COMISIA
EUROPEANĂ

Bruxelles, 7.2.2013
COM(2013) 48 final

2013/0027 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI

privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune

{SWD(2013) 31 final}
{SWD(2013) 32 final}

EXPUNERE DE MOTIVE

Scopul directivei propuse este de a asigura un nivel comun ridicat de securitate a rețelelor și a informației. Acest lucru înseamnă îmbunătățirea securității internetului și a rețelelor private, precum și a sistemelor informatice pe care se bazează funcționarea societății și a economiei. În acest scop, li se va solicita statelor membre să își îmbunătățească nivelul de pregătire și cooperarea reciprocă, iar operatorilor de infrastructuri critice, precum cele de energie și transport, principalilor furnizorii de servicii ale societății informaționale (platforme de comerț electronic, rețele de socializare etc.) și administrațiilor publice li se va solicita să adopte măsurile corespunzătoare pentru gestionarea riscurilor de securitate și raportarea incidentelor grave către autoritățile naționale competente.

Prezenta propunere este prezentată în corelare cu Comunicarea comună a Comisiei și a Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate privind o strategie europeană de securitate cibernetică. Obiectivul strategiei este de a oferi un mediu digital sigur și demn de încredere, promovând și protejând în același timp drepturile fundamentale și alte valori centrale ale UE. Prezenta propunere constituie acțiunea principală a strategiei. Alte acțiuni ale strategiei, din același domeniu, se concentrează pe sensibilizare, pe dezvoltarea unei piețe interne pentru produse și servicii de securitate cibernetică și pe încurajarea investițiilor în cercetare și dezvoltare. Aceste acțiuni vor fi completate de altele care vizează intensificarea luptei împotriva criminalității informatice și elaborarea unei politici a UE privind securitatea cibernetică la nivel internațional.

1.1. Motivele și obiectivele propunerii

Securitatea rețelelor și a informației (*Network and information security* - NIS) este din ce în ce mai importantă pentru economie și societate. NIS este, de asemenea, o condiție prealabilă importantă de creare a unui mediu fiabil pentru comerțul mondial cu servicii. Sistemele informatice pot fi însă afectate de incidente de securitate, cum ar fi greșeli umane, evenimente naturale, deficiențe tehnice sau atacuri răuvoitoare. Amploarea, frecvența și complexitatea acestor incidente crește din ce în ce mai mult. Un procent de 57 % dintre respondenții la consultarea publică online privind „Îmbunătățirea securității rețelelor și a informației în UE”[1] organizată de Comisie au afirmat că s-au confruntat în anul precedent cu incidente de securitate a rețelelor și a informației care le-au afectat grav activitatea. Lipsa NIS poate compromite servicii vitale care depind de integritatea rețelelor și a sistemelor informatice. Acest lucru poate provoca întreruperea funcționării unor întreprinderi, poate genera pierderi financiare substanțiale pentru economia UE și poate avea un impact negativ asupra bunăstării sociale.

În plus, ca instrumente de comunicare fără frontiere, sistemele de informare digitale ale statelor membre, în special internetul, sunt interconectate și au un rol esențial în facilitarea circulației transfrontaliere a mărfurilor, serviciilor și persoanelor. O perturbare majoră a funcționării acestor sisteme într-un stat membru poate afecta alte state membre și UE în ansamblul său. Prin urmare, reziliența și stabilitatea rețelelor și a sistemelor informatice este esențială pentru definitivarea pieței digitale unice și pentru buna funcționare a pieței interne. Probabilitatea de producere și frecvența incidentelor, precum și incapacitatea de a asigura o protecție eficientă subminează, de asemenea, încrederea publicului în serviciile furnizate de rețele și de sistemele informatice: de exemplu, sondajul Eurobarometru din 2012 privind securitatea cibernetică a arătat că 38 % dintre utilizatorii de internet din UE sunt preocupați de siguranța plăților online și și-au schimbat comportamentul în urma temerilor legate de securitate: 18 % sunt mai puțin înclinați să cumpere bunuri online și 15 % sunt mai puțin înclinați să utilizeze servicii bancare online[2].

Situația actuală din UE, care reflectă abordarea pur voluntară urmată până în prezent, nu asigură o protecție suficientă împotriva incidentelor și a riscurilor de securitate a rețelelor și a informației în întreaga UE. Capacitățile și mecanismele existente în domeniul NIS sunt pur și simplu insuficiente pentru a ține pasul cu evoluția rapidă a amenințărilor din acest sector și a asigura un nivel comun ridicat de protecție în toate statele membre.

În pofida inițiativelor întreprinse, statele membre au niveluri foarte diferite de capacitate și de pregătire, ceea ce conduce la fragmentarea abordărilor în UE. Ca urmare a faptului că rețelele și sistemele sunt interconectate, securitatea globală a rețelelor și a informației din UE este slăbită de statele membre cu un nivel insuficient de protecție. Această situație împiedică, de asemenea, formarea încrederii inter pares, care constituie o condiție preliminară pentru cooperare și schimb de informații. În consecință, numai un număr mic de state membre cu un nivel ridicat al capacităților cooperează între ele.

Ca urmare, nu există în prezent la nivelul UE un mecanism eficace de cooperare și colaborare eficientă între statele membre și de schimb de informații în condiții de încredere cu privire la incidentele și riscurile de securitate a rețelelor și a informației. Acest fapt poate conduce la intervenții necoordonate în domeniul reglementării, la strategii necoerente și standarde divergente, având ca rezultat o protecție insuficientă împotriva incidentelor și a riscurilor de securitate a rețelelor și a informației în întreaga UE. Pot apărea, de asemenea, obstacole în

[1] Consultarea publică online privind „Îmbunătățirea securității rețelelor și a informației în UE ” s-a desfășurat în perioada 23 iulie - 15 octombrie 2012.

[2] Eurobarometru 390/2012.

cadrul pieței interne generând costuri de conformitate pentru întreprinderile care operează în mai multe state membre.

În sfârșit, părților care administrează infrastructura critică sau care furnizează servicii esențiale pentru funcționarea societății nu li se impun obligații adecvate de a adopta măsuri de gestionare a riscurilor și de a face schimb de informații cu autoritățile relevante. Pe de o parte, întreprinderilor le lipsesc, prin urmare, stimulentele necesare pentru a aplica o gestionare serioasă a riscurilor, care implică evaluarea acestora și luarea de măsuri adecvate pentru asigurarea NIS. Pe de altă parte, multe dintre incidente nu sunt aduse la cunoștința autorităților competente și trec neobservate. Este însă esențial ca autoritățile publice să fie informate cu privire la incidente, pentru ca acestea să reacționeze, să ia măsuri corespunzătoare de atenuare și să stabilească priorități strategice adecvate în materie de NIS.

Cadrul actual de reglementare impune numai companiilor de telecomunicații să adopte măsuri de gestionare a riscurilor și să raporteze incidentele grave de securitate a rețelelor și a informației. Cu toate acestea, funcționarea multor altor sectoare se bazează pe TIC și, prin urmare, acestea ar trebui să fie preocupate, de asemenea, de NIS. O serie de furnizori de infrastructură și servicii specifice sunt deosebit de vulnerabili din cauza dependenței lor ridicate de funcționarea corectă a rețelelor și a sistemelor informatice. Aceste sectoare au un rol esențial în furnizarea principalelor servicii de suport pentru economie și societate, iar securitatea sistemelor lor este deosebit de importantă pentru funcționarea pieței interne. Sectoarele respective includ băncile, bursele, producția, transportul și distribuția de energie, transporturile (aeriene, feroviare, maritime), sănătatea, serviciile de internet și administrațiile publice.

Prin urmare, este nevoie de o schimbare majoră a modului în care este tratată în UE securitatea rețelelor și a informației. Sunt necesare obligații de reglementare pentru a crea condiții de concurență echitabile și a elimina actualele lacune legislative. Pentru a soluționa aceste probleme și a crește nivelul de securitate a rețelelor și a informației în Uniunea Europeană, directiva propusă vizează obiectivele expuse în continuare.

În primul rând, propunerea solicită tuturor statelor membre să se asigure că este instituit un nivel minim de capacități naționale prin înființarea autorităților competente în materie de NIS, crearea de echipe de intervenție în caz de urgență informatică (*Computer Emergency Response Teams* - CERT) și adoptarea strategiilor naționale privind NIS și a planurilor naționale de cooperare în domeniul NIS.

În al doilea rând, autoritățile naționale competente trebuie să coopereze în cadrul unei rețele care să permită o coordonare sigură și eficace, inclusiv schimbul coordonat de informații, precum și detectarea și răspunsul la nivelul UE. Prin această rețea, statele membre trebuie să facă schimb de informații și să coopereze pentru a contracara amenințările și incidentele în materie de NIS, pe baza planului european de cooperare în domeniul NIS.

În al treilea rând, conform modelului Directivei-cadru privind comunicațiile electronice, propunerea urmărește să asigure dezvoltarea unei culturi a gestionării riscurilor și partajarea informațiilor de către sectoarele public și privat. Se va solicita întreprinderilor din sectoarele critice evidențiate mai sus și administrațiilor publice să evalueze riscurile cu care se confruntă și să adopte măsuri adecvate și proporționate de asigurare a NIS. Aceste entități vor trebui să raporteze autorităților competente orice incidente care afectează grav rețelele și sistemele lor informatice și care au un impact semnificativ asupra continuității serviciilor critice și a aprovizionării cu bunuri.

1.2. Contextul general

Încă din 2001, în comunicarea sa intitulată *Network and Information Security: Proposal for A European Policy Approach* (Securitatea rețelelor și a informației: Propunere pentru o abordare de politică europeană), Comisia a subliniat importanța crescândă a NIS[3]. Comunicarea a fost urmată de adoptarea în 2006 a Strategiei pentru o societate informațională sigură (*Strategy for a Secure Information Society*)[4] care urmărea dezvoltarea unei culturi a securității rețelelor și a informației în Europa. Principalele elemente ale acesteia au fost aprobate printr-o rezoluție a Consiliului[5].

Comisia a adoptat apoi, la 30 martie 2009, o comunicare privind protecția infrastructurilor critice de informații (CIIP)[6] care s-a concentrat asupra protecției Europei împotriva perturbării funcționării sistemelor informatice, prin întărirea securității. Comunicarea a lansat un plan de acțiune pentru a sprijini eforturile depuse de statele membre în materie de prevenire și răspuns. Planul de acțiune a fost aprobat în cadrul concluziilor Președinției Conferinței ministeriale privind CIIP desfășurată la Tallinn în 2009. La 18 decembrie 2009, Consiliul a adoptat Rezoluția privind o abordare europeană a securității rețelelor și a informațiilor bazată pe colaborare[7].

Agenda digitală pentru Europa[8] adoptată în mai 2010 și concluziile aferente ale Consiliului[9] au subliniat viziunea comună conform căreia încrederea și securitatea sunt condiții prealabile fundamentale pentru adoptarea pe scară largă a TIC și pentru realizarea în acest fel a obiectivelor dimensiunii „creștere inteligentă" a Strategiei Europa 2020[10]. La capitolul „Încredere și securitate", Agenda digitală pentru Europa a evidențiat necesitatea ca toate părțile interesate să își unească forțele într-un efort global pentru asigurarea securității și a rezilienței infrastructurii TIC, punând accentul pe prevenire și pe gradul de pregătire și de conștientizare, precum și pentru elaborarea de mecanisme de securitate eficace și coordonate. În special acțiunea-cheie 6 a Agendei digitale pentru Europa prevede luarea de măsuri în vederea instituirii unei politici consolidate și la nivel înalt privind NIS.

În comunicarea sa din martie 2011 privind CIIP intitulată „Realizări și etape următoare: către un context global de securitate cibernetică"[11], Comisia a evaluat rezultatele obținute de la adoptarea Planului de acțiune pentru CIIP în 2009, concluzionând că implementarea planului a arătat că abordările pur naționale ale provocărilor în materie de securitate și reziliență nu sunt suficiente și că Europa trebuie să-și continue eforturile de elaborare a unei abordări coerente și cooperative la nivelul întregii UE. Comunicarea din 2011 privind CIIP a anunțat o serie de acțiuni, Comisia solicitând statelor membre să înființeze capacități în domeniul NIS și să instituie o cooperare transfrontalieră. Acțiunile nu au fost încă puse în aplicare, deși majoritatea acestora ar fi trebuit să fie finalizată până în 2012.

În concluziile sale din 27 mai 2011 privind CIIP, Consiliul Uniunii Europene a subliniat necesitatea stringentă de a asigura reziliența și securitatea sistemelor și a rețelelor TIC în condițiile oricăror perturbări accidentale sau intenționate, de a înființa în întreaga UE capacități de nivel ridicat în domeniul pregătirii, al securității și al rezilienței, de a extinde competențele tehnice pentru a permite Europei să răspundă provocării reprezentate de

---

3 COM(2001) 298.
4 COM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0251en01.pdf.
5 2007/068/01.
6 COM(2009) 149.
7 2009/C 321/01.
8 COM(2010) 245.
9 Concluziile Consiliului din 31 mai 2010 privind Agenda digitală pentru Europa (10130/10).
10 COM(2010) 2020 și Concluziile Consiliului European din 25 și 26 martie 2010 (EUCO 7/10).
11 COM(2011) 163.

protecția rețelelor și a infrastructurilor de informații și de a încuraja cooperarea dintre statele membre prin dezvoltarea mecanismelor de cooperare dintre acestea în caz de incident.

1.3. Dispozițiile Uniunii Europene și internaționale în vigoare în acest domeniu

În temeiul Regulamentului (CE) nr. 460/2004, Comunitatea Europeană a instituit în 2004 Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA)[12], cu scopul de a contribui la asigurarea unui nivel ridicat al NIS și de a dezvolta o cultură a NIS în UE. La 30 septembrie 2010 a fost adoptată o propunere de modernizare a mandatului ENISA[13], care este în prezent examinată de Consiliu și de Parlamentul European. Cadrul revizuit de reglementare pentru comunicații electronice[14], în vigoare din noiembrie 2009, impune obligații în materie de securitate furnizorilor de comunicații electronice[15]. Aceste obligații trebuiau transpuse la nivel național până în mai 2011.

Toți actorii care sunt operatori de date (de exemplu, băncile sau spitalele) sunt obligați, prin cadrul de reglementare privind protecția datelor[16], să instituie măsuri de securitate pentru protecția datelor cu caracter personal. De asemenea, în conformitate cu propunerea din 2012 a Comisiei referitoare la Regulamentul general privind protecția datelor[17], operatorii de date trebuie să raporteze autorităților naționale de supraveghere orice încălcare a securității datelor cu caracter personal. Aceasta înseamnă că, de exemplu, o încălcare a NIS care afectează furnizarea unui serviciu fără să compromită datele cu caracter personal (de exemplu, o avarie a sistemelor TIC ale unei centrale electrice care conduce la o pană de curent) nu trebuie notificată.

În temeiul Directivei 2008/114/CE privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, Programul european pentru protecția infrastructurii critice (EPCIP)[18] stabilește abordarea globală a protecției infrastructurilor critice în UE. Obiectivele EPCIP sunt pe deplin coerente cu prezenta propunere, iar directiva trebuie să se aplice fără a aduce atingere Directivei 2008/114/CE. EPCIP nu obligă operatorii să raporteze încălcările grave ale securității și nu stabilește mecanisme de cooperare între statele membre și de răspuns în caz de incidente.

Colegislatorii discută în prezent propunerea Comisiei de directivă privind atacurile împotriva sistemelor informatice[19], care vizează armonizarea criminalizării unor tipuri specifice de comportament. Aceasta acoperă doar criminalizarea unor tipuri specifice de comportament, nu și prevenirea riscurilor și a incidentelor de NIS, răspunsul la incidentele de NIS și atenuarea impactului acestora. Prezenta directivă trebuie să se aplice fără a aduce atingere Directivei privind atacurile împotriva sistemelor informatice.

La 28 martie 2012, Comisia a adoptat o comunicare privind instituirea unui Centru european de combatere a criminalității informatice (EC3)[20]. Acest centru a fost înființat la 11 ianuarie 2013 în cadrul Oficiului European de Poliție (EUROPOL) și reprezintă punctul focal al luptei împotriva criminalității informatice în UE. EC3 are scopul de a concentra experiența și

---

12 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

13 COM(2010) 521.

14 A se vedea http://ec.europa.eu/information_society/policy/ecomm/doc/library/regframeforec_dec2009.pdf.

15 Articolele 13a și 13b din Directiva-cadru.

16 Directiva 2002/58/CE din 12 iulie 2002.

17 COM(2012) 11.

18 COM(2006) 786 http://eur-lex.europa.eu/LexUriServ/site/en/com/2006/com2006_0786en01.pdf.

19 COM(2010) 517, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EN:PDF.

20 COM(2012) 140 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0140:FIN:EN:PDF.

cunoștințele europene în materie de criminalitate informatică pentru a ajuta statele membre la dezvoltarea capacităților, de a acorda sprijin statelor membre în investigațiile privind criminalitatea informatică și, în strânsă cooperare cu Eurojust, de a deveni vocea colectivă a investigatorilor europeni din domeniul criminalității informatice care activează în cadrul autorităților de aplicare a legii și al autorităților judiciare.

Instituțiile, agențiile și organismele europene și-au creat propria Echipă de intervenție în caz de urgență informatică, denumită CERT-EU.

La nivel internațional, activitatea UE în domeniul securității cibernetice se desfășoară atât în plan bilateral, cât și multilateral. În urma reuniunii la nivel înalt UE-SUA din 2010[21] a fost înființat Grupul de lucru UE-SUA privind securitatea cibernetică și criminalitatea informatică. UE este activă și în alte foruri multilaterale relevante, cum ar fi Organizația pentru Cooperare și Dezvoltare Economică (OCDE), Adunarea Generală a Organizației Națiunilor Unite, Uniunea Internațională a Telecomunicațiilor (ITU), Organizația pentru Securitate și Cooperare în Europa (OSCE), Summitul mondial privind societatea informațională (WSIS) și Forumul privind guvernanța internetului (FGI).

2. REZULTATELE CONSULTĂRILOR CU PĂRȚILE INTERESATE ȘI ALE EVALUĂRII IMPACTULUI

2.1. Consultarea părților interesate și utilizarea avizului experților

În perioada 23 iulie - 15 octombrie 2012 s-a desfășurat o consultare publică online privind „Îmbunătățirea NIS în UE”. Comisia a primit în total 160 de răspunsuri la chestionarul online.

Concluzia principală a fost că necesitatea de a îmbunătăți NIS în întreaga UE este general recunoscută de către părțile interesate. Mai precis: în opinia a 82,8 % dintre respondenți, guvernele din UE ar trebui să acționeze mai mult în direcția asigurării un nivel ridicat de NIS; 82,8 % au fost de părere că utilizatorii informațiilor și ai sistemelor nu sunt conștienți de actualele amenințări și incidente în materie de NIS; 66,3 % ar fi, în principiu, în favoarea introducerii prin reglementare a unei cerințe privind gestionarea riscurilor de NIS și 84,8 % au declarat că astfel de cerințe ar trebui stabilite la nivelul UE. Un număr mare de respondenți au considerat că ar fi important să se adopte cerințe privind NIS în special în următoarele sectoare: bănci și finanțe (91,1 %), energie (89,4 %), transporturi (81,7 %), sănătate (89,4 %), servicii de internet (89,1 %) și administrații publice (87,5 %). Respondenții au considerat, de asemenea, că în cazul introducerii unei cerințe de raportare către autoritatea națională competentă a cazurilor de încălcare a NIS, aceasta ar trebui să fie stabilită la nivelul UE (65,1 %) și să se aplice și administrațiilor publice (93,5%). În sfârșit, respondenții au afirmat că cerința de a aplica gestionarea riscurilor de NIS în conformitate cu cea mai avansată tehnologie nu ar implica pentru ei costuri suplimentare semnificative (63,4 %) și că cerința de a raporta cazurile de încălcare a securității nu ar conduce la costuri suplimentare semnificative (72,3 %).

Statele membre au fost consultate în cadrul unei serii de configurații relevante ale Consiliului, în contextul Forumului european al statelor membre (FESM), la Conferința privind securitatea cibernetică organizată de Comisie și de Serviciul European de Acțiune Externă la 6 iulie 2012, precum și cu ocazia reuniunilor bilaterale dedicate acestui subiect și convocate la cererea unui stat membru.

[21] http://europa.eu/rapid/press-release_MEMO-10-597_en.htm.

Au avut loc, de asemenea, discuții cu sectorul privat în cadrul Parteneriatului public-privat european pentru reziliență[22], precum și al unor reuniuni bilaterale. În ceea ce privește sectorul public, Comisia a purtat discuții cu ENISA și cu CERT pentru instituțiile UE.

2.2. Evaluarea impactului

Comisia a efectuat o evaluare a impactului a trei opțiuni de politică.

Opțiunea 1: statu quo (scenariul de bază), respectiv menținerea abordării actuale;

Opțiunea 2: abordare a reglementării, constând dintr-o propunere legislativă de instituire a unui cadru juridic comun al UE în materie de NIS referitor la capacitățile statelor membre, mecanismele de cooperare la nivelul UE și cerințele pentru principalii actori din sectorul privat și pentru administrațiile publice;

Opțiunea 3: abordare mixtă care combină inițiativele voluntare privind capacitățile statelor membre în domeniul NIS și mecanismele de cooperare la nivelul UE cu cerințele impuse prin reglementare principalilor actorii din sectorul privat și administrațiilor publice.

Comisia a concluzionat că opțiunea 2 are cel mai mare impact pozitiv, deoarece îmbunătățește considerabil protecția consumatorilor, a întreprinderilor și a guvernelor din UE împotriva incidentelor de NIS. În special obligațiile impuse statelor membre asigură un grad adecvat de pregătire la nivel național și contribuie la crearea unui climat de încredere reciprocă ce constituie o condiție prealabilă pentru o cooperare eficace la nivelul UE. Instituirea de mecanisme de cooperare la nivelul UE prin intermediul rețelei asigură acțiuni coerente și coordonate de prevenire și răspuns la incidentele și riscurile transfrontaliere de NIS. Introducerea pentru administrațiile publice și principalii actori din sectorul privat a cerințelor privind aplicarea gestionării riscurilor de NIS creează un puternic stimulent pentru gestionarea eficace a riscurilor de securitate. Obligația de a raporta incidentele de NIS cu impact semnificativ îmbunătățește capacitatea de răspuns în caz de incident și încurajează transparența. În plus, prin rezolvarea problemelor în domeniu pe plan intern, UE ar putea să își extindă prezența pe scena internațională și să devină un partener și mai credibil de cooperare la nivel bilateral și multilateral. În acest fel UE ar fi, de asemenea, mai bine plasată pentru a promova pe plan extern drepturile fundamentale și valorile sale centrale.

Evaluarea cantitativă a arătat că opțiunea 2 nu impune o sarcină disproporționată asupra statelor membre. De asemenea, costurile care trebuie suportate de sectorul privat sunt limitate, deoarece se presupune că multe dintre entitățile în cauză respectă deja cerințele de securitate existente (și anume, obligația operatorilor de date de a lua măsuri tehnice și organizatorice pentru a asigura protecția datelor cu caracter personal, inclusiv măsuri privind NIS). Cheltuielile actuale legate de securitate ale sectorului privat au fost, de asemenea, luate în considerare.

Prezenta propunere respectă principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă trebuie pusă în aplicare în conformitate cu aceste drepturi și principii.

[22] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r.

3. ELEMENTELE JURIDICE ALE PROPUNERII

3.1. Temeiul juridic

Uniunea Europeană este împuternicită să adopte măsuri pentru instituirea sau asigurarea funcționării pieței interne, în conformitate cu dispozițiile incidente ale tratatelor (articolul 26 din Tratatul privind funcționarea Uniunii Europene – TFUE). În conformitate cu articolul 114 din TFUE, UE poate adopta „măsurile privind *apropierea actelor cu putere de lege și a actelor administrative ale statelor membre* care au ca obiect instituirea și funcționarea pieței interne".

După cum s-a indicat mai sus, rețelele și sistemele informatice au un rol esențial în facilitarea circulației transfrontaliere a mărfurilor, serviciilor și persoanelor. Acestea sunt adesea interconectate, iar internetul este o rețea mondială. Ca urmare a acestei dimensiuni transnaționale intrinseci, o perturbare care are loc într-un stat membru poate afecta alte state membre și UE în ansamblul său. Prin urmare, reziliența și stabilitatea rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței interne.

Legislatorul european a recunoscut deja necesitatea de a armoniza normele de NIS pentru a asigura dezvoltarea pieței interne. Un caz concret în acest sens este Regulamentul (CE) nr. 460/2004 privind instituirea ENISA[23], care se bazează pe articolul 114 din TFUE.

Disparitățile dintre statele membre în ceea ce privește capacitățile naționale, politicile și nivelul de protecție în domeniul NIS creează obstacole în calea funcționării pieței interne și justifică o acțiune a UE.

3.2. Subsidiaritate

Intervenția europeană în domeniul securității rețelelor și a informației este justificată de principiul subsidiarității.

În primul rând, luând în considerare caracterul transfrontalier al NIS, lipsa de intervenție la nivelul UE ar conduce la o situație în care fiecare stat membru ar acționa pe cont propriu, fără a ține seama de interdependențele dintre rețelele și sistemele informatice din UE. Un grad adecvat de coordonare între statele membre ar asigura posibilitatea de a gestiona corect riscurile de NIS în contextul transfrontalier în care apar. Divergențele reglementărilor din domeniul NIS reprezintă o barieră în calea societăților care doresc să opereze în mai multe țări și în calea realizării, la nivel mondial, de economii de scară.

În al doilea rând, sunt necesare obligații de reglementare la nivelul UE pentru a crea condiții de concurență echitabile și a elimina lacunele legislative. Rezultatul abordării pur voluntare este că numai un număr mic de state membre cu un nivel ridicat al capacităților cooperează între ele. Pentru a implica toate statele membre, este necesar să se asigure faptul că acestea au nivelul de capacitate minim cerut. Măsurile privind NIS adoptate de guverne trebuie să fie coerente între ele și coordonate pentru a limita incidentele de NIS și a reduce la minimum consecințele acestora. Autoritățile competente și Comisia vor coopera în cadrul rețelei, prin schimb de bune practici și implicarea continuă a ENISA, pentru a facilita punerea în aplicare a directivei în mod convergent în întreaga UE. În plus, acțiunile concertate de politică în domeniul NIS pot avea un puternic impact pozitiv asupra protecției eficace a drepturilor fundamentale, în special a dreptului la protecția datelor cu caracter personal și a vieții private. Prin urmare, acțiunea la nivelul UE crește eficacitatea politicilor naționale existente și facilitează dezvoltarea acestora.

---

[23] Regulamentul (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 (JO L 77, 13.3.2004, p. 1).

Măsurile propuse sunt justificate și din punctul de vedere al proporționalității. Cerințele pentru statele membre sunt stabilite la nivelul minim necesar pentru a atinge un nivel adecvat de pregătire și a facilita cooperarea bazată pe încredere. Acest lucru permite, de asemenea, statelor membre să țină seama în mod cuvenit de aspectele naționale specifice și asigură aplicarea în mod proporționat a principiilor comune ale UE. Domeniul larg de aplicare va permite statelor membre să pună în aplicare directiva ținând seama de riscurile efective cu care se confruntă la nivel național și care sunt identificate în strategia națională privind NIS. Cerințele de aplicare a gestionării riscurilor vizează numai entitățile critice și impun măsuri proporționale cu riscurile. Consultarea publică a scos în evidență importanța asigurării securității acestor entități critice. Cerințele de raportare privesc numai incidentele cu impact semnificativ. După cum s-a indicat mai sus, măsurile nu impun costuri disproporționate, deoarece, în temeiul actualelor norme de protecție a datelor, multe dintre aceste entități, în calitate de operatori de date, au deja obligația de a asigura protecția datelor cu caracter personal.

Pentru a evita impunerea unei sarcini disproporționate asupra micilor operatori, în special asupra IMM-urilor, cerințele sunt proporționale cu riscurile la care sunt expuse rețeaua sau sistemul informatic în cauză și nu se aplică microîntreprinderilor. Riscurile vor trebui identificate în primul rând de către entitățile supuse acestor obligații, care vor decide ce măsuri trebuie adoptate pentru a atenua riscurile respective.

Obiectivele declarate pot fi mai bine realizate la nivelul UE, decât de către statele membre în mod individual, având în vedere aspectele transfrontaliere ale incidentelor și riscurilor de NIS. Prin urmare, UE poate adopta măsuri în conformitate cu principiul subsidiarității stabilit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității, directiva propusă nu depășește ceea ce este necesar pentru atingerea obiectivelor respective.

În vederea realizării obiectivelor, Comisia trebuie să fie împuternicită să adopte acte delegate în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene, pentru a completa sau a modifica anumite elemente neesențiale ale actului de bază. Propunerea Comisiei este orientată și către susținerea proporționalității în punerea în aplicare a obligațiilor impuse operatorilor privați și publici

În vederea asigurării unor condiții uniforme de punere în aplicare a actului de bază, Comisia trebuie să fie împuternicită să adopte acte de punere în aplicare în conformitate cu articolul 291 din Tratatul privind funcționarea Uniunii Europene.

Având în vedere în special domeniul larg de aplicare al directivei propuse și faptul că aceasta abordează domenii puternic reglementate, precum și obligațiile legale care decurg din capitolul IV al directivei, este necesar ca notificarea măsurilor de transpunere să fie însoțită de documente explicative. În conformitate cu Declarația politică comună a statelor membre și a Comisiei din 28 septembrie 2011 privind documentele explicative, statele membre s-au angajat să transmită, în cazuri justificate, împreună cu notificarea măsurilor de transpunere unul sau mai multe documente care să explice relația dintre componentele unei directive și părțile corespunzătoare din instrumentele naționale de transpunere. În cazul prezentei directive, legislatorul consideră că transmiterea unor astfel de documente este justificată.

4. IMPLICAȚIILE BUGETARE

Statele membre trebuie să utilizeze pentru cooperare și schimb de informații o infrastructură securizată. Propunerea va avea implicații pentru bugetul UE numai dacă statele membre optează pentru adaptarea infrastructurii existente (de exemplu sTESTA) și încredințează Comisiei această sarcină în contextul CFM 2014-2020. Costul unic este estimat la 1 250 000

EUR și urmează să fie suportat din bugetul UE, linia bugetară 09.03.02 (promovarea interconectării și a interoperabilității serviciilor publice naționale online, precum și a accesului la astfel de rețele – capitolul 09.03, mecanismul „Conectarea Europei” – rețele de telecomunicații), cu condiția să existe suficiente fonduri disponibile în cadrul MCE. În mod alternativ, statele membre pot fie să-și asume împreună costul unic de adaptare a unei infrastructuri existente, fie să decidă crearea unei noi infrastructuri și să suporte costurile aferente, estimate la aproximativ 10 milioane EUR pe an.

2013/0027 (COD)

Propunere de

DIRECTIVĂ A PARLAMENTULUI EUROPEAN ŞI A CONSILIULUI

privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune

PARLAMENTUL EUROPEAN ȘI CONSILIUL UNIUNII EUROPENE,

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

având în vedere propunerea Comisiei Europene,

după transmiterea proiectului de act legislativ către parlamentele naționale,

având în vedere avizul Comitetului Economic și Social European[1],

după consultarea Autorității Europene pentru Protecția Datelor,

hotărând în conformitate cu procedura legislativă ordinară,

întrucât:

(1) Rețelele împreună cu sistemele și serviciile informatice îndeplinesc un rol vital în societate. Fiabilitatea și securitatea lor sunt esențiale pentru activitățile economice și bunăstarea socială și, în special, pentru funcționarea pieței interne.

(2) Amploarea și frecvența incidentelor de securitate provocate deliberat sau întâmplătoare este în creștere și reprezintă o amenințare majoră pentru funcționarea rețelelor și a sistemelor informatice. Astfel de incidente pot să împiedice desfășurarea activităților economice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore economiei Uniunii.

(3) Ca instrumente de comunicare fără frontiere, sistemele de informare digitale și, în principal, internetul au un rol esențial în facilitarea circulației transfrontaliere a mărfurilor, serviciilor și persoanelor. Din cauza naturii lor transnaționale, o perturbare majoră a acestor sisteme survenită într-un stat membru poate afecta, de asemenea, alte state membre și Uniunea în ansamblul său. Prin urmare, reziliența și stabilitatea rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței interne.

(4) Trebuie stabilit un mecanism de cooperare la nivelul Uniunii, care să permită schimbul de informații, precum și detectarea și răspunsul coordonate în ceea ce privește securitatea rețelelor și a informației (*network and information security* - NIS). Pentru ca acest mecanism să fie eficace și să includă toate statele membre, este esențial ca acestea să dispună de capacitățile minime necesare și de o strategie care să asigure un nivel ridicat de NIS pe teritoriul lor. Administrațiile publice și operatorii infrastructurilor critice de informație trebuie să fie supuși, de asemenea, unor cerințe minime de securitate, pentru a promova o cultură a gestionării riscurilor și a asigura raportarea celor mai grave incidente.

[1] JO C […], […], p. […].

(5) Pentru a putea acoperi toate incidentele și riscurile relevante, prezenta directivă trebuie să se aplice tuturor rețelelor și sistemelor informatice. Obligațiile impuse administrațiilor publice și operatorilor de piață nu trebuie să se aplice însă întreprinderilor care furnizează rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului în sensul Directivei 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directiva-cadru)[2], care sunt supuse cerințelor specifice de securitate și integritate stabilite la articolul 13a din directiva respectivă, și nici furnizorilor de servicii de asigurare a încrederii.

(6) Capacitățile existente nu sunt suficiente pentru a asigura un nivel ridicat de securitate a rețelelor și a informației în Uniune. Statele membre au niveluri de pregătire foarte diferite care conduc la existența în Uniune a unor abordări fragmentate. Acest lucru determină un nivel inegal de protecție a consumatorilor și a întreprinderilor și subminează nivelul general de securitate a rețelelor și a informației în Uniune. La rândul său, lipsa unor cerințe minime comune pentru administrațiile publice și operatorii de piață face imposibilă instituirea unui mecanism global eficace de cooperare la nivelul Uniunii.

(7) Prin urmare, pentru a răspunde cu eficacitate la provocările din domeniul securității rețelelor și a sistemelor informatice este necesară o abordare globală la nivelul Uniunii, care să includă crearea capacităților comune minime și cerințele de planificare, schimbul de informații și coordonarea acțiunilor, precum și cerințele minime comune de securitate pentru toți operatorii de piață în cauză și pentru administrațiile publice.

(8) Dispozițiile prezentei directive nu trebuie să aducă atingere posibilității de care dispune fiecare stat membru de a lua măsurile necesare pentru a asigura protecția intereselor sale de securitate esențiale, a apăra ordinea și siguranța publică și a permite investigarea, detectarea și urmărirea infracțiunilor. În conformitate cu articolul 346 din TFUE, niciun stat membru nu are obligația de a furniza informații a căror divulgare o consideră contrară intereselor esențiale ale siguranței sale.

(9) Pentru a atinge și menține un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice, fiecare stat membru trebuie să aibă o strategie națională de securitate a rețelelor și a informației, care să definească obiectivele strategice și acțiunile concrete de politică ce trebuie puse în aplicare. Pentru a atinge niveluri ale capacității de răspuns care să permită o cooperare eficace și eficientă la nivel național și al Uniunii în caz de incidente, trebuie elaborate la nivel național planuri de cooperare în domeniul securității rețelelor și informației, care să respecte cerințele esențiale.

(10) Pentru a asigura aplicarea eficace a dispozițiilor adoptate în temeiul prezentei directive, trebuie înființat sau identificat în fiecare stat membru un organism responsabil cu coordonarea problemelor de securitate a rețelelor și a informației, care să constituie punctul focal al cooperării transfrontaliere la nivelul Uniunii. Aceste organisme trebuie să dispună de resurse tehnice, financiare și umane adecvate, pentru a-și îndeplini în mod eficace și eficient sarcinile atribuite și a realiza astfel obiectivele prezentei directive.

---

[2] JO L 108, 24.4.2002, p. 33.

(11) Toate statele membre trebuie să fie echipate în mod adecvat, din punctul de vedere al capacității atât tehnice, cât și organizatorice, pentru a preveni, a detecta, a combate și a atenua incidentele și riscurile la care sunt supuse rețelele și sistemele informatice. Prin urmare, în toate statele membre trebuie înființate echipe de intervenție în caz de urgență informatică funcționale și care să respecte cerințele esențiale, pentru a garanta existența capacităților eficace și compatibile care să administreze incidentele și riscurile și să asigure o cooperare eficientă la nivelul Uniunii.

(12) Pe baza progreselor semnificative obținute în cadrul Forumului european al statelor membre (FESM) în încurajarea dezbaterilor și a schimburilor de bune practici, inclusiv a elaborării principiilor de cooperare în caz de criză informatică europeană, statele membre și Comisia trebuie să formeze o rețea prin intermediul căreia să comunice permanent și care să susțină cooperarea lor. Acest mecanism de cooperare sigur și eficace trebuie să permită schimbul de informații, detectarea și răspunsul structurate și coordonate la nivelul Uniunii.

(13) Este necesar ca Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) să asiste statele membre și Comisia, oferind experiența sa, asigurând consiliere și facilitând schimbul de bune practici. În special la aplicarea prezentei directive, Comisia trebuie să consulte ENISA. Pentru a asigura o informare eficace și în timp util a statelor membre și a Comisiei, în rețeaua de cooperare trebuie să poată fi transmise alerte rapide cu privire la incidente și riscuri. În vederea dezvoltării capacităților și a cunoștințelor statelor membre, rețeaua de cooperare trebuie să funcționeze, de asemenea, ca un instrument pentru schimbul de bune practici, asistând membrii săi la crearea capacităților și coordonând organizarea evaluărilor inter pares și a exercițiilor de NIS.

(14) Trebuie creată o infrastructură de schimb de informații securizată, care să permită schimbul de informații sensibile și confidențiale în rețeaua de cooperare. Fără a aduce atingere obligației de a notifica rețelei de cooperare incidentele și riscurile care ating o dimensiune europeană, accesul la informațiile confidențiale provenind de la alte state membre trebuie acordat numai statelor membre care demonstrează că procedurile și resursele lor tehnice, financiare și umane, precum și infrastructura lor de comunicații le garantează o participare în rețea eficace, eficientă și sigură.

(15) Deoarece majoritatea rețelelor și a sistemelor informatice au operatori privați, cooperarea dintre sectorul public și cel privat este esențială. Operatorii de piață trebuie încurajați să-și creeze propriile mecanisme de cooperare informală pentru asigurarea securității rețelelor și a informației. Aceștia trebuie, de asemenea, să coopereze cu sectorul public și să facă schimb de informații și de bune practici, în schimbul sprijinului operațional în caz de incident.

(16) Pentru a asigura transparența și informarea adecvată a cetățenilor și a operatorilor de piață din UE, autoritățile competente trebuie să creeze un site web comun, pe care să publice informații neconfidențiale despre incidente și riscuri.

(17) Dacă informațiile sunt considerate confidențiale în conformitate cu normele Uniunii și cele naționale privind secretul comercial, această confidențialitate trebuie asigurată atunci când se efectuează activitățile și se îndeplinesc obiectivele stabilite de prezenta directivă.

(18) În special pe baza experiențelor naționale în materie de gestionare a crizelor și în cooperare cu ENISA, Comisia și statele membre elaborează un plan al Uniunii de cooperare în domeniul securității rețelelor și a informației, care definește mecanismele

de cooperare pentru contracararea riscurilor și a incidentelor. La administrarea avertismentelor rapide în cadrul rețelei de cooperare, trebuie să se țină seama în mod corespunzător de acest plan.

(19) Transmiterea în rețea a unei alerte rapide trebuie impusă numai dacă amploarea și gravitatea incidentului sau a riscului în cauză ating sau pot atinge un nivel la care este necesară o informare sau o coordonare a răspunsului la nivelul Uniunii. Prin urmare, alertele rapide trebuie să se limiteze la incidentele sau la riscurile reale sau potențiale care se extind rapid, depășesc capacitatea națională de răspuns sau afectează mai multe state membre. Pentru a permite o evaluare corectă, toate informațiile relevante pentru evaluarea riscului sau a incidentului trebuie comunicate rețelei de cooperare.

(20) După primirea și evaluarea unei alerte rapide, autoritățile competente trebuie să convină asupra unui răspuns coordonat, în conformitate cu planul Uniunii de cooperare în domeniul securității rețelelor și a informației. Autoritățile competente și Comisia trebuie informate cu privire la măsurile adoptate la nivel național ca urmare a răspunsului coordonat.

(21) Având în vedere dimensiunea mondială a problemelor de securitate a rețelelor și a informației, este nevoie de o cooperare internațională mai strânsă pentru a îmbunătăți standardele de securitate și schimbul de informații și pentru a promova o abordare internațională comună a acestor probleme.

(22) Responsabilitatea asigurării securității rețelelor și a informației revine în mare măsură administrațiilor publice și operatorilor de piață. Trebuie promovată și dezvoltată prin intermediul unor cerințe adecvate de reglementare și al practicilor voluntare din sector o cultură a gestionării riscurilor, care să implice evaluarea riscurilor și aplicarea unor măsuri de securitate adecvate riscurilor întâmpinate. Pentru ca rețeaua de cooperare să funcționeze în mod eficace, este esențială, de asemenea, stabilirea unor condiții uniforme care să asigure o cooperare eficientă între toate statele membre.

(23) În conformitate cu Directiva 2002/21/CE, întreprinderile furnizoare de rețele de comunicații publice sau de servicii de comunicații electronice accesibile publicului trebuie să ia măsurile adecvate pentru a garanta integritatea și securitatea acestora și trebuie să introducă cerințe de notificare a încălcării securității și a pierderii integrității. În conformitate cu Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice)[3], furnizorul unor servicii de comunicații electronice accesibile publicului trebuie să ia măsurile tehnice și organizatorice adecvate pentru a garanta securitatea acestora.

(24) Aceste obligații trebuie extinse dincolo de sectorul comunicațiilor electronice la principalii furnizori de servicii ale societății informaționale, definite în Directiva 98/34/CE a Parlamentului European și a Consiliului din 22 iunie 1998 referitoare la procedura de furnizare de informații în domeniul standardelor, reglementărilor tehnice și al normelor privind serviciile societății informaționale[4], pe care se bazează serviciile din aval ale societății informaționale sau activitățile online, cum ar fi platformele de comerț electronic, serviciile de procesare a plăților online, rețelele de socializare, motoarele de căutare, serviciile de cloud computing sau vânzarea de aplicații. Perturbarea acestor servicii suport ale societății informaționale împiedică furnizarea

[3] JO L 201, 31.7.2002, p. 37.
[4] JO L 204, 21.7.1998, p. 37.

altor servicii ale societății informaționale care se bazează pe primele ca elemente-cheie. Dezvoltatorii de programe informatice și producătorii de echipamente informatice nu sunt furnizori de servicii ale societății informaționale și, prin urmare, se exclud. Aceste obligații trebuie extinse, de asemenea, la administrațiile publice și la operatorii de infrastructură critică, ce utilizează intens tehnologia informației și comunicațiilor și sunt esențiali pentru funcționarea sectoarelor vitale ale economiei sau societății, cum ar fi energia electrică și gazele naturale, transporturile, instituțiile de credit, bursele și sănătatea. Perturbarea acestor rețele și sisteme informatice ar afecta piața internă.

(25) Măsurile tehnice și organizatorice impuse administrațiilor publice și operatorilor de piață nu trebuie să implice proiectarea, dezvoltarea sau fabricarea într-un anumit mod a unui anumit produs comercial al tehnologiei informației și comunicațiilor.

(26) Administrațiile publice și operatorii de piață trebuie să asigure securitatea rețelelor și a sistemelor aflate sub controlul lor. Acestea sunt în principal rețele și sisteme private, gestionarea securității lor fiind fie efectuată de către personalul IT intern, fie externalizată. Obligațiile în materie de securitate și notificare trebuie să se aplice operatorilor de piață relevanți și administrațiilor publice, indiferent dacă aceștia asigură ei înșiși întreținerea propriilor rețele și sisteme informatice sau externalizează această activitate.

(27) Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra micilor operatori și a utilizatorilor, cerințele trebuie să fie proporționale cu riscurile la care este expusă rețeaua sau sistemul informatic în cauză, ținând seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. Aceste cerințe nu trebuie să se aplice microîntreprinderilor.

(28) Autoritățile competente trebuie să acorde atenția cuvenită menținerii unor canale informale și sigure pentru schimbul de informații dintre operatorii de pe piață și dintre sectorul public și cel privat. Anunțarea publică a incidentelor raportate autorităților competente trebuie să găsească echilibrul cuvenit între interesul publicului de a fi informat cu privire la amenințări și eventualele daune comerciale sau în domeniul reputației pe care le pot suferi administrațiile publice și operatorii de piață care raportează incidentele. Atunci când sunt puse în aplicare obligațiile de notificare, autoritățile competente trebuie să acorde o atenție deosebită necesității de a păstra stricta confidențialitate a informațiilor despre vulnerabilitățile unui produs, înainte de apariția unor soluții de securitate adecvate.

(29) Autoritățile competente trebuie să dispună de mijloacele necesare pentru a-și îndeplini sarcinile, inclusiv de împuternicirea de a solicita operatorilor de piață și administrațiilor publice suficiente informații pentru a putea evalua nivelul de securitate al rețelelor și al sistemelor informatice, precum și date credibile și cuprinzătoare privind incidentele reale care au avut impact asupra funcționării rețelelor și a sistemelor informatice.

(30) În multe cazuri, incidentele sunt rezultatul activităților infracționale. Caracterul penal al incidentelor poate fi presupus, chiar dacă dovezile care îl atestă nu sunt suficient de clare de la început. În acest context, cooperarea adecvată dintre autoritățile competente și autoritățile de aplicare a legii trebuie să facă parte din răspunsul global eficace dat amenințării pe care o reprezintă incidentele de securitate. Pentru promovarea unui mediu sigur, securizat și mai rezilient este nevoie, în special, de raportarea în mod sistematic către autoritățile de aplicare a legii a incidentelor cu presupus caracter penal

grav. Caracterul penal grav al incidentelor trebuie evaluat în lumina legislației UE privind criminalitatea informatică.

(31) În multe cazuri, datele cu caracter personal sunt compromise în urma unor incidente. În acest context, autoritățile competente și autoritățile de protecție a datelor trebuie să coopereze și să facă schimb de informații cu privire la toate aspectele relevante pentru abordarea cazurilor de încălcare a securității datelor cu caracter personal în urma unor incidente. Statele membre trebuie să pună în aplicare obligația de a notifica incidentele de securitate într-un mod care reduce la minimum sarcina administrativă în cazurile în care incidentul de securitate este și o încălcare a securității datelor cu caracter personal în conformitate cu Regulamentul Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date[5]. Colaborând cu autoritățile competente și cu autoritățile de protecție a datelor, ENISA poate contribui la elaborarea unor mecanisme și formulare de schimb de informații, care să evite necesitatea de a utiliza două formulare de notificare. Formularul unic de notificare facilitează raportarea incidentelor care compromit datele cu caracter personal, reducând astfel sarcina administrativă impusă întreprinderilor și administrațiilor publice.

(32) Standardizarea cerințelor de securitate este un proces impulsionat de piață. Pentru a asigura o aplicare convergentă a standardelor de securitate, statele membre trebuie să încurajeze respectarea standardelor indicate sau conformitatea cu acestea, în vederea garantării unui nivel ridicat de securitate la nivelul Uniunii. În acest scop, ar putea fi necesară elaborarea unor standarde armonizate în conformitate cu Regulamentul (UE) nr. 1025/2012 al Parlamentului European și al Consiliului din 25 octombrie 2012 privind standardizarea europeană, de modificare a Directivelor 89/686/CEE și 93/15/CEE ale Consiliului și a Directivelor 94/9/CE, 94/25/CE, 95/16/CE, 97/23/CE, 98/34/CE, 2004/22/CE, 2007/23/CE, 2009/23/CE și 2009/105/CE ale Parlamentului European și ale Consiliului și de abrogare a Deciziei 87/95/CEE a Consiliului și a Deciziei nr. 1673/2006/CE a Parlamentului European și a Consiliului[6].

(33) Comisia trebuie să revizuiască periodic prezenta directivă, în special pentru a stabili dacă este necesară efectuarea unor modificări ca urmare a evoluției tehnologiei sau a condițiilor de piață.

(34) Pentru a permite buna funcționare a rețelei de cooperare, Comisiei trebuie să i se delege competența de a adopta acte în conformitate cu articolul 290 din Tratatul privind funcționarea Uniunii Europene referitoare la definirea criteriilor pe care trebuie să le îndeplinească un stat membru pentru a fi autorizat să participe la sistemul securizat de schimb de informații, specificarea mai detaliată a evenimentelor care declanșează alerta rapidă și definirea circumstanțelor în care operatorii de piață și administrațiile publice au obligația de a notifica incidentele.

(35) Este deosebit de important ca, în cursul activităților sale pregătitoare, Comisia să organizeze consultări adecvate, inclusiv la nivel de experți. Atunci când pregătește și redactează acte delegate, Comisia trebuie să asigure transmiterea simultană, în timp util și în mod adecvat a documentelor relevante către Parlamentul European și Consiliu.

(36) În vederea asigurării unor condiții uniforme de punere în aplicare a prezentei directive, Comisiei trebuie să i se confere competențe de executare în ceea ce privește

---

5 SEC(2012) 72 final.

6 JO L 316, 14.11.2012, p. 12.

cooperarea dintre autoritățile competente și Comisie în cadrul rețelei de cooperare, accesul la infrastructura securizată de schimb de informații, planul Uniunii de cooperare în domeniul securității rețelelor și a informației, formularele și procedurile aplicabile pentru informarea publicului cu privire la incidente și standardele și/sau specificațiile tehnice relevante pentru securitatea rețelelor și a informației. Aceste competențe trebuie exercitate în conformitate cu Regulamentul (UE) nr. 182/2011 al Parlamentului European și al Consiliului din 16 februarie 2011 de stabilire a normelor și principiilor generale privind mecanismele de control de către statele membre al exercitării competențelor de executare de către Comisie[7].

(37) În ceea ce privește aplicarea prezentei directive, Comisia trebuie să colaboreze, după caz, cu comitetele sectoriale relevante și cu organismele relevante instituite la nivelul UE în special în domeniile energiei, transporturilor și sănătății.

(38) Informațiile considerate confidențiale de către o autoritate competentă în conformitate cu normele Uniunii și cele naționale privind secretul comercial trebuie să facă obiectul schimbului de informații cu Comisia și cu alte autorități competente, numai dacă acest lucru este strict necesar pentru aplicarea prezentei directive. Schimbul de informații trebuie să se limiteze la informațiile relevante și să fie proporțional cu scopul urmărit.

(39) Schimbul de informații cu privire la riscuri și incidente desfășurat în cadrul rețelei de cooperare și îndeplinirea cerințelor de notificare a incidentelor către autoritățile naționale competente pot necesita prelucrarea datelor cu caracter personal. O astfel de prelucrare este necesară pentru realizarea obiectivelor de interes public urmărite de prezenta directivă și, prin urmare, este legitimă în temeiul articolului 7 din Directiva 95/46/CE. Aceasta nu constituie, din perspectiva obiectivelor legitime respective, o intervenție disproporționată și intolerabilă care să afecteze substanța însăși a dreptului la protecția datelor cu caracter personal garantat prin articolul 8 din Carta drepturilor fundamentale. În aplicarea prezentei directive, 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[8] se aplică, după caz. Atunci când datele sunt prelucrate de instituțiile și organele Uniunii în scopul punerii în aplicare a prezentei directive, o astfel de prelucrare trebuie să respecte Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului din 18 decembrie 2000 privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal de către instituțiile și organele comunitare și privind libera circulație a acestor date.

(40) Deoarece obiectivele prezentei directive, și anume asigurarea unui nivel ridicat de securitate a rețelelor și a informației în Uniune, nu pot fi realizate în măsură suficientă de către statele membre în mod individual și, prin urmare, din motive de efect al acțiunii, pot fi realizate mai bine la nivelul Uniunii, Uniunea poate adopta măsuri în conformitate cu principiul subsidiarității stabilit la articolul 5 din Tratatul privind Uniunea Europeană. În conformitate cu principiul proporționalității prevăzut la același articol, prezenta directivă nu depășește ceea ce este necesar pentru atingerea obiectivelor respective.

(41) Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o

[7] JO L 55, 28.2.2011, p. 13.
[8] JO L 145, 31.5.2001, p. 43.

cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă trebuie pusă în aplicare în conformitate cu aceste drepturi și principii.

ADOPTĂ PREZENTA DIRECTIVĂ:

CAPITOLUL I

DISPOZIȚII GENERALE

Articolul 1

Obiect și domeniu de aplicare

1. Prezenta directivă stabilește măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației (*network and information security* - NIS) în Uniune.

2. În acest scop, prezenta directivă:

(a) stabilește obligații pentru toate statele membre în ceea ce privește prevenirea și administrarea riscurilor și a incidentelor care afectează rețelele și sistemele informatice, precum și răspunsul la acestea;

(b) creează un mecanism de cooperare între statele membre pentru a asigura o aplicare uniformă a prezentei directive în Uniune și, dacă este necesar, o administrare și un răspuns coordonate și eficiente în caz de riscuri și incidente care afectează rețelele și sistemele informatice;

(c) stabilește cerințele de securitate pentru operatorii de piață și administrațiile publice.

3. Cerințele de securitate prevăzute la articolul 14 nu se aplică întreprinderilor care furnizează rețele de comunicații publice sau servicii de comunicații electronice accesibile publicului în sensul Directivei 2002/21/CE și care trebuie să respecte cerințele specifice de securitate și integritate prevăzute la articolele 13a și 13b din directiva respectivă și nici furnizorilor de servicii de asigurare a încrederii.

4. Prezenta directivă nu aduce atingere legislației UE privind criminalitatea informatică și nici Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora[9].

5. De asemenea, prezenta directivă nu aduce atingere Directivei 95/46/CE a Parlamentului European și a Consiliului din 24 octombrie 1995 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date[10] și nici Directivei 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice sau Regulamentului Parlamentului European și Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date[11].

6. Schimbul de informații în cadrul rețelei de cooperare prevăzut la capitol III și notificarea incidentelor de securitate a rețelelor și a informației prevăzută la articolul 14 pot necesita prelucrarea datelor cu caracter personal. O astfel de prelucrare, care

---

9 JO L 345, 23.12.2008, p. 75.

10 JO L 281, 23.11.1995, p. 31.

11 SEC(2012) 72 final.

este necesară pentru realizarea obiectivelor de interes public urmărite de prezenta directivă, trebuie autorizată de statul membru în temeiul articolului 7 din Directiva 95/46/CE și al Directivei 2002/58/CE, astfel cum au fost transpuse în legislația națională.

Articolul 2

Armonizarea minimă

Statele membre nu sunt împiedicate să adopte sau să mențină dispoziții care asigură un nivel de securitate mai ridicat și nu aduc atingere obligațiilor lor prevăzute de legislația Uniunii.

Articolul 3

Definiții

În sensul prezentei directive, se aplică următoarele definiții:

(1) „rețea și sistem informatic” înseamnă:

(a) o rețea de comunicații electronice în sensul Directivei 2002/21/CE și

(b) orice dispozitiv sau grup de dispozitive interconectate sau legate între ele, dintre care unul sau mai multe efectuează, în conformitate cu un program, o prelucrare automată a datelor electronice, precum și

(c) datele electronice stocate, prelucrate, recuperate sau transmise de elementele prevăzute la literele (a) și (b) în vederea funcționării, utilizării, protejării și întreținerii lor.

(2) „securitate” înseamnă capacitatea unei rețele sau a unui sistem informatic de a rezista, la un nivel de încredere dat, unei acțiuni accidentale sau răuvoitoare care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de rețeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora;

(3) „risc” înseamnă orice circumstanță sau eveniment care are un efect negativ potențial asupra securității;

(4) „incident” înseamnă orice circumstanță sau eveniment care are un efect negativ real asupra securității;

(5) „serviciu al societății informaționale” înseamnă un serviciu în sensul articolului 1 punctul 2 din Directiva 98/34/CE;

(6) „plan de cooperare în domeniul securității rețelelor și a informației” înseamnă un plan care stabilește un cadru pentru rolurile organizaționale, responsabilitățile și procedurile de menținere sau de restabilire a funcționării rețelelor și sistemelor informatice în cazul în care acestea sunt afectate de un risc sau de un incident;

(7) „administrarea incidentului” înseamnă toate procedurile utilizate pentru analiză, limitare și răspuns în cazul unui incident;

(8) „operator de piață” înseamnă:

(a) un furnizor de servicii ale societății informaționale care permit furnizarea altor servicii ale societății informaționale; o listă neexhaustivă a acestor furnizori este prevăzută în anexa II;

(b) un operator al unei infrastructuri critice care este esențială pentru menținerea activităților economice și societale vitale în domeniile energiei, transporturilor, serviciilor bancare, burselor și sănătății; o listă neexhaustivă a acestor operatori este prevăzută în anexa II.

(9) „standard” înseamnă un standard menționat în Regulamentul (UE) nr. 1025/2012;

(10) „specificație” înseamnă o specificație menționată în Regulamentul (UE) nr. 1025/2012;

(11) „furnizor de servicii de asigurare a încrederii” înseamnă o persoană fizică sau juridică ce furnizează orice serviciu electronic constând în crearea, verificarea, validarea, administrarea și păstrarea semnăturilor electronice, a sigiliilor electronice, a mărcilor temporale electronice, a documentelor electronice, a serviciilor de distribuție electronică, a autentificării unui site web și a certificatelor electronice, inclusiv a certificatelor pentru semnături electronice și sigilii electronice.

CAPITOLUL II

CADRELE NAȚIONALE DE SECURITATE A REȚELELOR ȘI A INFORMAȚIILOR

Articolul 4

Principiu

Statele membre asigură un nivel ridicat de securitate a rețelelor și a sistemelor informatice pe teritoriul lor în conformitate cu prezenta directivă.

Articolul 5

Strategia națională privind securitatea rețelelor și a informației și planul național de cooperare în domeniul securității rețelelor și a informației

1. Fiecare stat membru adoptă o strategie națională privind securitatea rețelelor și a informației care definește obiectivele strategice și măsurile concrete de politică și de reglementare necesare pentru a atinge și menține un nivel ridicat de securitate a rețelelor și a informației. Strategia națională privind NIS se referă, în special, la următoarele aspecte:

(a) definirea obiectivelor și a priorităților, pe baza unei analize actualizate a riscurilor și a incidentelor;

(b) un cadru de guvernanță pentru realizarea obiectivelor și a priorităților, inclusiv o definire clară a rolurilor și a responsabilităților organismelor guvernamentale și ale altor actori relevanți;

(c) identificarea măsurilor generale referitoare la gradul de pregătire, răspuns și redresare, inclusiv a mecanismelor de cooperare dintre sectorul public și cel privat;

(d) indicarea programelor de instruire, sensibilizare și formare;

(e) planurile de cercetare și dezvoltare și o descriere a modului în care aceste planuri reflectă prioritățile identificate.

2. Strategia națională privind NIS include un plan național de cooperare în domeniul NIS care cuprinde cel puțin următoarele:

(a) un plan de evaluare a riscurilor pentru a identifica riscurile și a evalua impactul unor incidente potențiale;

(b) definirea rolurilor și a responsabilităților diferiților actori implicați în punerea în aplicare a planului;

(c) definirea procedurilor de cooperare și de comunicare care asigură prevenirea, detectarea, răspunsul, repararea și redresarea, modulate în funcție de nivelul de alertă;

(d) o foaie de parcurs pentru exercițiile și formarea în domeniul NIS, destinate consolidării, validării și testării planului. Învățămintele desprinse trebuie documentate și integrate în actualizările planului.

3. Strategia națională privind NIS și planul național de cooperare în domeniul NIS sunt comunicate Comisiei în termen de o lună de la adoptarea lor.

Articolul 6

Autoritatea națională competentă în domeniul securității rețelelor și a sistemelor informatice

1. Fiecare stat membru desemnează o autoritate națională competentă în domeniul securității rețelelor și a sistemelor informatice (denumită în continuare „autoritatea competentă”).

2. Autoritățile competente monitorizează aplicarea prezentei directive la nivel național și contribuie la aplicarea uniformă a acesteia în întreaga Uniune.

3. Statele membre se asigură că autoritățile competente dispun de resursele tehnice, financiare și umane adecvate pentru a-și îndeplini în mod eficace și eficient sarcinile atribuite și a realiza astfel obiectivele prezentei directive. Statele membre asigură cooperarea eficace, eficientă și sigură a autorităților competente prin intermediul rețelei menționate la articolul 8.

4. Statele membre se asigură că autoritățile competente primesc de la administrațiile publice și de la operatorii de piață notificările incidentelor, astfel cum prevede articolul 14 alineatul (2), și că le sunt conferite competențele de punere în aplicare și de executare menționate la articolul 15.

5. Autoritățile competente se consultă și cooperează, după caz, cu autoritățile naționale de aplicare a legii și cu autoritățile de protecție a datelor competente.

6. Fiecare stat membru notifică fără întârziere Comisiei autoritatea competentă desemnată și sarcinile sale, precum și orice modificări ulterioare ale acestora. Fiecare stat membru comunică publicului autoritatea competentă desemnată.

Articolul 7

Echipa de intervenție în caz de urgență informatică

1. Fiecare stat membru înființează o Echipă de intervenție în caz de urgență informatică (denumită în continuare „CERT”) care este responsabilă pentru administrarea incidentelor și a riscurilor în conformitate cu o procedură bine definită și respectă cerințele stabilite în anexa I punctul (1). CERT poate fi înființată în cadrul autorității competente.

2. Statele membre se asigură că CERT dispun de resursele tehnice, financiare și umane adecvate pentru a-și îndeplini în mod eficace sarcinile stabilite în anexa I punctul (2).

3. Statele membre se asigură că CERT au la dispoziție o infrastructură securizată și rezilientă de comunicare și informare la nivel național, care este compatibilă și interoperabilă cu sistemul securizat de schimb de informații menționat la articolul 9.

4. Statele membre comunică Comisiei resursele și mandatul CERT, precum și procedura acestora de administrare a incidentelor.

5. CERT acționează sub supravegherea autorității competente, care reexaminează cu regularitate caracterul adecvat al resurselor și al mandatului, precum și eficacitatea procedurii de administrare a incidentelor.

CAPITOLUL III

COOPERAREA DINTRE AUTORITĂȚILE COMPETENTE

Articolul 8

Rețeaua de cooperare

1. Autoritățile competente și Comisia formează o rețea („rețeaua de cooperare”) pentru a coopera în domeniul combaterii riscurilor și incidentelor care afectează rețelele și sistemele informatice.

2. Prin intermediul rețelei de cooperare, Comisia și autoritățile competente se află în contact permanent. La cerere, Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) asistă rețeaua de cooperare, oferind experiență și consiliere.

3. În cadrul rețelei de cooperare, autoritățile competente:

   (a) transmit alerte rapide privind riscurile și incidentele în conformitate cu articolul 10;

   (b) asigură un răspuns coordonat în conformitate cu articolul 11;

   (c) publică cu regularitate pe un site web comun informații neconfidențiale privind alertele rapide și răspunsul coordonat în curs;

   (d) la cererea unui stat membru sau a Comisiei, discută și evaluează împreună una sau mai multe strategii naționale privind NIS sau planuri naționale de cooperare în domeniul NIS, menționate la articolul 5, în domeniul de aplicare al prezentei directive;

   (e) la cererea unui stat membru sau a Comisiei, discută și evaluează împreună eficacitatea echipelor CERT, în special atunci când au loc la nivelul Uniunii exerciții de NIS;

   (f) cooperează și fac schimb de informații cu privire la toate aspectele relevante cu Centrul european de combatere a criminalității informatice din cadrul Europol și cu alte organisme europene relevante, în special în domeniile protecției datelor, energiei, transporturilor, serviciilor bancare, burselor și sănătății;

   (g) fac schimb de informații și bune practici între ele și cu Comisia și își acordă reciproc asistență în ceea ce privește crearea capacităților din domeniul NIS;

   (h) organizează cu regularitate evaluări inter pares privind capacitățile și nivelul de pregătire;

   (i) organizează exerciții de NIS la nivelul Uniunii și participă, după caz, la exercițiile internaționale de NIS.

4. Comisia stabilește, prin acte de punere în aplicare, măsurile necesare pentru a facilita cooperarea dintre autoritățile competente și Comisie menționată la alineatele (2) și (3). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de consultare menționată la articolul 19 alineatul (2).

Articolul 9

Sistemul securizat de schimb de informații

1. Pentru schimbul de informații sensibile și confidențiale desfășurat în rețeaua de cooperare este utilizată o infrastructură securizată.

2. Comisia este împuternicită să adopte, în conformitate cu articolul 18, acte delegate privind definirea criteriilor pe care trebuie să le îndeplinească un stat membru pentru a fi autorizat să participe la sistemul securizat de schimb de informații, referitoare la:

   (a) disponibilitatea unei infrastructuri securizate și reziliente de comunicare și informare la nivel național, compatibilă și interoperabilă cu infrastructura securizată a rețelei de cooperare în conformitate cu articolul 7 alineatul (3) și

   (b) existența unor resurse tehnice, financiare și umane și a unor proceduri adecvate pentru participarea eficace, eficientă și sigură a autorităților competente și a CERT la sistemul securizat de schimb de informații în temeiul articolului 6 alineatul (3), al articolului 7 alineatul (2) și al articolului 7 alineatul (3).

3. Comisia adoptă, prin acte de punere în aplicare, decizii privind accesul statelor membre la această infrastructură securizată, în conformitate cu criteriile menționate la alineatele (2) și (3). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 19 alineatul (3).

Articolul 10

Alertele rapide

1. Autoritățile competente sau Comisia transmit alerte rapide în cadrul rețelei de cooperare cu privire la riscurile și incidentele care îndeplinesc cel puțin una dintre următoarele condiții:

   (a) cresc rapid sau pot crește rapid în amploare;

   (b) depășesc sau pot depăși capacitatea națională de răspuns;

   (c) afectează sau pot afecta mai multe state membre.

2. În cadrul alertelor rapide, autoritățile competente și Comisia comunică orice informațiile relevante aflate în posesia lor și care pot fi utile pentru evaluarea riscului sau a incidentului.

3. La cererea unui stat membru sau din proprie inițiativă, Comisia poate solicita altui stat membru să furnizeze orice informații relevante cu privire la un risc sau la un incident specific.

4. Dacă riscul sau incidentul care face obiectul alertei rapide are un presupus caracter penal, autoritățile competente sau Comisia informează Centrul european de combatere a criminalității informatice din cadrul Europol.

5. Comisia este împuternicită să adopte, în conformitate cu articolul 18, acte delegate privind specificarea mai detaliată a riscurilor și a incidentelor care declanșează alerta rapidă menționată la alineatul (1).

Articolul 11

Răspunsul coordonat

1. După transmiterea alertei rapide menționate la articolul 10, autoritățile competente convin, în urma evaluării informațiilor relevante, asupra unui răspuns coordonat în conformitate cu planul Uniunii de cooperare în domeniul NIS menționat la articolul 12.

2. Diferitele măsuri adoptate la nivel național ca urmare a răspunsului coordonat se comunică rețelei de cooperare.

Articolul 12

Planul Uniunii de cooperare în domeniul securității rețelelor și a informației

1. Comisia este împuternicită să adopte, prin acte de punere în aplicare, un plan al Uniunii de cooperare în domeniul securității rețelelor și informației. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 19 alineatul (3).

2. Planul Uniunii de cooperare în domeniul NIS prevede:

   (a) în scopul aplicării articolului 10:

      – definirea formatului și a procedurilor pentru colectarea și schimbul de informații compatibile și comparabile cu privire la riscuri și incidente de către autoritățile competente,

      – definirea procedurilor și a criteriilor de evaluare a riscurilor și a incidentelor de către rețeaua de cooperare.

   (b) procedurile care trebuie urmate pentru a da răspunsul coordonat prevăzut la articolul 11, inclusiv identificarea rolurilor și a responsabilităților și procedurile de cooperare;

   (c) o foaie de parcurs pentru exercițiile și formarea în domeniul NIS, destinate consolidării, validării și testării planului.

   (d) un program de transfer de cunoștințe între statele membre pentru crearea capacităților și învățarea inter pares;

   (e) un program de sensibilizare și de formare între statele membre.

3. Planul Uniunii de cooperare în domeniul NIS se adoptă în termen de cel mult un an de la intrarea în vigoare a prezentei directive și se revizuiește cu regularitate.

Articolul 13

Cooperarea internațională

Fără a aduce atingere posibilității de care dispune rețeaua de cooperare de a desfășura o cooperare internațională informală, Uniunea poate încheia acorduri internaționale cu țări terțe sau cu organizații internaționale, care permit și organizează participarea acestora la unele activități ale rețelei de cooperare. Astfel de acorduri trebuie să țină seama de necesitatea de a asigura o protecție adecvată a datelor cu caracter personal diseminate în rețeaua de cooperare.

CAPITOLUL IV

SECURITATEA REȚELELOR ȘI A SISTEMELOR INFORMATICE ALE ADMINISTRAȚIILOR PUBLICE ȘI ALE OPERATORILOR DE PIAȚĂ

Articolul 14

Cerințe de securitate și notificarea incidentelor

1. Statele membre se asigură că administrațiile publice și operatorii de piață iau măsurile tehnice și organizatorice adecvate pentru a gestiona riscurile de securitate a rețelelor și a sistemelor informatice aflate sub controlul lor și pe care le utilizează în activitățile lor. Ținând seama de cea mai avansată tehnologie, aceste măsuri trebuie să garanteze un nivel de securitate adecvat riscului existent. Trebuie luate, în special, măsuri pentru a preveni și a reduce la minimum impactul incidentelor care afectează rețeaua sau sistemul informatic utilizat pentru furnizarea serviciilor esențiale, asigurând astfel continuitatea serviciilor care se bazează pe rețeaua sau sistemul informatic respectiv.

2. Statele membre se asigură că administrațiile publice și operatorii de piață notifică autorității competente incidentele care au un impact semnificativ asupra securității serviciilor esențiale pe care le furnizează.

3. Cerințele prevăzute la alineatele (1) și (2) se aplică tuturor operatorilor de piață care furnizează servicii în Uniunea Europeană.

4. Autoritatea competentă poate informa publicul ea însăși sau poate solicita acest lucru administrațiilor publice și operatorilor de piață, în cazul în care consideră că divulgarea incidentului servește interesului public. O dată pe an autoritatea competentă transmite rețelei de cooperare un raport de sinteză privind notificările primite și măsurile luate în conformitate cu prezentul alineat.

5. Comisia este împuternicită să adopte, în conformitate cu articolul 18, acte delegate privind definirea circumstanțelor în care administrațiile publice și operatorii de piață au obligația de a notifica incidentele.

6. Cu respectarea actelor delegate adoptate în temeiul alineatului (5), autoritățile competente pot emite orientări și, dacă este necesar, instrucțiuni privind circumstanțele în care administrațiile publice și operatorii de piață au obligația de a notifica incidentele.

7. Comisia este împuternicită să stabilească, prin acte de punere în aplicare, formatele și procedurile aplicabile în scopul alineatului (2). Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 19 alineatul (3).

8. Alineatele (1) și (2) nu se aplică microîntreprinderilor definite în Recomandarea 2003/361/CE Comisiei din 6 mai 2003 privind definirea microîntreprinderilor și a întreprinderilor mici și mijlocii[12].

Articolul 15

Punere în aplicare și executare

1. Statele membre se asigură că autoritățile competente sunt împuternicite să investigheze cazurile în care administrațiile publice sau operatorii de piață nu se conformează obligațiilor care le revin în temeiul articolului 14, precum și efectele acestei neconformări asupra securității rețelelor și a sistemelor informatice.

[12] JO L 124, 20.5.2003, p. 36.

2. Statele membre se asigură că autoritățile competente sunt împuternicite să solicite operatorilor de piață și administrațiilor publice:

   (a) să furnizeze informațiile necesare pentru evaluarea securității rețelelor și a sistemelor lor informatice, inclusiv documente privind politicile de securitate;

   (b) să se supună unui audit de securitate efectuat de un organism calificat independent sau de o autoritate națională și să le pună la dispoziție rezultatele acestuia.

3. Statele membre se asigură că autoritățile competente sunt împuternicite să emită instrucțiuni obligatorii pentru operatorii de piață și pentru administrațiile publice.

4. Autoritățile competente notifică autorităților de aplicare a legii incidentele cu presupus caracter penal grav.

5. Autoritățile competente lucrează în strânsă cooperare cu autoritățile de protecție a datelor cu caracter personal în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal.

6. Statele membre se asigură că orice obligații impuse administrațiilor publice și operatorilor de piață în temeiul prezentului capitol pot fi supuse unui control jurisdicțional.

Articolul 16

Standardizare

1. Pentru a asigura aplicarea convergentă a articolului 14 alineatul (1), statele membre încurajează utilizarea standardelor și/sau a specificațiilor relevante pentru securitatea rețelelor și a informației.

2. Comisia stabilește, prin acte de punere în aplicare, o listă a standardelor menționate la alineatul (1). Lista se publică în Jurnalul Oficial al Uniunii Europene.

CAPITOLUL V

DISPOZIȚII FINALE

Articolul 17

Sancțiuni

1. Statele membre stabilesc normele privind sancțiunile aplicabile în cazul încălcării dispozițiilor naționale adoptate în temeiul prezentei directive și iau toate măsurile necesare pentru a asigura punerea în aplicare a acestora. Sancțiunile prevăzute trebuie să fie eficace, proporționale și disuasive. Statele membre notifică dispozițiile respective Comisiei cel târziu până la data transpunerii prezentei directive și informează Comisia fără întârziere cu privire la orice modificări ulterioare ale acestora.

2. Statele membre se asigură că, atunci când un incident de securitate afectează date cu caracter personal, sancțiunile prevăzute sunt coerente cu sancțiunile stabilite de Regulamentul Parlamentului European și al Consiliului privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date[13].

[13] SEC(2012) 72 final.

Articolul 18

Exercitarea delegării de competențe

1. Competența de a adopta acte delegate este conferită Comisiei în condițiile stabilite de prezentul articol.

2. Se conferă Comisiei competența de a adopta actele delegate menționate la articolul 9 alineatul (2), la articolul 10 alineatul (5) și la articolul 14 alineatul (5). Comisia întocmește un raport privind delegarea de competențe cu cel puțin nouă luni înainte de sfârșitul perioadei de cinci ani. Delegarea de competențe se prelungește tacit cu perioade de durată identică, cu excepția cazului în care Parlamentul European sau Consiliul se opun unei astfel de prelungiri cu cel puțin trei luni înainte de încheierea fiecărei perioade.

3. Delegarea de competențe menționată la articolul 9 alineatul (2), la articolul 10 alineatul (5) și la articolul 14 alineatul (5) poate fi revocată în orice moment de Parlamentul European sau de Consiliu. Prin decizia de revocare ia sfârșit delegarea competențelor specificată în decizia respectivă. Decizia intră în vigoare în ziua următoare publicării sale în *Jurnalul Oficial al Uniunii Europene* sau la o dată ulterioară, pe care o specifică. Decizia nu afectează validitatea actelor delegate care sunt deja în vigoare.

4. După ce adoptă un act delegat, Comisia îl notifică simultan Parlamentului European și Consiliului.

5. Un act delegat adoptat în temeiul articolului 9 alineatul (2), al articolului 10 alineatul (5) și al articolului 14 alineatul (5) intră în vigoare numai dacă nici Parlamentul European și nici Consiliul nu formulează obiecții în termen de două luni de la data la care li s-a notificat actul respectiv sau dacă, înainte de expirarea acestui termen, atât Parlamentul European, cât și Consiliul informează Comisia că nu vor prezenta obiecții. Termenul respectiv se prelungește cu două luni la inițiativa Parlamentului European sau a Consiliului.

Articolul 19

Procedura comitetului

1. Comisia este asistată de un comitet (Comitetul pentru securitatea rețelelor și a informației). Acesta este un comitet în sensul Regulamentului (UE) nr. 182/2011.

2. Atunci când se face trimitere la prezentul alineat, se aplică articolul 4 din Regulamentul (UE) nr. 182/2011.

3. Atunci când se face trimitere la prezentul alineat, se aplică articolul 5 din Regulamentul (UE) nr. 182/2011.

Articolul 20

Revizuire

Comisia revizuiește periodic funcționarea prezentei directive și prezintă un raport Parlamentului European și Consiliului. Primul raport se transmite în termen de cel mult trei ani de la data transpunerii menționată la articolul 21. În acest scop, Comisia poate solicita statelor membre să furnizeze informații, fără întârzieri nejustificate.

Articolul 21

Transpunere

1. Statele membre adoptă și publică, până cel târziu la [un an și jumătate după data adoptării], actele cu putere de lege și actele administrative necesare pentru a se conforma prezentei directive. Statele membre comunică fără întârziere Comisiei textul acestor acte.

   Statele membre aplică actele în cauză începând cu [un an și jumătate după data adoptării].

   Atunci când statele membre adoptă actele respective, acestea conțin o trimitere la prezenta directivă sau sunt însoțite de o astfel de trimitere la data publicării lor oficiale. Statele membre stabilesc modalitatea de efectuare a acestei trimiteri.

2. Statele membre comunică Comisiei textul principalelor dispoziții de drept intern pe care le adoptă în domeniul reglementat de prezenta directivă.

Articolul 22

Intrare în vigoare

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

Articolul 23

Destinatari

Prezenta directivă se adresează statelor membre.

Adoptată la Bruxelles,

Pentru Parlamentul European,	*Pentru Consiliu*
Președintele	*Președintele*

ANEXA I

Obligații și sarcini ale Echipei de intervenție în caz urgență informatică (CERT)

Obligațiile și sarcinile CERT sunt definite în mod adecvat și clar pe baza unei politici naționale și/sau a unei reglementări naționale. Acestea includ următoarele elemente:

(1) Obligații ale CERT

(a) CERT asigură o disponibilitate înaltă a serviciilor sale de comunicații, evitând punctele unice de defecțiune și dispunând de mai multe mijloace pentru a fi contactată și pentru a contacta alte entități. În plus, canalele de comunicare trebuie să fie clar specificate și bine cunoscute bazei sale de utilizatori și partenerilor de cooperare.

(b) CERT pune în aplicare și gestionează măsuri de securitate pentru a asigura confidențialitatea, integritatea, disponibilitatea și autenticitatea informațiilor pe care le primește și le tratează.

(c) Birourile CERT și sistemele informatice de suport sunt situate pe amplasamente securizate.

(d) Se înființează un sistem de gestionare a calității pentru monitorizarea performanței CERT și asigurarea unui proces permanent de îmbunătățire. Acesta se bazează pe sisteme de măsurare clar definite care includ niveluri formale de serviciu și indicatori principali de performanță.

(e) Continuitatea activităților:

- CERT trebuie să dispună de un sistem adecvat de gestionare și rutare a cererilor, cu scopul de a facilita transferurile,
- CERT trebuie să dispună de efective de personal adecvate, pentru a asigura o disponibilitate permanentă,
- CERT se bazează pe o infrastructură a cărei continuitate este asigurată. În acest scop, se instalează sisteme redundante și un spațiu de lucru de rezervă pentru CERT, care să asigure un acces permanent la mijloace de comunicare.

(2) Sarcinile CERT

(a) Sarcinile CERT includ cel puțin următoarele:

- monitorizarea incidentelor la nivel național,
- transmiterea alertelor rapide, a alertelor și a anunțurilor și diseminarea informațiilor privind riscurile și incidentele către părțile interesate relevante,
- răspunsul la incidente,
- furnizarea analizei dinamice de risc și de incident și sensibilizarea situațională,
- sensibilizarea publicului larg cu privire la riscurile asociate activităților online,
- organizarea de campanii privind NIS;

(b) CERT stabilește relații de cooperare cu sectorul privat.

(c) Pentru a facilita cooperarea, CERT promovează adoptarea și utilizarea unor practici comune sau standardizate pentru:

- procedurile de administrare a incidentelor și a riscurilor,

– sistemele de clasificare a incidentelor, riscurilor și informațiilor,

– taxonomia sistemelor de măsurare,

– formatele de schimb de informații cu privire la riscuri și incidente și convențiile de denumire a sistemelor.

ANEXA II

Lista operatorilor de piață

menționați la articolul 3 alineatul (8) litera (a):

1. platforme de comerț electronic

2. procesatori de plăți online

3. rețele de socializare

4. motoare de căutare

5. servicii de cloud computing

6. magazine de aplicații online

menționați la articolul 3 alineatul (8) litera (b):

1. Energie

- furnizori de energie electrică și gaz
- operatori de sisteme de distribuție a energiei electrice și/sau a gazelor și comercianți cu amănuntul către consumatorii finali
- operatori de sisteme de transport al gazelor naturale, operatori de depozite și operatori de GNL
- operatori de sisteme de transport al energiei electrice
- conducte de transport al petrolului și depozite de petrol
- operatori de pe piața energiei electrice și a gazelor naturale
- operatori ai instalațiilor de producție a petrolului și gazelor naturale și ai instalațiilor de rafinare și de tratare

2. Transporturi

- transportatori aerieni (transport aerian de marfă și de pasageri)
- transportatori maritimi (societăți de transport maritim și costier de pasageri și societăți de transport maritim și costier de mărfuri)
- căi ferate (gestionari de infrastructură, întreprinderi integrate și operatori de transport feroviar)
- aeroporturi
- porturi
- operatori de control al gestionării traficului
- servicii logistice auxiliare: (a) depozitare și stocare, (b) manipularea mărfurilor și c) alte servicii auxiliare de transport

3. Bănci: instituții de credit conform articolului 4 alineatul (1) din Directiva 2006/48/CE.

4. Infrastructuri ale pieței financiare: burse de valori și contrapartide centrale/case de compensare

5. Sectorul sănătății: instituții de asistență medicală (inclusiv spitale și clinici private) și alte entități implicate în furnizarea de asistență medicală

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB

1.3. Tipul propunerii/inițiativei

1.4. Obiective

1.5. Motivul (motivele) propunerii/inițiativei

1.6. Durata acțiunii și impactul financiar al acesteia

1.7. Modul (modurile) de gestionare avute în vedere

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și raportare

2.2. Sistemul de gestionare și control

2.3. Măsuri de prevenire a fraudelor și a neregulilor

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

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

3.2. Impactul estimat asupra cheltuielilor

3.2.1. Sinteza impactului estimat asupra cheltuielilor

3.2.2. Impactul estimat asupra creditelor operaționale

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

3.2.5. Participarea terților la finanțare

3.3. Impactul estimat asupra veniturilor

FIȘĂ FINANCIARĂ LEGISLATIVĂ

1. CADRUL PROPUNERII/INIȚIATIVEI

1.1. Titlul propunerii/inițiativei

Propunere de Directivă a Parlamentului European și a Consiliului privind măsuri de asigurare a unui nivel ridicat de securitate a rețelelor și a informației în Uniune.

1.2. Domeniul (domeniile) de politică în cauză în structura ABM/ABB[37]

- 09 – Rețele de comunicații, conținut și tehnologie

1.3. Tipul propunerii/inițiativei

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

☐ Propunerea/inițiativa se referă la o **acțiune nouă ca urmare a unui proiect-pilot/unei acțiuni pregătitoare**[38]

☐ Propunerea/inițiativa se referă la **prelungirea unei acțiuni existente**

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

1.4. Obiective

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

Scopul directivei propuse este de a asigura un nivel comun ridicat de securitate a rețelelor și a informației (NIS) în UE.

1.4.2. Obiectiv(e) specific(e) și activitatea (activitățile) ABM/ABB în cauză

Propunerea stabilește măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice în Uniune.

Obiectivele specifice sunt următoarele:

1. Instituirea unui nivel minim de NIS în statele membre și creșterea, în consecință, a nivelului general de pregătire și răspuns.

2. Îmbunătățirea cooperării în domeniul NIS la nivelul UE în vederea combaterii cu eficacitate a incidentelor și a amenințărilor transfrontaliere. Va fi instituită o infrastructură securizată de schimb de informații, care va permite schimbul de informații sensibile și confidențiale între autoritățile competente.

3. Crearea unei culturi de gestionare a riscurilor și intensificarea schimbului de informații între sectoarele privat și public.

Activitățile ABM/ABB în cauză

Directiva privește entități (întreprinderi și organizații, inclusiv unele IMM-uri) dintr-o serie de sectoare (energie, transporturi, instituții de credit și burse, asistență medicală și furnizori de servicii esențiale de internet), precum și administrațiile publice. Directiva abordează legăturile cu autoritățile de aplicare a legii și cu autoritățile de protecție a datelor, precum și aspectele legate de NIS ale relațiilor externe.

- 09 – Rețele de comunicații, conținut și tehnologie

- 02 - Întreprinderi

[37] ABM (Activity Based Management): Gestionarea pe activități – ABB (Activity Based Budgeting): Stabilirea bugetului pe activități.

[38] Astfel cum sunt menționate la articolul 49 alineatul (6) litera (a) sau (b) din Regulamentul financiar.

- 32 - Energie
- 06 - Mobilitate și transporturi
- 17 - Sănătate și protecția consumatorilor
- 18 - Afaceri interne
- 19 – Relații externe
- 33 - Justiție
- 12- Piața internă

1.4.3. Rezultatul (rezultatele) și impactul preconizate

A se preciza efectele pe care propunerea/inițiativa ar trebui să le aibă asupra beneficiarilor vizați/grupurilor vizate.

Protecția consumatorilor, a întreprinderilor și a guvernelor din UE împotriva incidentelor, a amenințărilor și a riscurilor de NIS s-ar îmbunătăți în mod considerabil.

Mai multe detalii sunt disponibile la punctul 8.2 (Impactul opțiunii 2 – Abordarea reglementării) din documentul de lucru al serviciilor Comisiei, și anume Evaluarea impactului care însoțește prezenta propunere legislativă.

1.4.4. Indicatori de rezultat și de impact

A se preciza indicatorii care permit monitorizarea punerii în aplicare a propunerii/inițiativei.

Indicatorii de monitorizare și evaluare se găsesc în secțiunea 10 din Evaluarea impactului.

1.5. Motivul (motivele) propunerii/inițiativei

1.5.1. Cerințe de îndeplinit pe termen scurt sau lung

Fiecărui stat membru i se solicită să dispună de:

- o strategie națională privind NIS;
- un plan național de cooperare în domeniul NIS;
- o autoritate națională competentă în materie de NIS; și
- o echipă de intervenție în caz de urgență informatică (CERT)

La nivelul UE, statelor membre li se solicită să coopereze prin intermediul unei rețele.

Administrațiilor publice și actorilor principali din sectorul privat li se solicită să aplice gestionarea riscurilor de NIS și să raporteze autorităților competente incidentele de NIS care au un impact semnificativ.

1.5.2. Valoarea adăugată a implicării UE

Având în vedere caracterul transfrontalier al NIS, divergențele legislațiilor și ale politicilor în domeniu reprezintă o barieră în calea întreprinderilor care doresc să opereze în mai multe țări și în calea realizării economiilor de scară. Lipsa intervenției la nivelul UE ar conduce la situația în care fiecare stat membru ar acționa în mod individual, fără a lua în considerare interdependența rețelelor și a sistemelor informatice.

Prin urmare, obiectivele declarate pot fi mai bine realizate prin acțiuni la nivelul UE, decât prin acțiuni individuale ale statelor membre.

1.5.3. Învățăminte desprinse din experiențele anterioare similare

Propunerea decurge din constatarea că sunt necesare obligații de reglementare pentru a crea condiții uniforme și a elimina unele lacune legislative. În acest domeniu, abordarea

pur voluntară a condus la desfășurarea cooperării numai între un număr mic de state membre cu un nivel ridicat al capacităților.

1.5.4. Coerența și posibila sinergie cu alte instrumente relevante

Propunerea este pe deplin coerentă cu Agenda digitală pentru Europa și, prin urmare, cu Strategia Europa 2020. Propunerea este, de asemenea, coerentă cu cadrul de reglementare al UE în domeniul comunicațiilor electronice, cu Directiva UE privind infrastructurile critice europene și cu Directiva UE privind protecția datelor și completează aceste acte.

Propunerea însoțește Comunicarea Comisiei și a Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate privind Strategia europeană de securitate cibernetică și este o parte esențială a acestei comunicări.

1.6. Durata acțiunii și impactul financiar al acesteia

– ☐ Propunere/inițiativă **pe durată determinată**

– ☐ Propunere/inițiativă în vigoare de la [ZZ/LL]AAAA până la [ZZ/LL]AAAA

– ☐ Impact financiar din AAAA până în AAAA

– ☒ Propunere/inițiativă **pe durată nedeterminată**

– Perioada de transpunere va începe imediat după adoptare (conform estimărilor, în 2015) și va dura 18 luni. Punerea în aplicare a directivei va începe însă după adoptarea sa și va implica instituirea infrastructurii securizate care va susține cooperarea dintre statele membre.

– Va fi urmată de perioada de funcționare în regim de croazieră.

1.7. Modul (modurile) de gestionare preconizate[39]

– ☒ Gestionare centralizată directă de către Comisie

– ☒ Gestionare centralizată indirectă, cu delegarea sarcinilor de execuție:

– ☐agențiilor executive

– ☒ organismelor instituite de Comunități[40]

– ☐ organismelor publice naționale/organismelor cu misiune de serviciu public

– ☐ persoanelor 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 împreună cu țări terțe

– ☐ Gestionare în comun cu organizații internaționale, inclusiv cu Agenția Spațială Europeană

Dacă se indică mai multe moduri de gestionare, se furnizează detalii suplimentare în secțiunea „Observații".

Observații
ENISA, o agenție descentralizată creată de Comunități, poate asista statele membre și Comisia în punerea în aplicare a directivei, pe baza mandatului său și a redistribuirii resurselor prevăzută în cadrul financiar multianual 2014-2020 pentru această agenție.

[39] Explicațiile privind modurile de gestionare, precum și trimiterile la Regulamentul financiar sunt disponibile pe site-ul BudgWeb: http://www.cc.cec/budg/man/budgmanag/budgmanag_en.htmlhttp://www.cc.cec/budg/man/budgmanag/budgmanag_en.html

[40] Astfel cum sunt menționate la articolul 185 din Regulamentul financiar.

2. MĂSURI DE GESTIONARE

2.1. Dispoziții în materie de monitorizare și raportare

A se preciza frecvența și condițiile aferente acestor dispoziții.

Comisia va revizui periodic funcționarea directivei și va prezenta un raport Parlamentului European și Consiliului.

De asemenea, Comisia va evalua transpunerea corectă a directivei de către statele membre.

Propunerea privind MCE prevede și posibilitatea de a efectua o evaluare a metodelor de executare a proiectelor, precum și a impactului punerii în aplicare a acestora, pentru a aprecia dacă obiectivele, inclusiv cele legate de protecția mediului, au fost atinse.

2.2. Sistemul de gestionare și control

2.2.1. Riscul identificat

- întârzieri în executarea proiectelor în ceea ce privește crearea infrastructurii securizate

2.2.2. Metodele de control preconizate

Acordurile și deciziile de punere în aplicare a acțiunilor din cadrul MCE vor prevedea supravegherea și controlul financiar de către Comisie, sau de către orice reprezentant autorizat de Comisie, precum și efectuarea unor audituri de către Curtea de Conturi și a unor controale la fața locului de către Oficiul European de Luptă Antifraudă (OLAF).

2.2.3. Costurile și beneficiile controalelor și rata probabilă de neconformitate

Controalele *ex ante* și *ex post* bazate pe riscuri, precum și posibilitatea de a efectua audituri la fața locului vor permite menținerea costurile controalelor la un nivel rezonabil.

2.3. Măsuri de prevenire a fraudelor și neregulilor

A se preciza măsurile de prevenire și de protecție existente sau preconizate.

La punerea în aplicare a acțiunilor finanțate în temeiul prezentei directive, Comisia va lua măsurile adecvate pentru a asigura protejarea intereselor financiare ale Uniunii prin aplicarea măsurilor preventive împotriva fraudei, a corupției și a oricăror alte activități ilegale, prin controale eficace și, dacă se constată nereguli, prin recuperarea sumelor plătite în mod necuvenit și, după caz, prin sancțiuni eficace, proporționale și disuasive.

Comisia sau reprezentanții acesteia și Curtea de Conturi au competența de a efectua audituri, atât pe baza documentelor, cât și la fața locului, în ceea ce îi privește pe toți beneficiarii de granturi, contractorii și subcontractorii care au primit fonduri din partea Uniunii în temeiul programului.

Oficiul European de Luptă Antifraudă (OLAF) poate efectua controale și inspecții la fața locului la operatorii economici care beneficiază direct sau indirect de o astfel de finanțare, în conformitate cu procedurile prevăzute în Regulamentul (Euratom, CE) nr. 2185/96, cu scopul de a stabili dacă a avut loc o fraudă, un act de corupție sau orice altă activitate ilegală care afectează interesele financiare ale Uniunii și este

legată de un acord de grant sau de o decizie de acordare a unui grant sau de un contract de finanțare din partea Uniunii.

Fără a aduce atingere celor de mai sus, acordurile de cooperare cu țări terțe și cu organizații internaționale, precum și acordurile de grant, deciziile de acordare a unui grant și contractele rezultate din punerea în aplicare a prezentei directive împuternicesc în mod expres Comisia, Curtea de Conturi și OLAF să efectueze astfel de audituri, controale și inspecții la fața locului.

MCE prevede modele standard pentru contracte, granturi și achiziții, care vor stabili măsurile antifraudă general aplicabile.

3. IMPACTUL FINANCIAR ESTIMAT AL PROPUNERII/INIȚIATIVEI

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

- Linii bugetare existente

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul cheltuielilor	Contribuție			
	Numărul [Descriere … … … … … … … … … … … …]	Dif./Nedif. (41)	Țări AELS[42]	Țări candidate[43]	Țări terțe	În sensul articolului 18 alineatul (1) litera (aa) din Regulamentul financiar
	09 03 02 Promovarea interconectării și a interoperabilității serviciilor publice naționale online, precum și a accesului la astfel de rețele	Dif.	NU	NU	NU	NU

- Noile linii bugetare a căror creare se solicită (Nu se aplică)

În ordinea rubricilor din cadrul financiar multianual și a liniilor bugetare.

Rubrica din cadrul financiar multianual	Linia bugetară	Tipul cheltuielilor	Contribuție			
	Număr [Rubrică……...]	Dif./Nedif.	Țări AELS	Țări candidate	Țări terțe	În sensul articolului 18 alineatul (1) litera (aa) din Regulamentul financiar
	[XX.YY.YY.YY]		DA/NU	DA/NU	DA/NU	DA/NU

41 Dif. = credite diferențiate / Nedif. = credite nediferențiate.

42 AELS: Asociația Europeană a Liberului Schimb

43 Țările candidate și, după caz, țările 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	Creştere inteligentă şi favorabilă incluziunii

DG: <…….>			2015* [44]	Anul **2016**	Anul **2017**	Anul **2018**	Anii următori (2019-2021) şi în continuare			**TOTAL**
• Credite operaţionale										
09 03 02	Angajamente	(1)	1,250**	0,000						**1,250**
	Plăţi	(2)	0,750	0,250	0,250					**1,250**
Credite cu caracter administrativ finanţate din bugetul anumitor programe[45]			**0,000**							**0,000**
Numărul liniei bugetare		(3)	**0,000**							**0,000**
TOTAL credite pentru DG <…….>	Angajamente	=1+1a +3	1,250	0,000						**1,250**
	Plăţi	=2+2a +3	0,750	0,250	0,250					**1,250**

• TOTAL credite operaţionale	Angajamente	(4)	1,250	0,000						**1,250**
	Plăţi	(5)	0,750	0,250	0,250					**1,250**
• TOTAL credite cu caracter administrativ finanţate din		(6)	**0,000**							

[44] Anul N este anul în care începe punerea în aplicare a propunerii/iniţiativei.

[45] Asistenţă tehnică şi/sau administrativă şi cheltuieli de sprijin pentru punerea în aplicare a programelor şi/sau a acţiunilor UE (fostele linii „BA”), cercetare indirectă şi cercetare directă.

bugetul anumitor programe										
TOTAL credite în cadrul RUBRICII 1 din cadrul financiar multianual	Angajamente	=4+ 6	1,250	0,000						**1,250**
	Plăți	=5+ 6	0,750	0,250	0,250					**1,250**

* Calendarul exact va depinde de data adoptării propunerii de către autoritatea legislativă (și anume, dacă directiva va fi aprobată în cursul anului 2014, adaptarea infrastructurii existente ar începe în 2015, în caz contrar, un an mai târziu).

** Dacă statele membre decid să utilizeze o infrastructură existentă și să acopere costul unic de adaptare a acesteia din bugetul UE, astfel cum s-a explicat la punctele 1.4.3 și 1.7, costul de adaptare a unei rețele pentru susținerea cooperării dintre statele membre, conform capitolului III din directivă (alertă rapidă, răspuns coordonat etc.), este estimat la 1 250 000 EUR. Această sumă este puțin mai mare decât cea menționată în Evaluarea impactului („aproximativ 1 milion EUR”), deoarece se bazează pe o estimare mai precisă a modulelor necesare pentru o astfel de infrastructură. Modulele necesare și costurile aferente se bazează pe o estimare efectuată de JRC, în urma experienței sale de dezvoltare a unor sisteme similare în alte domenii, precum sănătatea publică, și includ următoarele: un sistem de alertă rapidă și notificare a incidentelor de NIS (275 000 EUR); o platformă de schimb de informații (400 000 EUR); un sistem de alertă rapidă și răspuns (275 000 EUR) și un centru de criză (300 000 EUR) totalizând 1 250 000 EUR. Se prevede întocmirea unui plan mai detaliat de punere în aplicare în cadrul viitorului studiu de fezabilitate prevăzut de contractul specific SMART 2012/0010: „Studiu de fezabilitate și activități pregătitoare pentru punerea în aplicare a unui Sistem european de alertă rapidă și răspuns în caz de atac informatic și perturbări”.

În cazul în care propunerea/inițiativa afectează mai multe rubrici:

• TOTAL credite operaționale	Angajamente	(4)	0,000	0,000						
	Plăți	(5)	0,000	0,000						
• TOTAL credite cu caracter administrativ finanțate din bugetul anumitor programe		(6)	**0,000**	**0,000**						
TOTAL credite în cadrul RUBRICILOR 1 – 4 din cadrul financiar multianual (suma de referință)	Angajamente	=4+ 6	1,250	0,000						1,250
	Plăți	=5+ 6	0,750	0,250	0,250					1,250

Rubrica din cadrul financiar multianual	**5**	„Cheltuieli administrative”

milioane EUR (cu 3 zecimale)

		Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anii următori (2019-2021) și în continuare			**TOTAL**
DG:CNECT									
• Resurse umane		0,572	0,572	0,572	0,572	0,572	0,572	**0,572**	**4,004**
• Alte cheltuieli administrative		0,318	0,118	0,318	0,118	0,318	0,118	**0,118**	**1,426**
TOTAL DG CNECT	Credite	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

TOTAL credite în cadrul RUBRICII 5 din cadrul financiar multianual	(Total angajamente = Total plăți)	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

milioane EUR (cu 3 zecimale)

		Anul **2015**[46]	Anul **2016**	Anul **2017**	Anul **2018**	Anii următori (2019-2021) și în continuare			**TOTAL**
TOTAL credite în cadrul RUBRICILOR 1 – 5 din cadrul financiar multianual	Angajamente	2,140	0,690	0,890	0,690	0,890	0,690	0,690	**6,680**
	Plăți	1,640	0,940	1,140	0,690	0,890	0,690	0,690	**6,680**

[46] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

3.2.2. Impactul estimat asupra creditelor operaționale

– ☐ Propunerea/inițiativa nu implică utilizarea de credite operaționale

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

– Credite de angajament în milioane EUR (cu 3 zecimale)

A se indica obiectivele și realizările ⇩			Anul **2015***		Anul **2016**		Anul **2017**		Anul **2018**		Anii următori (2019-2021) și în continuare						**TOTAL**	
	REALIZĂRI																	
	Tipul [47]	Costul mediu	Numărul	Costul	Numărul	Costul	Numărul	Costul	Numărul	Costul	Numărul	Costul	Numărul	Costul	Numărul	Costul	Numărul total	Costul total
OBIECTIVUL SPECIFIC NR. 2[48] Infrastructură securizată de schimb de informații																		
- Realizare	Adaptarea infrastructurii																	
Subtotal obiectivul specific nr. 2			1	1,250**													1	1,250
COSTURI TOTALE				1,250														1,250

[47] Realizările se referă la produsele și serviciile care vor fi furnizate (de ex.: numărul de schimburi de studenți finanțate, numărul de km de drumuri construiți etc.).

[48] Conform descrierii de la punctul 1.4.2. „Obiectiv(e) specific(e)…”

* Calendarul exact va depinde de data adoptării propunerii de către autoritatea legislativă (și anume, dacă directiva va fi aprobată în cursul anului 2014, adaptarea infrastructurii existente ar începe în 2015, în caz contrar, un an mai târziu).

**A se vedea punctul 3.2.1.

3.2.3. Impactul estimat asupra creditelor cu caracter administrativ

3.2.3.1. Sinteză

– ☐ Propunerea/inițiativa nu implică utilizarea de credite administrative

– ☑ Propunerea/inițiativa implică utilizarea de credite administrative, conform explicațiilor de mai jos:

milioane EUR (cu 3 zecimale)

	Anul **2015**[49]	Anul **2016**	Anul **2017**	Anul **2018**	Anii următori (2019-2021) și în continuare			**TOTAL**
RUBRICA 5 din cadrul financiar multianual								
Resurse umane	0,572	0,572	0,572	0,572	0,572	0,572	0,572	**4,004**
Alte cheltuieli administrative	0,318	0,118	0,318	0,118	0,318	0,118	0,118	**1,426**
Subtotal RUBRICA 5 din cadrul financiar multianual	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
În afara RUBRICII 5[50] **din cadrul financiar multianual**								
Resurse umane	0,000	0,000						**0,000**
Alte cheltuieli cu caracter administrativ								
Subtotal în afara RUBRICII 5 din cadrul financiar multianual	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**
TOTAL	0,890	0,690	0,890	0,690	0,890	0,690	0,690	**5,430**

Necesarul de credite administrative va fi acoperit de creditele deja alocate DG CNECT pentru gestionarea acțiunii și/sau care au fost redistribuite în cadrul DG-ului, completate, dacă este necesar, cu resursele suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și ținând seama de constrângerile bugetare.

Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) ar putea asista statele membre și Comisia în punerea în aplicare a directivei, pe baza mandatului său și

[49] Anul N este anul în care începe punerea în aplicare a propunerii/inițiativei.

[50] Asistență tehnică și/sau administrativă și cheltuieli de sprijin pentru punerea în aplicare a programelor și/sau a acțiunilor UE (fostele linii „BA”), cercetare indirectă și cercetare directă.

prin redistribuirea resurselor prevăzută în cadrul financiar multianual 2014-2020 pentru această agenție, și anume, fără alocări suplimentare bugetare sau de resurse umane.

3.2.3.2. Necesarul de resurse umane estimat

– ☐ Propunerea/inițiativa nu implică utilizarea de resurse umane

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

În principiu, nu este nevoie de o forță de muncă suplimentară. Necesarul de resurse umane va fi foarte limitat și va fi acoperit de efectivele de personal ale DG-ului în cauză, care sunt deja alocate pentru gestionarea acțiunii.

Estimarea se exprimă în numere întregi (sau cel mult cu o zecimală)

		Anul **2015**	Anul **2016**	Anul **2017**	Anul **2018**	Anii următori (2019-2021) și în continuare		
• Posturi din schema de personal (posturi de funcționari și de agenți temporari)								
09 01 01 01 (la sediu și în birourile de reprezentare ale Comisiei)		4	4	4	4	4	4	4
XX 01 01 02 (în delegații)								
XX 01 05 01 (cercetare indirectă)								
10 01 05 01 (cercetare directă)								
• Personal extern (în echivalent normă întreagă: ENI)[51]								
09 01 02 01 (AC, INT, END din „pachetul global”)		1	1	1	1	1	1	1
XX 01 02 02 (AC, INT, JED, AL și END în delegații)								
XX 01 04 ***yy***[52]	- la sediu[53]							
	- în delegații							
XX 01 05 02 (AC, INT, END în cadrul cercetării indirecte)								
10 01 05 02 (AC, INT, END în cadrul cercetării directe)								
Alte linii bugetare (a se preciza)								
TOTAL		**5**	**5**	**5**	**5**	**5**	**5**	**5**

XX este domeniul de politică sau titlul din buget în cauză.

Necesarul de resurse umane va fi acoperit de efectivele de personal ale DG CNECT alocate deja pentru gestionarea acțiunii și/sau redistribuite intern în cadrul DG-ului, completate, dacă este necesar, cu resursele suplimentare ce ar putea fi alocate DG-ului care gestionează acțiunea în cadrul procedurii de alocare anuală și ținând seama de constrângerile bugetare.

Agenția Europeană pentru Securitatea Rețelelor Informatice și a Datelor (ENISA) ar putea asista statele membre și Comisia în punerea în aplicare a directivei, pe baza

51 AC = agent contractual; INT = personal pus la dispoziție de agenții de muncă temporară („Intérimaire”); JED = „Jeune Expert en Délégation” (expert tânăr în delegații); AL = agent local; END= expert național detașat.

52 Sub plafonul pentru personal extern din credite operaționale (fostele linii „BA”).

53 În principal pentru fonduri structurale, Fondul european agricol pentru dezvoltare rurală (FEADR) și Fondul european pentru pescuit (FEP).

mandatului său actual și prin redistribuirea resurselor prevăzută în cadrul financiar multianual 2014-2020 pentru această agenție, și anume, fără alocări suplimentare bugetare sau de resurse umane.

Descrierea sarcinilor care trebuie efectuate:

Funcționari și agenți temporari	- Pregătirea actelor delegate în conformitate cu articolul 14 alineatul (3) - Pregătirea actelor de punere în aplicare în conformitate cu articolul 8, articolul 9 alineatul (2), articolul 12, articolul 14 alineatul (5), articolul 16 - Contribuție la cooperarea prin intermediul rețelei atât la nivelul politicii, cât și la nivel operațional. - Participare la negocieri internaționale și, eventual, încheierea acordurilor internaționale
Personal extern	Sprijin pentru toate sarcinile de mai sus, în funcție de necesități.

3.2.4. Compatibilitatea cu cadrul financiar multianual actual

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

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

Impactul financiar estimat asupra cheltuielilor operaționale ale propunerii se va produce dacă statele membre decid să adapteze o infrastructură existentă și încredințează Comisiei efectuarea acestei adaptări în contextul cadrului financiar multianual 2014-2020. Costul unic aferent va fi acoperit în cadrul MCE, în condițiile disponibilității unor fonduri suficiente. În mod alternativ, statele membre pot să suporte împreună fie costurile adaptării infrastructurii, fie costurile de creare a unei noi infrastructuri.

– ☐ Propunerea/inițiativa necesită recurgerea la instrumentul de flexibilitate sau revizuirea cadrului financiar multianual[54].

Nu se aplică.

3.2.5. Participarea terților la finanțare

– Propunerea/inițiativa nu prevede cofinanțare din partea terților

3.3. Impactul estimat asupra veniturilor

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

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