condițiile pertinente care se aplică personalului agenției.

Articolul 26
Limbile

1. Dispozițiile Regulamentului nr. 1 din 15 aprilie 1958 de stabilire a regimului lingvistic al Comunității Economice Europene[36] se aplică agenției. Statele membre și celelalte organisme desemnate de către acestea se pot adresa agenției și pot primi răspunsuri într-una din limbile oficiale ale Uniunii Europene, la alegere.

2. Serviciile de traducere necesare funcționării agenției sunt asigurate de către Centrul de Traduceri pentru Organismele Uniunii Europene.

[36] JO 17, 6.10.1958, p. 385/58. Regulament modificat ultima dată prin Actul de aderare din 1994.

Articolul 27

Protecția datelor cu caracter personal

Atunci când prelucrează date referitoare la persoane fizice, agenția se află sub incidența dispozițiilor Regulamentului (CE) nr. 45/2001.

Articolul 28

Participarea țărilor terțe

1. Agenția este deschisă participării țărilor terțe care au încheiat acorduri cu Uniunea Europeană în temeiul cărora au adoptat și aplicat legislația Uniunii în domeniile reglementate de prezentul regulament.

2. În temeiul dispozițiilor pertinente din aceste acorduri, se încheie înțelegeri care specifică în special natura, măsura și modul în care aceste țări vor participa la activitatea agenției, cuprinzând dispoziții privind participarea la inițiativele întreprinse de agenție, contribuțiile financiare și personalul.

SECȚIUNEA 6 DISPOZIȚII FINALE

Articolul 29

Clauza de reexaminare

1. În termen de trei ani de la data instituirii menționată la articolul 34, Comisia, luând în considerare opiniile tuturor părților interesate relevante, efectuează o evaluare pe baza termenilor de referință convenți cu consiliul de administrație. Evaluarea examinează impactul și eficacitatea agenției în realizarea obiectivelor prevăzute la articolul 2, precum și eficacitatea practicilor de lucru ale agenției. Comisia întreprinde evaluarea îndeosebi în scopul de a determina dacă agenția este în continuare un instrument eficace și dacă durata de funcționare a agenției trebuie prelungită dincolo de perioada specificată la articolul 34.

2. Concluziile evaluării sunt transmise de Comisie Parlamentului European și Consiliului și sunt făcute publice.

3. Consiliul de administrație primește evaluarea și înaintează Comisiei recomandările sale privind modificări ale prezentului regulament, ale agenției și ale practicilor sale de lucru. Consiliul de administrație și directorul executiv trebuie să ia în considerare rezultatele evaluării în planificarea multianuală a agenției.

Articolul 30

Cooperarea statului membru gazdă

Statul membru gazdă a agenției asigură cele mai bune condiții posibile pentru funcționarea corectă și eficientă a agenției.

Articolul 31
Controlul administrativ

Activitățile agenției fac obiectul supravegherii de către Ombudsman, în conformitate cu articolul 228 din tratat.

Articolul 32
Abrogare și succesiune

1. Regulamentul (CE) nr. 460/2004 se abrogă.

Trimiterile la Regulamentul (CE) nr. 460/2004 și la ENISA se interpretează ca trimiteri la prezentul regulament și la agenție.

2. Agenția succede agenției instituite prin Regulamentul (CE) nr. 460/2004 în ceea ce privește toate aspectele legate de proprietate, acorduri, obligații legale, contracte de muncă, angajamente financiare și răspunderi.

Articolul 33
Durată

Agenția se înființează de la [...] pentru o perioadă de cinci ani.

Articolul 34
Intrare în vigoare

Prezentul regulament intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene* și se aplică de la 14 martie 2012 sau din ziua următoare datei publicării, dacă aceasta survine la o dată ulterioară.

Prezentul regulamentul este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la […],

Pentru Parlamentul European	*Pentru Consiliu*
Președintele	*Președintele*

FIŞĂ FINANCIARĂ LEGISLATIVĂ PENTRU PROPUNERI

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de regulament al Parlamentului European şi al Consiliului privind Agenţia europeană pentru securitatea reţelelor şi a informaţiilor („European Network and Information Security Agency" – ENISA)

1.2. Domeniu (domenii) politice vizate în structura ABM/ABB[37]

Societate informațională și media.

Cadru de reglementare pentru Agenda digitală

1.3. Tipul propunerii/inițiativei

☐ Propunerea/inițiativa se referă la o **acțiune nouă**

☐ Propunerea/inițiativa se referă la o **acțiune nouă în urma unui proiect-pilot/acțiuni pregătitoare**[38]

☑ Propunerea/inițiativa se referă la **extinderea unei acțiuni existente**

☐ Propunerea/inițiativa se referă la **o acțiune reorientată spre o nouă acțiune**

1.4. Obiective

1.4.1. Obiectiv(e) strategic(e) multianual(e) ale Comisiei vizat(e) de propunere/inițiativă

Coerența abordărilor în materie de reglementare – furnizarea de orientări şi consilierea Comisiei şi a statelor membre în vederea actualizării şi dezvoltării unui cadru normativ global în domeniul NIS.

Prevenire, detectare şi reacție – îmbunătățirea gradului de pregătire, prin contribuții la capacitatea europeană de alertă rapidă şi de reacție la incidente, prin planuri şi exerciții de urgență paneuropene.

Dezvoltarea cunoştinţelor factorilor de decizie politică – furnizarea de asistență şi consultanță Comisiei şi statelor membre în vederea atingerii unui nivel ridicat de cunoştinţe, pe întreg teritoriul Uniunii, în ceea ce priveşte securitatea reţelelor şi a informațiilor şi aplicarea acesteia la părţile interesate din sector. Sunt incluse, de asemenea, generarea, analizarea şi punerea la dispoziție a datelor cu privire la aspectele economice şi la impactul

[37] ABM (*Activity-Based Management*): gestionarea pe activități (*Activity-Based Budgeting* – ABB): stabilirea bugetului pe activități.

[38] Conform articolului 49 alineatul (6) litera (a) sau (b) din regulamentul financiar.

încălcărilor NIS, factori care stimulează părțile interesate să investească în măsuri în domeniul NIS, în identificarea riscurilor şi a indicatorilor situației NIS în Uniune, etc.

Responsabilizarea părților interesate – dezvoltarea unei culturi a securității şi a gestionării riscurilor prin stimularea schimbului de informații şi a cooperării extinse între actorii din sectorul public şi privat, totodată în beneficiul direct al cetățenilor, precum şi prin dezvoltarea unei culturi de sensibilizare în materie de NIS.

Protejarea Europei de amenințările internaționale – atingerea unui nivel ridicat de cooperare cu țări terțe şi organizații internaționale pentru promovarea unei abordări comune la nivel mondial a NIS şi pentru a da un impact inițiativelor internaționale de înalt nivel în Europa;

Înspre o implementare concertată – facilitarea colaborării la implementarea politicilor NIS.

Lupta împotriva criminalității cibernetice - integrarea aspectelor NIS ale luptei împotriva criminalității cibernetice în dezbaterile şi schimbul de bune practici între părțile interesate din sectorul public şi privat, în special prin cooperarea cu autoritățile din cadrul (foştilor) piloni 2 si 3, de exemplu cu Europol.

1.4.2. Obiectiv(e) specific(e) şi activitățile (activitățile) ABM/ABB vizate

Obiectivul specific nr.

Sporirea securității rețelelor şi a informațiilor (NIS), pentru a dezvolta o cultură a securității rețelelor şi informațiilor în beneficiul cetățenilor, al consumatorilor, al întreprinderilor şi al organizațiilor din sectorul public şi pentru a identifica provocările politice ridicate de internet şi de rețelele viitorului

Activități ABM/ABB vizate

Politica în domeniul comunicațiilor electronice şi securitatea rețelelor

1.4.3. Rezultatul (rezultatele) şi impactul (impacturile) preconizate

Se preconizează că inițiativa va produce următoarele impacturi economice:

- creşterea disponibilității informațiilor privind provocările şi riscurile actuale şi viitoare în ceea ce privește securitatea și reziliența

- o colectare mai eficientă a informațiilor relevante privind riscurile, amenințările și vulnerabilitățile de către fiecare stat membru în parte

- un nivel sporit al gradului de informare al factorilor de decizie politică în luarea deciziilor

- o calitate sporită a dispozițiilor de politică în materie de NIS în statele membre, prin diseminarea de bune practici

- economii de scară în ceea ce privește reacția la incidente la nivelul UE

- creşterea volumului de investiții, datorită obiectivelor de politică comune și standardelor în materie de securitate și reziliență uniformizate la nivelul UE

- un risc operațional mai scăzut pentru întreprinderi, datorită unui nivel crescut al securității și al rezilienței

- măsuri mai coerente în ceea ce privește lupta împotriva criminalității cibernetice.

Se preconizează că inițiativa va produce următoarele impacturi sociale:

- o încredere sporită a utilizatorilor în serviciile și sistemele societății informaționale;

- o încredere sporită în funcționarea pieței interne a UE, prin atingerea unui nivel mai înalt de protecție a consumatorilor;

- ameliorarea schimburilor de informații și cunoștințe cu țările nemembre ale UE;

- o mai bună protejare a drepturilor fundamentale ale omului în UE, prin asigurarea unui nivel uniform de protecție a datelor cu caracter personal și a vieții private a cetățenilor Uniunii Europene.

Impacturile preconizate asupra mediului sunt minime:

- reducerea impactului emisiilor de CO2 datorită, de exemplu, reducerii numărului călătoriilor, rezultat din încrederea sporită în utilizarea sistemelor şi a serviciilor TIC, şi datorită consumului redus de energie, rezultat din economiile de scară în implementarea obligațiilor de securitate.

1.4.4. Indicatori de rezultat și de impact

Indicatorii de monitorizare per obiectiv sunt următorii:

Coerența abordărilor în materie de reglementare:

- numărul de state membre care au aplicat recomandările agenției în procesul de elaborare a propriilor politici

- numărul de studii având ca obiectiv identificarea discrepanțelor și a inconsecvențelor în materie de standardizare în ceea ce privește NIS

- armonizarea abordărilor statelor membre în ceea ce privește NIS

Prevenire, detectare și reacție:

- numărul de cursuri de formare organizate având ca temă securitatea rețelelor

- existența unui sistem operațional de alertă rapidă în caz de riscuri și atacuri emergente

- numărul de exerciții NIS coordonate de agenție la nivelul UE

Dezvoltarea cunoștințelor factorilor de decizie politică:

- numărul de studii vizând colectarea de date referitoare la riscurile actuale și previzibile în materie de NIS și la tehnologiile de prevenire a riscurilor

- numărul de consultări cu organisme publice care activează în domeniul NIS

- existența unui cadru european pentru organizarea colectării de date referitoare la NIS

Responsabilizarea părților interesate:

- numărul de bune practici stabilite pentru întreprinderi

- nivelul investițiilor în măsuri de securitate realizate de părțile interesate din sectorul privat

Protejarea Europei de amenințările internaționale:

- numărul de conferințe între statele membre, pentru stabilirea de obiective comune în materie de NIS

- numărul de reuniuni între experți europeni și internaționali din domeniul NIS

Înspre o implementare concertată:

- numărul de evaluări ale conformității reglementare/legislative

- numărul de practici NIS la scara UE

Lupta împotriva criminalității cibernetice:

- regularitatea interacțiunilor cu agențiile din cadrul foștilor piloni 2 și 3

- numărul situațiilor în care a fost furnizată expertiză în cadrul anchetelor penale

1.5. Motivul (motivele) propunerii/inițiativei

1.5.1. Cerință(e) de îndeplinit pe termen scurt sau lung

ENISA a fost creată inițial în 2004 pentru a face față amenințărilor și posibilelor încălcări subsecvente ale NIS. De atunci, provocările din sfera NIS au evoluat odată cu tehnologia și cu piața și au făcut obiectul unor noi reflecții și dezbateri, permițând astăzi o actualizare și o descriere mai detaliată a problemelor concrete identificate și a modului în care acestea sunt afectate de schimbările survenite în peisajul NIS.

1.5.2. Valoarea adăugată a implicării UE

Problemele din sfera NIS nu se limitează la granițele naționale și, prin urmare, nu pot fi rezolvate în mod eficace numai la nivel național. În același timp, există o mare diversitate în ceea ce privește modul în care autoritățile publice din diferite state membre tratează problema. Aceste diferențe pot constitui un obstacol major în calea implementării unor mecanisme adecvate la nivelul Uniunii pentru consolidarea NIS în Europa. Din cauza interconectării infrastructurilor TIC, eficacitatea măsurilor luate la nivel național într-unul dintre statele membre este încă puternic influențată de nivelul scăzut al măsurilor adoptate în celelalte state

membre şi de lipsa de cooperare transfrontalieră sistematică. Măsurile insuficiente în materie de NIS care provoacă un incident într-un stat membru pot cauza perturbări ale serviciilor în alte state membre.

În plus, multiplicarea cerințelor în materie de securitate implică povara unui cost asupra întreprinderilor care operează la nivelul Uniunii Europene şi duce la fragmentare şi la lipsa competitivității pe piața internă europeană.

În timp ce dependența de rețele şi de sistemele informatice este în creştere, pregătirea pentru soluționarea incidentelor pare insuficientă.

Sistemele naționale actuale de alertă rapidă şi gestionare a incidentelor prezintă deficiențe importante. Procesele şi practicile de monitorizare și de raportare a incidentelor de securitate a rețelelor diferă în mod semnificativ de la un stat membru la altul. În unele țări procesele nu sunt oficializate, în timp ce în alte țări nu există nicio autoritate competentă pentru primirea şi prelucrarea rapoartelor privind incidentele. Nu există sisteme europene. În consecință, furnizarea necesităților de bază ar putea fi fundamental perturbată de incidente NIS şi se impune pregătirea unor reacții adecvate. Comunicarea Comisiei privind CIIP a subliniat, de asemenea, nevoia existenței unei capacități de alertă rapidă şi reacție la incidente la nivel european, susținute eventual prin exerciții la scară europeană.

Există o nevoie/necesitate clară de instrumente politice care să aibă ca scop identificarea proactivă a riscurilor şi vulnerabilităților în materie de NIS, stabilind mecanisme de reacție adecvate (de exemplu, prin identificarea şi diseminarea de bune practici) şi asigurându-se că aceste mecanisme de reacție sunt cunoscute şi aplicate de către părțile interesate.

1.5.3. Învățăminte desprinse din experiențe anterioare similare

A se vedea subpunctele *1.5.1* şi *1.5.2*.

1.5.4. Coerența şi posibila sinergie cu alte instrumente relevante

Prezenta inițiativă este pe deplin coerentă cu dezbaterea generală privind NIS şi alte inițiative politice care se concentrează asupra viitorului NIS. Ea este una dintre componentele principale ale Agendei digitale pentru Europa, acesta din urmă fiind o inițiativă emblematică a strategiei Europa 2020.

1.6. Durata și impactul financiar

☑ Propunere/inițiativă cu **durată limitată**

– ☑ Punctul de pornire pentru prelungirea cu 5 ani va fi 14.3.2012, sau data la care noul regulament intră în vigoare, în cazul în care acest lucru survine la o dată ulterioară.

– ☑ Impact financiar din 2012 până în 2017

☐ Propunere/inițiativă cu **durată nelimitată**

– Implementare cu o perioadă de creștere în intensitate din AAAA până în AAAA,

– urmată de o perioadă de funcționare în regim de croazieră.

1.7. Modul (modurile) de gestionare avut(e) în vedere[39]

☐ **Gestionarea centralizată directă** de către Comisie

☑ **Gestionare centralizată indirectă** cu delegarea sarcinilor de implementare către:

– ☐ agenții executive

– ☑ organisme instituite de Comunități[40]

– ☐ organisme publice naționale/organisme cu atribuții de serviciu public

– ☐ persoane cărora li se încredințează executarea unor acțiuni specifice în temeiul titlului V din Tratatul privind Uniunea Europeană, identificate în actul de bază relevant în sensul articolului 49 din regulamentul financiar

☐ **Gestionare partajată** cu statele membre

☐ **Gestionare descentralizată** cu țări terțe

☐ **Gestionare în comun** cu organizații internaționale ***(de precizat)***

---

[39] Detalii referitoare la modurile de gestionare și trimiterile la regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Menționate la articolul 185 din regulamentul financiar.

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și de raportare

Directorul executiv este responsabil cu evaluarea și monitorizarea efectivă a performanțelor agenției în raport cu obiectivele acesteia și raportează anual consiliului de administrație.

Directorul executiv întocmește un proiect de raport general privind toate activitățile desfășurate de agenție în anul precedent, care compară, în special, rezultatele obținute cu obiectivele trasate prin programul anual de lucru. În urma adoptării de către consiliul de administrație, acest raport este înaintat Parlamentului European, Consiliului, Comisiei, Curții de Conturi, Comitetului Economic și Social European și Comitetului Regiunilor și este, de asemenea, publicat.

2.2. Sistemul de gestiune și control

2.2.1. Riscul (riscurile) identificat(e)

De la înființarea ENISA în 2004, agenția a fost supusă atât unor evaluări interne, cât și externe.

În conformitate cu articolul 25 din Regulamentul ENISA, primul pas în cadrul acestui proces l-a reprezentat evaluarea independentă a ENISA realizată în 2006-2007 de către o comisie de experți externi. Raportul comisiei de experți externi[41] a confirmat că motivele inițiale de ordin politic care au stat la baza înființării ENISA, precum și obiectivele (sale primare)/inițiale ale acesteia sunt încă valabile; raportul a fost de asemenea util pentru ridicarea unora dintre problemele care trebuiau abordate.

În martie 2007, Comisia a înaintat un raport asupra acestei evaluări către consiliul de administrație, care și-a formulat ulterior propriile recomandări privind viitorul agenției și modificarea Regulamentului ENISA[42].

În iunie 2007, Comisia a prezentat propria sa apreciere cu privire la rezultatele evaluării externe și la recomandările consiliului de administrație, într-o comunicare către Parlamentul European și către Consiliu[43]. Comunicarea preciza că trebuie să se aleagă între extinderea mandatului agenției și înlocuirea agenției cu un alt mecanism, de exemplu cu un forum permanent al factorilor interesați sau cu o rețea de organizații pentru securitate. De asemenea, comunicarea lansa o consultare publică asupra acestui aspect, solicitând contribuția factorilor interesați de la nivel european prin intermediul unei liste de întrebări în scopul orientării discuțiilor ulterioare[44].

---

41 http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm.

42 Așa cum prevede articolul 25 din regulamentul ENISA. Textul integral al documentului adoptat de consiliul de administrație al ENISA, care conține de asemenea și comentariile consiliului, este disponibil la adresa de internet: http://enisa.europa.eu/pages/03_02.htm.

43 Comunicarea Comisiei către Parlamentul European și către Consiliu privind evaluarea Agenției europene pentru securitatea rețelelor și a informațiilor (ENISA), COM(2007) 285 final, 1.6.2007: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT.

44 http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en.

2.2.2. Metoda (metodele) de control preconizată(e)

A se vedea subpunctele 2.1. și 2.2.1. de mai sus.

2.3. Măsuri de prevenire a fraudelor și neregulilor

Personalul agenției verifică plățile pentru orice fel de servicii sau de studii solicitate, înainte de efectuarea plății, luând în considerare toate obligațiile contractuale, principiile economice și bunele practici financiare sau de gestionare. Toate acordurile și contractele încheiate între agenție și beneficiarii plăților vor cuprinde dispoziții antifraudă (control, cerințe privind raportarea etc.).

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI*

3.1. Rubrica (rubricile) din cadrul financiar multianual și linia bugetară (liniile bugetare) afectată (afectate)

- Linii bugetare de cheltuieli existente

Poziția din cadrul financiar multianual	Linie bugetară	Tip de cheltuieli	Contribuție			
	Număr / Descriere	CD/CND (45)	Țări AELS[46]	Țări candidate[47]	țări terțe	în sensul articolului 18(1)(aa) din regulamentul financiar
1.a Competitivitate pentru creștere economică și ocuparea locurilor de muncă	09 02 03 01 Agenția europeană pentru securitatea rețelelor și a informațiilor – subvenție în cadrul titlurilor 1 și 2	CD	DA	NU	NU	NU
	09 02 03 02 Agenția europeană pentru securitatea rețelelor și a informațiilor – subvenție în cadrul titlului 3	CD	DA	NU	NU	NU
5 Cheltuieli administrative	09 01 01 Cheltuieli cu personalul în activitate în domeniul politic Societate informațională și media	CND	NU	NU	NU	NU
	09 01 02 11 Alte cheltuieli de gestiune	CND	NU	NU	NU	NU

* Impactul financiar estimat al propunerii pentru perioada ulterioară perioadei actuale de programare financiară 2007-2013 nu este acoperit de prezenta fişă financiară legislativă. Pe baza propunerii Comisiei privind regulamentul de stabilire a cadrului financiar multianual dincolo de anul 2013 şi ţinând cont de concluziile evaluării impactului, Comisia va prezenta o fişă financiară legislativă modificată.

45 CD = credite diferențiate / CND = credite nediferențiate.

46 AELS: Asociația Europeană a Liberului Schimb.

47 Țări candidate și, acolo unde este cazul, țări potențial candidate din Balcanii de Vest.

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

milioane EUR (cu 3 zecimale)

Rubrica din cadrul financiar multianual:	1.a	Competitivitate pentru creștere economică și ocuparea locurilor de muncă

ENISA			1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	**TOTAL 14 mar. 2012 – 13 mar. 2017**
Credite operaționale										
09 02 03 02 Agenția europeană pentru securitatea rețelelor și a informațiilor – subvenție în cadrul titlului 3	Angajamente	(1)	0,454	1,976	2,470	--	--	--	--	--
	Plăți	(2)	0,454	1,976	2,470	--	--	--	--	--
Creditele administrative										
09 02 03 01 Agenția europeană pentru securitatea rețelelor și a informațiilor – subvenție în cadrul titlurilor 1 și 2		(3)	1,293	4,697	6,120	--	--	--	--	--
TOTAL credite în cadrul RUBRICII 1.a	Angajamente	=1 +3	1,747	6,673	8,590	--	--	--	--	--
	Plăți	=2+3	1,747	6,673	8,590	--	--	--	--	--

TOTAL credite operaționale	Angajamente	(4)	0,454	1,976	2,470	--	--	--	--	--
	Plăți	(5)	0,454	1,976	2,470	--	--	--	--	--
TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)	1,293	4,697	6,120	--	--	--	--	--
TOTAL credite în cadrul RUBRICII 1.a din programul-cadru multianual	Angajamente	=4+6	1,747	6,673	8,590	--	--	--	--	--
	Plăți	=5+6	1,747	6,673	8,590	--	--	--	--	--

milioane EUR (cu 3 zecimale)

Rubrica din cadrul financiar multianual:	5	Cheltuieli administrative

		1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	Total
Resurse umane		0,085	0,342	0,427	--	--	--	--	--
Alte cheltuieli administrative		0,002	0,013	0,015	--	--	--	--	--
TOTAL DG INFSO	Credite	0,087	0,355	0,442	--	--	--	--	--

TOTAL credite în cadrul RUBRICII 5 din cadrul financiar multianual	(Total angajamente = Total plăți)	0,087	0,355	0,442	--	--	--	--	--

		1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	Total
TOTAL credite în cadrul RUBRICIILOR 1-5 din cadrul financiar multianual	Angajamente	1,834	7,028	9,032	--	--	--	--	--
	Plata	1,834	7,028	9,032	--	--	--	--	--

3.2.2. Impactul estimat asupra creditelor operaționale

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

– ☑ Propunerea/inițiativa implică utilizarea creditelor operaționale, conform explicațiilor de mai jos:

Credite de angajament în milioane EUR (cu 3 zecimale)

Obiectivele și realizările ⇩	1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	**TOTAL 14 mar. 2012 – 13 mar. 2017**
Coerența abordărilor în materie de reglementare	0,114	0,494	0,620	--	--	--	--	--
Prevenire, detectare și reacție	0,114	0,494	0,620	--	--	--	--	--
Dezvoltarea cunoștințelor factorilor de decizie politică	0,068	0,297	0,370	--	--	--	--	--
Responsabilizarea părților interesate	0,050	0,218	0,270	--	--	--	--	--
Protejarea Europei de amenințările internaționale	0,023	0,099	0,120	--	--	--	--	--
Înspre o implementare concertată	0,064	0,276	0,340	--	--	--	--	--
Lupta împotriva criminalității cibernetice	0,023	0,098	0,120	--	--	--	--	--
COST TOTAL	0,454	1,976	2,460	--	--	--	--	--

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ[48]

3.2.3.1. Sinteză

– ☐ Propunerea/inițiativa nu implică utilizarea de credite administrative

– ☑ Propunerea/inițiativa implică utilizarea creditelor cu caracter administrativ, conform explicațiilor de mai jos:

a) Cheltuieli administrative în cadrul rubricii 5 din cadrul financiar multianual

milioane EUR (cu 3 zecimale)

RUBRICA 5 din cadrul financiar multianual	1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	**Total 14 mar. 2012 – 13 mar. 2017**
Resurse umane	0,085	0,342	0,427	--	--	--	--	--
Alte cheltuieli administrative	0,002	0,013	0,015	--	--	--	--	--
TOTAL	0,087	0,355	0,442	--	--	--	--	--

b) Cheltuieli administrative legate de ENISA – vizate de linia bugetară 09.020301 Securitatea rețelelor și a informației în Europa: Titlurile 1 – Personal și 2 – Funcționarea agenției".

milioane EUR (cu 3 zecimale)

	1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	**Total 14 mar. 2012 – 13 mar. 2017**
Resurse umane - Titlul 1 – Personalul	1,153	4,329	5,607	--	--	--	--	--
Alte cheltuieli de natură administrativă - Titlurile 1 – Personalul și 2 – Funcționarea agenției	0,140	0,368	0,513	--	--	--	--	--
TOTAL	**1,293**	**4,697**	**6,120**	--	--	--	--	--

[48] Anexa la fișa financiară legislativă nu este completată, întrucât ea nu se aplică prezentei propuneri.

3.2.3.2. Necesarul de resurse umane estimat

În fiecare an, schema de personal a agenției trebuie explicată și justificată printr-un document intitulat Plan de politică a personalului, care trebuie înaintat autorității bugetare.

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane

– ☑ Propunerea/inițiativa implică utilizarea de resurse umane, conform explicațiilor de mai jos:

a) Resurse umane din cadrul Comisiei

	1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017
Posturi din schema de personal (posturi de funcționari și de agenți temporari)							
XX 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)	3,5	3,5	3,5	--	--	--	--
TOTAL	**3,5**	**3,5**	**3,5**	--	--	--	--

b) Resurse umane ale ENISA

		1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017
Schema de personal a ENISA (în echivalent normă întreagă ENI)								
Funcționari sau agenți temporari	AD	29	31	31	--	--	--	--
	AST	15	16	16	--	--	--	--
TOTAL funcționari sau agenți temporari		44	47	47	--	--	--	--
Alte categorii de personal (în ENI)								
Agenți contractuali		13	14	14	--	--	--	--
Experți naționali detașați (END)		5	5	5	--	--	--	--
Total other staff		18	19	19	--	--	--	--
TOTAL		**62**	**66**	**66**	--	--	--	--

Descrierea sarcinilor care trebuie îndeplinite de personalul agenției:

Funcționari și agenți temporari	Agenția va continua: – să îndeplinească o funcție consultativă și de coordonare, în cadrul căreia **va colecta și analiza date** privind securitatea informațiilor. În prezent, organizații publice și private având diverse obiective colectează date privind incidentele din domeniul IT, precum și alte date relevante pentru securitatea informațiilor. Nu există însă niciun organism central la nivel european care să poată colecta și analiza aceste date în mod exhaustiv și să poată formula opinii și recomandări în vederea sprijinirii activității UE în materie de politică a securității rețelelor și a informațiilor; – să îndeplinească **rolul de centru de expertiză** la care pot apela atât statele membre, cât și instituțiile UE în vederea obținerii unor **opinii și recomandări privind aspecte tehnice** legate de securitate; – să contribuie la o **cooperare extinsă între diverșii actori** din domeniul securității informațiilor, de exemplu prin oferirea de asistență pentru activitățile continuatoare vizând asigurarea securității comerțului electronic. O astfel de cooperare va reprezenta o condiție prealabilă vitală pentru funcționarea în condiții de securitate a rețelelor și sistemelor informatice din Europa. Este necesară participarea și implicarea tuturor părților interesate; – să contribuie la o abordare coordonată în ceea ce privește securitatea informațiilor, prin oferirea de **asistență statelor membre**, de exemplu în domeniul **promovării evaluării riscurilor** și al activităților de sensibilizare; – să asigure **interoperabilitatea rețelelor și a sistemelor informatice** atunci când statele membre **aplică** cerințe de ordin tehnic cu impact asupra securității; – să identifice necesitățile **relevante în ceea ce privește standardizarea**, să evalueze standardele și sistemele de certificare existente în domeniul securității și să promoveze o utilizare pe scară cât mai largă a acestora, în sprijinul aplicării legislației UE; – să sprijine **cooperarea internațională** în acest domeniu, care devine din ce în ce mai necesară dat fiind caracterul mondial al aspectelor legate de securitatea rețelelor și a informațiilor.
Personal extern	A se vedea mai sus

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

– ☑ Propunerea/inițiativa este compatibilă cu cadrul financiar multianual existent.

– ☐ Propunerea/inițiativa necesită o reprogramare a rubricii corespunzătoare din cadrul financiar multianual.

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau la revizuirea cadrului financiar multianual[49].

Finanțarea UE după 2013 va fi examinată în cadrul unei dezbateri la nivelul Comisiei privind toate propunerile pentru perioada de după 2013. Aceasta înseamnă că, odată ce Comisia a făcut propunerea pentru următorul cadru financiar multianual, Comisia va prezenta o situație financiară legislativă modificată, ținând seama de concluziile evaluării impactului.

3.2.5. Contribuția părților terțe

– ☐ Propunerea/inițiativa nu prevede cofinanțare din partea terților

– ☑ Propunerea/inițiativa prevede cofinanțare, estimată în cele ce urmează:

Credite orientative în milioane EUR (cu 3 zecimale)

	1 ian. – 13 mar. 2012	14 mar. – 31 dec. 2012	2013	2014	2015	2016	1 ian. – 13 mar. 2017	**Total 14 mar. 2012 – 13 mar. 2017**
EFTA	0,042	0,160	0,206	--	--	--	--	--

3.3. Impactul estimat asupra veniturilor

– ☑ Propunerea/inițiativa nu are impact financiar asupra veniturilor.

– ☐ Propunerea/inițiativa are următorul impact financiar:

– ☐ asupra resurselor proprii

– ☐ asupra diverselor venituri

[49] A se vedea punctele 19 și 24 din Acordul interinstituțional.