Parlamentul European
2014-2019

Comisia pentru libertăți civile, justiție și afaceri interne

2017/0225(COD)

16.3.2018

AVIZ

al Comisiei pentru libertăți civile, justiție și afaceri interne

destinat Comisiei pentru industrie, cercetare și energie

referitor la propunerea de regulament al Parlamentului European și al Consiliului privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”)
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Raportor pentru aviz: Jan Philipp Albrecht

JUSTIFICARE SUCCINTĂ

Raportorul pentru aviz salută propunerea Comisiei referitoare la „o lege privind securitatea cibernetică”[1], deoarece aceasta definește mai bine rolul ENISA în ecosistemul schimbat al securității informatice și dezvoltă măsurile privind standardele de securitate informatică, certificarea și etichetarea, astfel încât sistemele bazate pe TIC, inclusiv obiecte conectate, să devină mai sigure.

Totuși, raportorul pentru aviz consideră că se pot efectua mai multe îmbunătățiri. Raportorul pentru aviz este ferm convins că securitatea informațiilor este esențială pentru protecția drepturilor fundamentale ale cetățenilor, consacrate în Carta drepturilor fundamentale a UE, precum și pentru combaterea criminalității informatice și protejarea democrației și a statului de drept.

Drepturile fundamentale: sistemele nesigure pot conduce la încălcarea securității datelor sau frauda de identitate, care ar putea provoca daune reale și suferință pentru persoanele fizice, inclusiv un risc la adresa vieții acestora, a vieții private, a demnității sau bunurilor acestora. De exemplu, martorii pot fi expuși riscului de intimidare și de vătămare fizică sau femeile pot fi expuse riscului violenței domestice, în cazul în care adresele acestora sunt făcute publice. Pentru internetul obiectelor fizice care conține, de asemenea, mecanisme de acționare fizică și nu doar senzori, integritatea fizică și viața persoanelor pot fi expuse riscului din cauza atacurilor la adresa sistemelor informatice; amendamentele propuse de raportor se concentrează, în special, asupra protecției oferite de articolele 1, 2, 3, 6, 7, 8, 11 și 17 din Carta drepturilor fundamentale a UE. Există chiar jurisprudență constituțională emergentă, care derivă un „drept fundamental la confidențialitatea și integritatea sistemelor informatice-tehnice”[2] din drepturile generale ale persoanei, adaptate la actuala lume digitală.

Combaterea criminalității informatice: anumite forme de infracțiuni comise online, cum ar fi atacurile de tip phishing sau fraudele financiare și bancare, constau din abuzul de încredere, care nu poate fi combătut prin măsuri de securitate informatică — împotriva acestor forme ale criminalității, raportorul pentru aviz salută propunerile de sensibilizare periodică și campaniile de educare a publicului, destinate utilizatorilor finali, organizate de ENISA. Alte forme de infracțiuni online implică atacuri împotriva sistemelor de informații, cum ar fi atacurile de piraterie sau blocarea distribuită a serviciului (DDoS) — împotriva acestor forme ale criminalității, raportorul consideră că întărirea securității informatice va consolida efectiv lupta împotriva criminalității cibernetice și, în special, prevenirea acesteia.

Democrația și statul de drept: atacurile împotriva sistemelor IT din partea guvernelor și actorilor nestatali reprezintă o amenințare evidentă și din ce în ce mai mare la adresa democrației, din cauza imixtiunii în alegerile libere și echitabile, de exemplu prin manipularea unor fapte și a unor opinii care influențează modul în care vor vota cetățenii, intervenind în procesul de votare și schimbând rezultatele votului sau subminând încrederea în integritatea procesului de votare.

---

[1] Comisia Europeană, Propunerea de regulament al Parlamentului European și al Consiliului privind ENISA, „Agenția UE pentru securitate cibernetică”, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate cibernetică pentru tehnologia informației și comunicațiilor („Legea privind securitatea cibernetică”) COM(2017) 477 final/2.

[2] Curtea Constituțională a Germaniei, Hotărârea din 27 februarie 2008, cauzele 1 BvR 370/07, 1 BvR 595/07.

Prin urmare, raportorul pentru aviz sugerează, în proiectul său de aviz LIBE, modificarea propunerii Comisiei Europene, concentrându-se pe următoarele aspecte-cheie LIBE:

- Agenția ar trebui să joace un rol mai important în promovarea adoptării unor tehnologii preventive solide de protecție a
  vieții private și a unor măsuri de securitate informatică de către toți actorii din societatea informațională europeană;

- Agenția ar trebui să propună politici care să stabilească în mod clar responsabilitățile și obligațiile juridice pentru toate părțile interesate care participă la ecosistemele TIC, în cazul în care abținerea de a acționa cu diligența necesară în materie de securitate informatică ar putea duce la efecte majore de securitate, distrugeri masive ale mediului, ar putea declanșa o criză financiară sau economică sistemică;

- Agenția ar trebui să propună cerințe de referință clare și obligatorii în materie de securitate informatică, în consultare cu experții în securitatea informatică;

- Agenția ar trebui să propună un sistem de certificare de securitate informatică, care să permită furnizorilor de TIC să mărească gradul de transparență pentru consumator cu privire la potențialul de actualizare și perioada de suport tehnic pentru software. Acest sistem de certificare ar trebui să fie dinamic, deoarece securitatea este un proces care necesită îmbunătățiri constante;

- Agenția ar trebui să facă mai ușoară și mai puțin costisitoare implementarea principiilor de securitate de la stadiul conceperii, prin emiterea de orientări și bune practici pentru fabricanții de produse TIC;

- Agenția ar trebui ca, la invitația instituțiilor, a organelor, a birourilor și a agențiilor Uniunii, precum și a statelor membre, să efectueze în mod periodic audituri preventive de securitate informatică a infrastructurilor de importanță critică (dreptul la audit);

- Agenția ar trebui să raporteze imediat vulnerabilitățile de securitate informatică care nu sunt încă cunoscute în mod public de producători. Agenția nu ar trebui să ascundă sau să exploateze vulnerabilitățile nedivulgate din întreprinderi și produse în scopuri proprii. Prin dezvoltarea, achiziționarea și exploatarea ușilor secrete din sistemele informatice, cu banii contribuabililor, organismele guvernamentale pun în pericol securitatea cetățenilor. Pentru a proteja alte părți interesate care interacționează în mod responsabil cu astfel de vulnerabilități, Agenția ar trebui să propună politici privind schimbul responsabil de informații cu privire la „zero zile” și alte tipuri de vulnerabilități în materie de securitate, care nu sunt încă cunoscute publicului, facilitând eliminarea vulnerabilităților;

- Pentru a permite Uniunii să ajungă la nivelul industriilor de securitate informatică din țările terțe, Agenția ar trebui să identifice și să inițieze lansarea unui proiect UE pe termen lung de securitate informatică, de o amploare comparabilă cu ceea ce s-a adoptat pentru industria aeronautică, prin Airbus;

Propunerea Comisiei ar trebui să evite utilizarea termenului de „securitate cibernetică”, deoarece este vag din punct de vedere juridic și ar putea da naștere la incertitudini. Raportorul

pentru aviz propune înlocuirea termenului „securitate cibernetică” cu cel de „securitate informatică” pentru a îmbunătăți securitatea juridică.

AMENDAMENTE

Comisia pentru libertăți civile, justiție și afaceri interne recomandă Comisiei pentru industrie, cercetare și energie, care este comisie competentă, să ia în considerare următoarele amendamente:

Amendamentul 1

Propunere de regulament
Titlu

Textul propus de Comisie	*Amendamentul*
REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI	REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI
privind ENISA, „Agenția UE pentru ***securitate cibernetică”***, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate ***cibernetică*** pentru tehnologia ***informației și comunicațiilor*** („Legea privind securitatea ***cibernetică”***)	privind ENISA, „Agenția UE pentru ***Securitatea Rețelelor și a Informațiilor”***, de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea de securitate pentru tehnologia ***informatică*** („Legea privind securitatea ***informatică”***)
	(Această modificare se aplică întregului text.)

Justificare

Prefixul „ciber”, derivat din operele științifico-fantastice din anii 1960 a fost din ce în ce mai utilizat pentru a descrie aspectele negative ale internetului (atac cibernetic, criminalitate cibernetică etc.), dar este foarte vag din punct de vedere juridic. Raportorul pentru aviz propune înlocuirea termenului de „securitate cibernetică” cu cel de „securitate informatică” din motive de securitate juridică.

Amendamentul 2

Propunere de regulament
Considerentul 2

Textul propus de Comisie	*Amendamentul*

(2) În prezent, rețelele și sistemele informatice sunt utilizate la scară generală de către cetățenii, întreprinderile și administrațiile din întreaga Uniune. Digitizarea și conectivitatea sunt pe cale să devină caracteristici principale ale unui număr tot mai mare de produse și servicii, preconizându-se că, odată cu apariția internetului obiectelor (IoT), în UE, în următorul deceniu, vor intra în folosință milioane, dacă nu chiar miliarde de dispozitive digitale conectate. Deși numărul dispozitivelor conectate la internet este în creștere, securitatea și reziliența nu sunt incluse suficient de la nivelul de proiect, ceea ce conduce la o securitate ***cibernetică*** insuficientă. În acest context, din cauză că certificarea nu este utilizată decât într-o măsură limitată, utilizatorii, indiferent dacă sunt persoane fizice sau organizații, nu dispun de suficiente informații cu privire la caracteristicile de securitate ***cibernetică*** ale produselor și serviciilor TIC, ceea ce erodează încrederea în soluțiile digitale.	(2) În prezent, rețelele și sistemele informatice sunt utilizate la scară generală de către cetățenii, întreprinderile și administrațiile din întreaga Uniune. Digitizarea și conectivitatea sunt pe cale să devină caracteristici principale ale unui număr tot mai mare de produse și servicii, preconizându-se că, odată cu apariția internetului obiectelor (IoT), în UE, în următorul deceniu, vor intra în folosință milioane, dacă nu chiar miliarde de dispozitive digitale conectate. Deși numărul dispozitivelor conectate la internet este în creștere, securitatea și reziliența nu sunt incluse suficient de la nivelul de proiect, ceea ce conduce la o securitate ***informatică*** insuficientă. În acest context, din cauză că certificarea nu este utilizată decât într-o măsură limitată ***și fragmentată***, utilizatorii, indiferent dacă sunt persoane fizice sau organizații, nu dispun de suficiente informații cu privire la caracteristicile de securitate ***informatică*** ale produselor și serviciilor TIC, ceea ce erodează încrederea în soluțiile digitale. ***Rețelele TIC constituie elementul central al produselor și serviciilor digitale, care au potențialul de a sprijini cetățenii în toate aspectele vieții lor și de a stimula creșterea economică a Europei. Pentru a se asigura că obiectivele pieței unice digitale sunt pe deplin realizate, trebuie să fie funcționale elementele esențiale ale tehnologiei pe care se bazează domenii importante precum eHealth, IoT, inteligența artificială, tehnologia cuantică, precum și sistemele inteligente de transport și de producție avansată.***

Amendamentul 3

Propunere de regulament
Considerentul 4

Textul propus de Comisie	*Amendamentul*
(4) În condițiile în care atacurile cibernetice sunt în creștere, o economie și	(4) În condițiile în care atacurile cibernetice sunt în creștere, o economie și

o societate conectată care sunt mai vulnerabile la amenințările și atacurile cibernetice necesită dispozitive de protecție mai puternice. Cu toate acestea, deși atacurile cibernetice sunt adesea transfrontaliere, răspunsurile oferite de politicile autorităților de securitate ***cibernetică*** și de aplicare a legii sunt predominant naționale. Incidentele de securitate cibernetică de mare amploare sunt de natură să perturbe furnizarea serviciilor esențiale pe întregul teritoriu al UE. Din acest motiv, trebuie să se asigure un răspuns și o gestionare eficace a crizelor la nivelul UE, care să se bazeze pe politicile specifice și pe instrumentele mai generale de solidaritate europeană și asistență reciprocă. În plus, pentru factorii de decizie politică, sector și utilizatori este important, prin urmare, să existe o evaluare periodică a situației în materie de securitate ***cibernetică*** și reziliență în Uniune, pornind de la date fiabile la nivelul Uniunii, precum și de la o prognoză sistematică a evoluțiilor, provocărilor și amenințărilor viitoare, atât la nivelul Uniunii, cât și la nivel mondial.	o societate conectată care sunt mai vulnerabile la amenințările și atacurile cibernetice necesită dispozitive de protecție mai puternice ***si mai sigure***. Cu toate acestea, deși atacurile cibernetice sunt adesea transfrontaliere, răspunsurile oferite de politicile autorităților de securitate ***informatică*** și de aplicare a legii sunt predominant naționale. Incidentele de securitate cibernetică de mare amploare sunt de natură să perturbe furnizarea serviciilor esențiale pe întregul teritoriu al UE. Din acest motiv, trebuie să se asigure un răspuns și o gestionare eficace a crizelor la nivelul UE, care să se bazeze pe politicile specifice și pe instrumentele mai generale de solidaritate europeană și asistență reciprocă. În plus, pentru factorii de decizie politică, sector și utilizatori este important, prin urmare, să existe o evaluare periodică a situației în materie de securitate ***informatică*** și reziliență în Uniune, pornind de la date fiabile la nivelul Uniunii, precum și de la o prognoză sistematică a evoluțiilor, provocărilor și amenințărilor viitoare, atât la nivelul Uniunii, cât și la nivel mondial.

Amendamentul 4

Propunere de regulament
Considerentul 5

Textul propus de Comisie	*Amendamentul*
(5) Având în vedere intensificarea provocărilor în materie de securitate ***cibernetică*** cu care se confruntă Uniunea, este necesar un set cuprinzător de măsuri care să se bazeze pe acțiunile anterioare ale Uniunii și să promoveze obiective care se consolidează reciproc. Printre acestea se numără necesitatea de a spori și mai mult capabilitățile și gradul de pregătire ale statelor membre și ale întreprinderilor, precum și de a îmbunătăți cooperarea și coordonarea între statele membre și instituțiile, agențiile și organele UE. Mai	(5) Având în vedere intensificarea provocărilor în materie de securitate ***informatică*** cu care se confruntă Uniunea, este necesar un set cuprinzător de măsuri care să se bazeze pe acțiunile anterioare ale Uniunii și să promoveze obiective care se consolidează reciproc. Printre acestea se numără necesitatea de a spori și mai mult capabilitățile și gradul de pregătire ale statelor membre și ale întreprinderilor, precum și de a îmbunătăți cooperarea și coordonarea între statele membre și instituțiile, agențiile și organele UE. Mai

mult decât atât, amenințările cibernetice nu se opresc la frontiere, motiv pentru care este necesară dezvoltarea capabilităților de la nivelul Uniunii care ar putea completa acțiunea statelor membre, în special în cazul incidentelor și crizelor de securitate cibernetică transfrontaliere de mare amploare. De asemenea, sunt necesare eforturi suplimentare pentru a spori gradul de sensibilizare a cetățenilor și întreprinderilor cu privire la aspectele legate de securitatea ***cibernetică***. În plus, oferirea de informații transparente cu privire la nivelul de securitate al produselor și serviciilor TIC ar urma să permită pieței unice digitale să se bucure de o încredere și mai mare. Acest lucru poate fi facilitat printr-o certificare la nivelul UE care să prevadă cerințe comune în materie de securitate ***cibernetică*** și criterii de evaluare aplicabile pe toate piețele naționale și în toate sectoarele.	mult decât atât, amenințările cibernetice nu se opresc la frontiere, motiv pentru care este necesară dezvoltarea capabilităților de la nivelul Uniunii care ar putea completa acțiunea statelor membre, în special în cazul incidentelor și crizelor de securitate cibernetică transfrontaliere de mare amploare. De asemenea, sunt necesare eforturi suplimentare pentru a ***oferi un răspuns coordonat al UE și pentru a*** spori gradul de sensibilizare a cetățenilor și întreprinderilor cu privire la aspectele legate de securitatea ***informatică***. În plus, oferirea de informații transparente cu privire la nivelul de securitate al produselor și serviciilor TIC ar urma să permită pieței unice digitale să se bucure de o încredere și mai mare. Acest lucru poate fi facilitat printr-o certificare la nivelul UE care să prevadă cerințe comune în materie de securitate ***informatică*** și criterii de evaluare aplicabile pe toate piețele naționale și în toate sectoarele. ***Pe lângă certificarea la nivelul UE, există o serie de măsuri voluntare acceptate la scară largă pe piață, în funcție de produs, serviciu, utilizare sau standard. Aceste măsuri, precum și abordarea ascendentă din industrie, inclusiv utilizarea securității de la stadiul conceperii, efectul de levier și contribuția la standardele internaționale, ar trebui să fie încurajate.***

Amendamentul 5

Propunere de regulament
Considerentul 7

Textul propus de Comisie	*Amendamentul*
(7) Uniunea a luat deja măsuri importante pentru a asigura securitatea ***cibernetică*** și a crește încrederea în tehnologiile digitale. În 2013, a fost adoptată Strategia de securitate cibernetică a Uniunii Europene, menită să orienteze politicile prin care Uniunea răspunde la amenințările și riscurile în materie de	(7) Uniunea a luat deja măsuri importante pentru a asigura securitatea ***informatică*** și a crește încrederea în tehnologiile digitale. În 2013, a fost adoptată Strategia de securitate cibernetică a Uniunii Europene, menită să orienteze politicile prin care Uniunea răspunde la amenințările și riscurile în materie de

securitate ***cibernetică***. În cadrul eforturilor depuse pentru a proteja mai bine europenii în mediul online, în 2016 Uniunea a adoptat primul act legislativ în domeniul securității ***cibernetice***, și anume Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune („Directiva privind securitatea rețelelor și a informațiilor”). Directiva privind securitatea rețelelor și a informațiilor a ***instituit*** cerințe privind capabilitățile naționale în domeniul securității ***cibernetice***, a creat primele mecanisme de intensificare a cooperării strategice și operaționale între statele membre și a introdus obligații privind măsurile de securitate și notificările incidentelor în sectoare vitale pentru economie și societate, cum ar fi energia, transporturile, apa, băncile, infrastructurile pieței financiare, asistența medicală, infrastructurile digitale, precum și furnizorii de servicii digitale esențiale (motoarele de căutare, serviciile de cloud computing și piețele online). ENISA a primit un rol esențial de sprijinire a punerii în aplicare a directivei menționate mai sus. În plus, combaterea eficace a criminalității cibernetice se numără printre prioritățile importante ale Agendei europene privind securitatea, contribuind la obiectivul general de obținere a unui nivel ridicat de securitate ***cibernetică***.

securitate ***informatică***. În cadrul eforturilor depuse pentru a proteja mai bine europenii în mediul online, în 2016 Uniunea a adoptat primul act legislativ în domeniul securității ***informatice***, și anume Directiva (UE) 2016/1148 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune („Directiva privind securitatea rețelelor și a informațiilor”). Directiva privind securitatea rețelelor și a informațiilor ***îndeplinește strategia privind piața unică digitală și, împreună cu alte instrumente, cum ar fi Directiva.../... [de instituire*** a ***Codului european al comunicațiilor electronice], Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului[1a] și Directiva 2002/58/CE a Parlamentului European și a Consiliului[1b], instituie*** cerințe privind capabilitățile naționale în domeniul securității ***informatice***, a creat primele mecanisme de intensificare a cooperării strategice și operaționale între statele membre și a introdus obligații privind măsurile de securitate și notificările incidentelor în sectoare vitale pentru economie și societate, cum ar fi energia, transporturile, apa, băncile, infrastructurile pieței financiare, asistența medicală, infrastructurile digitale, precum și furnizorii de servicii digitale esențiale (motoarele de căutare, serviciile de cloud computing și piețele online). ENISA a primit un rol esențial de sprijinire a punerii în aplicare a directivei menționate mai sus. În plus, combaterea eficace a criminalității cibernetice se numără printre prioritățile importante ale Agendei europene privind securitatea, contribuind la obiectivul general de obținere a unui nivel ridicat de securitate ***informatică***.

[1a] Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal

și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

[1b] Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37).

Amendamentul 6

Propunere de regulament
Considerentul 8

Textul propus de Comisie	*Amendamentul*
(8) Este recunoscut faptul că, de la adoptarea Strategiei de securitate cibernetică a UE, în 2013, și de la ultima revizuire a mandatului agenției, contextul general de politici a cunoscut schimbări semnificative, legate, de asemenea, de apariția unui mediu mondial mai incert și mai puțin sigur. În acest context, în cadrul noii politici de securitate ***cibernetică*** a Uniunii, este necesar să se revizuiască mandatul ENISA pentru a defini rolul care îi revine în ecosistemul de securitate ***cibernetică*** rezultat în urma acestor evoluții și pentru a oferi asigurarea că agenția ***contribuie în mod eficace la*** răspunsul Uniunii la provocările în materie de securitate ***cibernetică*** ce își au originea în această transformare radicală a naturii amenințărilor, pentru care, astfel cum se recunoaște în evaluarea agenției, mandatul actual nu este suficient.	(8) Este recunoscut faptul că, de la adoptarea Strategiei de securitate cibernetică a UE, în 2013, și de la ultima revizuire a mandatului agenției, contextul general de politici a cunoscut schimbări semnificative, legate, de asemenea, de apariția unui mediu mondial mai incert și mai puțin sigur. În acest context, în cadrul noii politici de securitate ***informatică*** a Uniunii, este necesar să se revizuiască mandatul ENISA pentru a defini rolul care îi revine în ecosistemul de securitate ***informatică*** rezultat în urma acestor evoluții și pentru a oferi asigurarea că agenția ***își asumă un rol central care va îmbunătăți efectiv*** răspunsul Uniunii la provocările în materie de securitate ***informatică*** ce își au originea în această transformare radicală a naturii amenințărilor, pentru care, astfel cum se recunoaște în evaluarea agenției, mandatul actual nu este suficient.

Amendamentul 7

Propunere de regulament

Considerentul 11

Textul propus de Comisie	*Amendamentul*
(11) Având în vedere agravarea provocărilor în materie de securitate ***cibernetică*** cu care se confruntă Uniunea, ar fi necesară o sporire a resurselor financiare și umane alocate agenției, care să corespundă consolidării rolului și sarcinilor sale, precum și poziției sale critice în ecosistemul de organizații care apără ecosistemul digital european.	(11) Având în vedere agravarea provocărilor în materie de securitate ***informatică*** cu care se confruntă Uniunea, ar fi necesară o sporire a resurselor financiare și umane alocate agenției, care să corespundă consolidării rolului și sarcinilor sale, precum și poziției sale critice în ecosistemul de organizații care apără ecosistemul digital european. ***Ar trebui să se acorde atenția cuvenită consolidării în continuare a capacității agenției.***

Justificare

Este esențial să remediem lipsa de capacitate a agenției. De asemenea, sunt necesare eforturi vizând dezvoltarea în continuare a agenției, având în vedere cât de importantă este securitatea cibernetică în prezent și, mai mult, cât de importantă va fi „mâine”. De remarcat interferența Rusiei în alegeri, creșterea capacităților superputerilor și a statelor din întreaga lume, digitizarea iminentă a sectoarelor majore.

Amendamentul 8

Propunere de regulament
Considerentul 11 a (nou)

Textul propus de Comisie	*Amendamentul*
	(11a) În era digitală, provocările din domeniul securității informatice sunt adesea strâns legate de provocările din domeniul protecției datelor, al protecției vieții private, precum și al protecției comunicațiilor electronice. Pentru ca agenția să poată aborda în mod corespunzător aceste provocări, sunt necesare cooperarea strânsă și consultările frecvente cu organismele instituite în temeiul Regulamentului (CE) nr. 45/2001 al Parlamentului European și al Consiliului[1a], al Regulamentului (UE) nr. 2016/679, al Directivei (UE) 2016/680 și al Regulamentului (CE) nr. 1211/2009,

precum și cu industria și societatea civilă.

[1a]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 (JO L 8, 12.1.2001, p. 1).

Amendamentul 9

Propunere de regulament
Considerentul 12

Textul propus de Comisie	*Amendamentul*
(12) Agenția ar trebui să dezvolte și să mențină un nivel ridicat de expertiză și să funcționeze ca punct de referință, instaurând încrederea în piața unică grație independenței sale, calității consilierii acordate și informațiilor diseminate, transparenței procedurilor și metodelor sale de operare, precum și eforturilor depuse în îndeplinirea sarcinilor sale. Agenția ar trebui să contribuie în mod proactiv la eforturile depuse la nivel național și la nivelul UE, îndeplinindu-și totodată sarcinile în deplină cooperare cu instituțiile, organele, oficiile și agențiile Uniunii și cu statele membre. În plus, agenția ar trebui să se bazeze pe informațiile primite de la sectorul privat și alte părți interesate relevante și pe cooperarea cu acestea. ***Este necesar să se stabilească printr-o*** serie de sarcini ***modul în*** care agenția trebuie să ***își*** realizeze ***obiectivele***, ***permițându-i*** în ***același timp să funcționeze flexibil***.	(12) Agenția ar trebui să dezvolte și să mențină un nivel ridicat de expertiză și să funcționeze ca punct de referință, instaurând încrederea în piața unică grație independenței sale, calității consilierii acordate și informațiilor diseminate, transparenței procedurilor și metodelor sale de operare, precum și eforturilor depuse în îndeplinirea sarcinilor sale. Agenția ar trebui să contribuie în mod proactiv la eforturile depuse la nivel național și la nivelul UE, îndeplinindu-și totodată sarcinile în deplină cooperare cu instituțiile, organele, oficiile și agențiile Uniunii și cu statele membre. În plus, agenția ar trebui să se bazeze pe informațiile primite de la sectorul privat și alte părți interesate relevante și pe cooperarea cu acestea. ***Ar trebui definite o agendă clară și o*** serie de sarcini ***și obiective pe*** care agenția trebuie să ***le*** realizeze, ***acordând totodată atenția cuvenită flexibilității necesare operațiunilor sale. În măsura posibilului, ar trebui păstrat cel mai înalt grad de transparență și de diseminare a informațiilor.***

Amendamentul 10

Propunere de regulament
Considerentul 14

Textul propus de Comisie	*Amendamentul*
(14) Sarcina fundamentală a agenției este de a promova punerea în aplicare coerentă a cadrului juridic relevant, în special punerea în aplicare eficace a Directivei privind securitatea rețelelor și a informațiilor, care este esențială pentru sporirea rezilienței cibernetice. Având în vedere evoluția rapidă a naturii amenințărilor la adresa securității ***cibernetice***, este clar că statele membre trebuie să fie sprijinite printr-o abordare mai cuprinzătoare, bazată pe mai multe politici, a consolidării rezilienței cibernetice.	(14) Sarcina fundamentală a agenției este de a promova punerea în aplicare coerentă a cadrului juridic relevant, în special punerea în aplicare eficace a Directivei privind securitatea rețelelor și a informațiilor, ***Directivei .../... [de instituire a Codului european al comunicațiilor electronice], a Regulamentului (UE) 2016/679 și a Directivei 2002/58/CE,*** care este esențială pentru sporirea rezilienței cibernetice. Având în vedere evoluția rapidă a naturii amenințărilor la adresa securității ***informatice***, este clar că statele membre trebuie să fie sprijinite printr-o abordare mai cuprinzătoare, bazată pe mai multe politici, a consolidării rezilienței cibernetice.

Amendamentul 11

Propunere de regulament
Considerentul 21 a (nou)

Textul propus de Comisie	*Amendamentul*
	(21a) Comisia ar trebui să propună introducerea cooperării obligatorii între statele membre în ceea ce privește protecția infrastructurilor critice de informație.

Amendamentul 12

Propunere de regulament
Considerentul 26

Textul propus de Comisie	*Amendamentul*
(26) Pentru a înțelege mai bine provocările din domeniul securității	(26) Pentru a înțelege mai bine provocările din domeniul securității

cibernetice și a oferi consiliere strategică pe termen lung statelor membre și instituțiilor Uniunii, este necesar ca agenția să analizeze riscurile actuale și pe cele emergente. În acest scop, agenția ar trebui să colecteze informațiile relevante în cooperare cu statele membre și, după caz, cu organismele de statistică și cu alte entități, să efectueze analize privind tehnologiile emergente și să furnizeze evaluări tematice privind impactul societal, juridic, economic și în materie de reglementare al inovațiilor tehnologice asupra securității rețelelor și informațiilor, în special asupra securității ***cibernetice***. În plus, agenția ar trebui să sprijine statele membre și instituțiile, agențiile și organele Uniunii în ceea ce privește identificarea tendințelor emergente și prevenirea problemelor legate de securitatea ***cibernetică***, prin efectuarea de analize ale amenințărilor și ***incidentelor***.

informatice și a oferi consiliere strategică pe termen lung statelor membre și instituțiilor Uniunii, este necesar ca agenția să analizeze riscurile actuale și pe cele emergente***, incidentele și vulnerabilitățile***. În acest scop, agenția ar trebui să colecteze informațiile relevante în cooperare cu statele membre și, după caz, cu organismele de statistică și cu alte entități, să efectueze analize privind tehnologiile emergente și să furnizeze evaluări tematice privind impactul societal, juridic, economic și în materie de reglementare al inovațiilor tehnologice asupra securității rețelelor și informațiilor, în special asupra securității ***informatice***. În plus, agenția ar trebui să sprijine statele membre și instituțiile, agențiile și organele Uniunii în ceea ce privește identificarea tendințelor emergente și prevenirea problemelor legate de securitatea ***informatică***, prin efectuarea de analize ale amenințărilor***, incidentelor*** și ***vulnerabilităților***.

Amendamentul 13

Propunere de regulament
Considerentul 28

Textul propus de Comisie	*Amendamentul*
(28) Agenția ar trebui să contribuie la sensibilizarea publicului cu privire la riscurile legate de securitatea ***cibernetică*** și să furnizeze, în atenția cetățenilor și organizațiilor, orientări privind bunele practici care trebuie adoptate de utilizatorii individuali. De asemenea, agenția ar trebui să contribuie la promovarea celor mai bune practici și soluții în rândul persoanelor fizice și organizațiilor, prin colectarea și analiza informațiilor ***aflate la dispoziția publicului*** referitoare la incidentele semnificative și prin întocmirea de rapoarte cu scopul de a furniza orientări întreprinderilor ***și*** cetățenilor și ***de a îmbunătăți nivelul global de pregătire*** și ***reziliență***. În plus, agenția ar trebui să	(28) Agenția ar trebui să contribuie la sensibilizarea publicului cu privire la riscurile legate de securitatea ***informatică*** și să furnizeze, în atenția cetățenilor și organizațiilor, orientări privind bunele practici care trebuie adoptate de utilizatorii individuali. De asemenea, ***pentru a îmbunătăți nivelul global de pregătire și reziliență,*** agenția ar trebui să contribuie la promovarea celor mai bune practici și soluții în rândul persoanelor fizice și ***al*** organizațiilor, prin colectarea și analiza informațiilor referitoare la incidentele semnificative și prin întocmirea de rapoarte cu scopul de a furniza orientări întreprinderilor***,*** cetățenilor și ***autorităților competente de la nivel european*** și

organizeze, în cooperare cu instituțiile, organele, oficiile și agențiile statelor membre și ale Uniunii, activități de informare periodice și campanii publice de educație pentru utilizatorii finali***, având ca scop promovarea unor*** comportamente individuale online mai sigure și ***sensibilizarea*** cu privire la eventualele pericole din spațiul cibernetic, inclusiv actele de criminalitate cibernetică, cum ar fi atacurile de tip phishing, rețelele botnet, fraudele financiare și bancare, precum și ***promovarea consilierii*** de bază ***privind autentificarea*** și ***protecția datelor***. Agenția ar trebui să joace un rol central în accelerarea sensibilizării utilizatorilor finali cu privire la securitatea dispozitivelor.	***național***. În plus, agenția ar trebui să organizeze, în cooperare cu instituțiile, organele, oficiile și agențiile statelor membre și ale Uniunii, activități de informare periodice și campanii publice de educație pentru utilizatorii finali***. Aceste campanii ar trebui să promoveze educația în domeniul securității informatice și*** comportamente individuale online mai sigure și ***să sensibilizeze*** cu privire la eventualele pericole din spațiul cibernetic, inclusiv actele de criminalitate cibernetică, cum ar fi atacurile de tip phishing, rețelele botnet, fraudele financiare și bancare***, falsificarea și materialele ilegale***, precum și ***să pledeze pentru protecția datelor și autentificarea*** de bază ***pentru a preveni furtul de date*** și ***de identitate***. Agenția ar trebui să joace un rol central în accelerarea sensibilizării utilizatorilor finali cu privire la securitatea dispozitivelor.

Amendamentul 14

Propunere de regulament
Considerentul 28 a (nou)

Textul propus de Comisie	*Amendamentul*
	(28a) Agenția ar trebui să sensibilizeze publicul cu privire la riscurile legate de incidentele de fraudă și furturile de date care pot afecta grav drepturile fundamentale ale persoanelor, pot submina statul de drept și pot pune în pericol stabilitatea societăților democratice, inclusiv a proceselor democratice din statele membre.

Amendamentul 15

Propunere de regulament
Considerentul 30

Textul propus de Comisie	*Amendamentul*
(30) Pentru a asigura îndeplinirea în	(30) Pentru a asigura îndeplinirea în

totalitate a obiectivelor sale, agenția ar trebui să colaboreze cu instituțiile, agențiile și organismele relevante, inclusiv cu CERT-UE, Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol, Agenția Europeană de Apărare (AEA), Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă (eu-LISA), Agenția Europeană de Siguranță a Aviației (AESA) și orice altă agenție a UE implicată în securitatea ***cibernetică***. Agenția ar trebui, de asemenea, să colaboreze cu autoritățile care îndeplinesc sarcini de protecție a datelor pentru a face schimb de cunoștințe de specialitate și de bune practici și pentru a oferi consiliere privind aspectele legate de securitatea ***cibernetică*** ce ar putea avea un impact asupra activității acestora. Reprezentanții autorităților naționale și ale Uniunii responsabile de aplicarea legii și de protecția datelor ar trebui să fie eligibili pentru a fi reprezentați în grupul permanent al părților interesate din cadrul agenției. În activitatea sa de colaborare cu organele responsabile de aplicarea legii, cu privire la aspectele de securitate a rețelelor și a informațiilor care ar putea avea un impact asupra activității acestora, agenția ar trebui să respecte canalele de informații și rețelele existente.

totalitate a obiectivelor sale, agenția ar trebui să colaboreze cu instituțiile, agențiile și organismele relevante, inclusiv cu CERT-UE, Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol, Agenția Europeană de Apărare (AEA), Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă (eu-LISA), Agenția Europeană de Siguranță a Aviației (AESA)***, Agenția GNSS European (GSA)*** și orice altă agenție a UE implicată în securitatea ***informatică***. Agenția ar trebui, de asemenea, să colaboreze cu autoritățile ***Uniunii și autoritățile naționale*** care îndeplinesc sarcini de protecție a datelor pentru a face schimb de cunoștințe de specialitate și de bune practici și pentru a oferi consiliere privind aspectele legate de securitatea ***informatică*** ce ar putea avea un impact asupra activității acestora. Reprezentanții autorităților naționale și ale Uniunii responsabile de aplicarea legii și de protecția datelor ar trebui să fie eligibili pentru a fi reprezentați în grupul permanent al părților interesate din cadrul agenției. În activitatea sa de colaborare cu organele responsabile de aplicarea legii, cu privire la aspectele de securitate a rețelelor și a informațiilor care ar putea avea un impact asupra activității acestora, agenția ar trebui să respecte canalele de informații și rețelele existente.

Justificare

Dat fiind că există probleme de securitate informatică în cadrul programului Galileo, în special în sectoarele terestre, cooperarea cu Agenția GNSS European consolidează rolul ENISA, sporind în același timp credibilitatea programului Galileo.

Amendamentul 16

Propunere de regulament
Considerentul 35

Textul propus de Comisie	*Amendamentul*

(35) Agenția ar trebui să încurajeze statele membre și furnizorii de servicii să-și ridice standardele generale de securitate, astfel încât toți utilizatorii de internet să poată lua măsurile necesare pentru a-și asigura securitatea ***cibernetică*** personală. În particular, furnizorii de servicii și fabricanții de produse ar trebui să retragă sau să recicleze produsele și serviciile care nu îndeplinesc standardele de securitate ***cibernetică***. În cooperare cu autoritățile competente, ENISA poate difuza informații privind nivelul de securitate ***cibernetică*** al produselor și serviciilor oferite pe piața internă și emite avertismente prin care să oblige furnizorii și fabricanții să îmbunătățească securitatea, inclusiv ***cibernetică***, a produselor și serviciilor lor.

(35) Agenția ar trebui să încurajeze statele membre***, producătorii de hardware și software și de TIC, precum*** și furnizorii de servicii ***online*** să-și ridice standardele generale de securitate, astfel încât toți utilizatorii de internet să poată lua măsurile necesare pentru a-și asigura securitatea ***informatică*** personală. În particular, furnizorii de servicii și fabricanții de produse ar trebui să retragă sau să recicleze produsele și serviciile care nu îndeplinesc standardele de securitate ***informatică***. În cooperare cu autoritățile competente, ENISA poate difuza informații privind nivelul de securitate ***informatică*** al produselor și serviciilor oferite pe piața internă și emite avertismente prin care să oblige furnizorii și fabricanții să îmbunătățească securitatea, inclusiv ***informatică***, a produselor și serviciilor lor. ***Agenția ar trebui să colaboreze cu părțile interesate pentru a dezvolta o abordare la nivelul UE vizând divulgarea responsabilă a vulnerabilităților și ar trebui să promoveze cele mai bune practici în acest domeniu.***

Amendamentul 17

Propunere de regulament
Considerentul 44

Textul propus de Comisie	*Amendamentul*
(44) Agenția ar trebui să aibă drept organism consultativ un grup permanent al părților interesate, pentru a asigura un dialog regulat cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. Grupul permanent al părților interesate, instituit de consiliul de administrație la propunerea directorului executiv, ar trebui să se concentreze pe probleme relevante pentru părțile interesate și să le aducă în atenția agenției. Componența grupului permanent al părților interesate și sarcinile încredințate acestuia, care urmează să fie consultat în special în	(44) Agenția ar trebui să aibă drept organism consultativ un grup permanent al părților interesate, pentru a asigura un dialog regulat cu sectorul privat, cu organizațiile de consumatori și cu alte părți interesate relevante. Grupul permanent al părților interesate, instituit de consiliul de administrație la propunerea directorului executiv, ar trebui să se concentreze pe probleme relevante pentru părțile interesate și să le aducă în atenția agenției. Componența grupului permanent al părților interesate și sarcinile încredințate acestuia, care urmează să fie consultat în special în

legătură cu proiectul de program de activitate, ar trebui să asigure faptul că părțile interesate sunt reprezentate într-o măsură suficientă în ceea ce privește activitatea agenției .	legătură cu proiectul de program de activitate, ar trebui să asigure faptul că părțile interesate sunt reprezentate într-o măsură suficientă în ceea ce privește activitatea agenției . ***Având în vedere importanța cerințelor de certificare pentru a asigura încrederea în IoT, Comisia ar trebui să ia în considerare, în mod special, măsuri de punere în aplicare pentru a asigura armonizarea la nivelul Uniunii a standardelor de securitate pentru dispozitivele IoT.***

Amendamentul 18

Propunere de regulament
Considerentul 50

Textul propus de Comisie	*Amendamentul*
(50) În prezent, certificarea de securitate ***cibernetică*** a produselor și serviciilor TIC nu este utilizată decât într-o măsură limitată. Atunci când există, certificarea se aplică în principal la nivelul statelor membre sau în cadrul sistemelor instituite de sector. În acest context, un certificat emis de o autoritate națională de securitate ***cibernetică*** nu este, în principiu, recunoscut de celelalte state membre. Prin urmare, este posibil ca întreprinderile să fie nevoite să își certifice produsele și serviciile în fiecare dintre statele membre în care își desfășoară activitatea, pentru a putea participa, de exemplu, la procedurile de achiziții publice naționale. În plus, deși apar noi sisteme, nu pare să existe o abordare coerentă și holistică a aspectelor orizontale ale securității ***cibernetice***, de exemplu în domeniul internetului obiectelor. Sistemele existente prezintă importante deficiențe și diferențe în ceea ce privește produsele vizate, nivelurile de asigurare, criteriile de fond și utilizarea efectivă.	(50) În prezent, certificarea de securitate ***informatică*** a produselor și serviciilor TIC nu este utilizată decât într-o măsură limitată. Atunci când există, certificarea se aplică în principal la nivelul statelor membre sau în cadrul sistemelor instituite de sector. În acest context, un certificat emis de o autoritate națională de securitate ***informatică*** nu este, în principiu, recunoscut de celelalte state membre. Prin urmare, este posibil ca întreprinderile să fie nevoite să își certifice produsele și serviciile în fiecare dintre statele membre în care își desfășoară activitatea, pentru a putea participa, de exemplu, la procedurile de achiziții publice naționale***, aceste proceduri adăugând costuri suplimentare întreprinderilor***. În plus, deși apar noi sisteme, nu pare să existe o abordare coerentă și holistică a aspectelor orizontale ale securității ***informatice***, de exemplu în domeniul internetului obiectelor. Sistemele existente prezintă importante deficiențe și diferențe în ceea ce privește produsele vizate, nivelurile de asigurare, criteriile de fond și utilizarea efectivă. ***O abordare de la caz la caz ar trebui să asigure că serviciile și produsele sunt supuse unor***

	sisteme de certificare corespunzătoare. În plus, o abordare bazată pe riscuri este necesară pentru identificarea eficientă și reducerea riscurilor și pentru a evita creșterea costurilor pentru producători.

Amendamentul 19

Propunere de regulament
Considerentul 52

Textul propus de Comisie	*Amendamentul*
(52) Având în vedere cele de mai sus, este necesar să se instituie un cadru european de certificare de securitate ***cibernetică*** prin care să se stabilească principalele cerințe orizontale pentru sistemele europene de certificare de securitate ***cibernetică*** ce urmează să fie create și să se permită recunoașterea și utilizarea în toate statele membre a certificatelor pentru produse și servicii TIC. Cadrul european ar trebui să aibă o dublă finalitate: pe de o parte, acesta ar trebui să contribuie la creșterea încrederii în produsele și serviciile TIC care au fost certificate în conformitate cu aceste sisteme, pe de altă parte, cadrul ar trebui să evite multiplicarea de certificări naționale de securitate ***cibernetică*** ce se contrazic sau se suprapun și să permită astfel reducerea costurilor pentru întreprinderile care își desfășoară activitatea pe piața unică digitală. Aceste sisteme ar trebui să fie nediscriminatorii și să se bazeze pe standarde internaționale și/sau ale Uniunii, cu excepția cazului în care aceste standarde sunt ineficace sau inadecvate pentru îndeplinirea obiectivelor legitime ale UE în această privință.	(52) Având în vedere cele de mai sus, este necesar să se instituie un cadru ***armonizat*** european de certificare de securitate ***informatică*** prin care să se stabilească principalele cerințe orizontale pentru sistemele europene de certificare de securitate ***informatică*** ce urmează să fie create și să se permită recunoașterea și utilizarea în toate statele membre a certificatelor pentru produse și servicii TIC. Cadrul european ar trebui să aibă o dublă finalitate: pe de o parte, acesta ar trebui să contribuie la creșterea încrederii în produsele și serviciile TIC care au fost certificate în conformitate cu aceste sisteme, pe de altă parte, cadrul ar trebui să evite multiplicarea de certificări naționale de securitate ***informatică*** ce se contrazic sau se suprapun și să permită astfel reducerea costurilor pentru întreprinderile care își desfășoară activitatea pe piața unică digitală. Aceste sisteme ar trebui să fie nediscriminatorii și să se bazeze pe standarde internaționale și/sau ale Uniunii, cu excepția cazului în care aceste standarde sunt ineficace sau inadecvate pentru îndeplinirea obiectivelor legitime ale UE în această privință.

Amendamentul 20

Propunere de regulament
Considerentul 55

Textul propus de Comisie	*Amendamentul*
(55) Sistemele europene de certificare de securitate ***cibernetică*** ar trebui să aibă drept scop asigurarea conformității cu cerințele specificate a produselor și serviciilor TIC certificate în temeiul unui astfel de sistem. Aceste cerințe se referă la capacitatea de a rezista, la un anumit nivel de asigurare, la acțiuni care au scopul de a compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate ori transmise sau prelucrate ori funcțiile sau serviciile oferite de aceste produse, procese, servicii și sisteme sau accesibile prin intermediul lor, în sensul prezentului regulament. În prezentul regulament nu pot fi detaliate cerințele de securitate ***cibernetică*** referitoare la toate produsele și serviciile TIC. Produsele și serviciile TIC și necesitățile conexe în materie de securitate ***cibernetică*** sunt atât de variate încât este foarte dificil să se elaboreze cerințe generale de securitate ***cibernetică*** cu valabilitate universală. Prin urmare, este necesar să se adopte o noțiune largă și generală a securității ***cibernetice*** în scopul certificării, completată printr-o serie de obiective de securitate ***cibernetică*** specifice, care trebuie să fie luate în considerare atunci când se concep sisteme europene de certificare de securitate ***cibernetică***. Modalitățile prin care aceste obiective vor fi atinse de produse și servicii TIC specifice ar trebui să fie detaliate și mai precis, într-o etapă ulterioară, la nivelul fiecărui sistem de certificare adoptat de Comisie, de exemplu prin trimitere la standarde sau la specificații tehnice.	(55) Sistemele europene de certificare de securitate ***informatică*** ar trebui să aibă drept scop asigurarea conformității cu cerințele specificate a produselor și serviciilor TIC certificate în temeiul unui astfel de sistem. Aceste cerințe se referă la capacitatea de a rezista, la un anumit nivel de asigurare, la acțiuni care au scopul de a compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate ori transmise sau prelucrate ori funcțiile sau serviciile oferite de aceste produse, procese, servicii și sisteme sau accesibile prin intermediul lor, în sensul prezentului regulament. În prezentul regulament nu pot fi detaliate cerințele de securitate ***informatică*** referitoare la toate produsele și serviciile TIC. Produsele și serviciile TIC și necesitățile conexe în materie de securitate ***informatică*** sunt atât de variate***, la fel ca și ciclul lor de viață,*** încât este foarte dificil să se elaboreze cerințe generale de securitate ***informatică*** cu valabilitate universală. Prin urmare, este necesar să se adopte o noțiune largă și generală a securității ***informatice*** în scopul certificării, completată printr-o serie de obiective de securitate ***informatică*** specifice, care trebuie să fie luate în considerare atunci când se concep sisteme europene de certificare de securitate ***informatică***. Modalitățile prin care aceste obiective vor fi atinse de produse și servicii TIC specifice ar trebui să fie detaliate și mai precis, într-o etapă ulterioară, la nivelul fiecărui sistem de certificare adoptat de Comisie ***în strânsă consultare cu statele membre și părțile interesate din industrie***, de exemplu prin trimitere la standarde sau la specificații tehnice. ***Schemele de certificare individuale ar trebui concepute astfel încât toți actorii implicați în dezvoltarea produselor și serviciilor IT relevante să fie încurajați să elaboreze și să adopte standarde, norme și principii care să asigure cel mai înalt nivel posibil de securitate pe tot parcursul***

ciclului de viață.

Amendamentul 21

Propunere de regulament
Considerentul 55 a (nou)

Textul propus de Comisie	*Amendamentul*
	(55a) ENISA ar trebui să elaboreze o schemă de certificare cu perspectivă globală pentru a preveni viitoarele bariere în calea comerțului. În procesul de elaborare a criteriilor pentru sistemul de certificare, ENISA ar trebui să se angajeze în dialog cu partenerii relevanți din sector pentru a asigura fezabilitatea din perspectiva pieței.

Amendamentul 22

Propunere de regulament
Considerentul 56

Textul propus de Comisie	*Amendamentul*
(56) Comisia ar trebui să fie împuternicită să adreseze ENISA solicitarea de a pregăti propuneri de sisteme pentru produse sau servicii TIC specifice. Pe baza propunerii de sistem prezentate de ENISA, Comisia ar trebui să fie împuternicită după aceea să adopte sistemul european de certificare de securitate ***cibernetică*** prin intermediul unor acte de punere în aplicare. Ținând seama de scopul general și de obiectivele de securitate identificate în prezentul regulament, sistemele europene de certificare de securitate ***cibernetică*** adoptate de Comisie ar trebui să specifice un set minim de elemente referitoare la obiectul, domeniul de aplicare și funcționarea fiecărui sistem. Acestea ar trebui să includă, printre altele, domeniul de aplicare și obiectul certificării de securitate ***cibernetică***, inclusiv categoriile	(56) Comisia ar trebui să fie împuternicită să adreseze ENISA solicitarea de a pregăti propuneri de sisteme pentru produse sau servicii TIC specifice. Pe baza propunerii de sistem prezentate de ENISA, Comisia ar trebui să fie împuternicită după aceea să adopte sistemul european de certificare de securitate ***informatică*** prin intermediul unor acte de punere în aplicare. Ținând seama de scopul general și de obiectivele de securitate identificate în prezentul regulament, sistemele europene de certificare de securitate ***informatică*** adoptate de Comisie ar trebui să specifice un set minim de elemente referitoare la obiectul, domeniul de aplicare și funcționarea fiecărui sistem. Acestea ar trebui să includă, printre altele, domeniul de aplicare și obiectul certificării de securitate ***informatică***, inclusiv categoriile

de produse și servicii TIC care fac obiectul acesteia, specificații detaliate cu privire la cerințele de securitate ***cibernetică***, de exemplu prin trimitere la standarde sau la specificații tehnice, criteriile specifice și metodele de evaluare, precum și nivelul asigurării vizate: de bază, substanțială și/sau ridicată.	de produse și servicii TIC care fac obiectul acesteia, specificații detaliate cu privire la cerințele de securitate ***informatică***, de exemplu prin trimitere la standarde sau la specificații tehnice, criteriile specifice și metodele de evaluare, precum și nivelul asigurării vizate: de bază, substanțială și/sau ridicată. ***Nivelurile de asigurare ar trebui să fie definite de la caz la caz, pentru a garanta că serviciile și produsele TIC fac obiectul unor sisteme de certificare adecvate, și ar trebui să ia în considerare cazurile diverse de utilizare individuale, precum și propria răspundere și educația utilizatorilor.***

Amendamentul 23

Propunere de regulament
Considerentul 57

Textul propus de Comisie	*Amendamentul*
(57) Recurgerea la certificarea europeană de securitate ***cibernetică*** ar trebui să rămână voluntară, cu excepția cazului în care există dispoziții contrare în legislația Uniunii sau în cea națională. Cu toate acestea, în scopul îndeplinirii obiectivelor prezentului regulament și pentru a se evita fragmentarea pieței interne, sistemele sau procedurile naționale de certificare de securitate ***cibernetică*** pentru produsele și serviciile TIC care fac obiectul unui sistem european de certificare de securitate ***cibernetică*** ar trebui să înceteze să mai producă efecte de la data stabilită de Comisie în actul de punere în aplicare. În plus, statele membre ar trebui să nu introducă noi sisteme naționale de certificare pentru produse și servicii TIC care fac deja obiectul unui sistem european de certificare de securitate ***cibernetică*** existent.	(57) Recurgerea la certificarea europeană de securitate ***informatică*** ar trebui să rămână voluntară, cu excepția cazului în care există dispoziții contrare în legislația Uniunii sau în cea națională. ***După această etapă inițială și în funcție de stadiul punerii în aplicare în statele membre și de caracterul critic al unui produs sau serviciu, ar putea fi introduse sisteme de certificare potențial obligatorii pentru anumite produse și servicii TIC, pe baza unei abordări pe etape, pentru generațiile viitoare de tehnologie și ca răspuns la obiectivele de politică ale viitorului.*** Cu toate acestea, în scopul îndeplinirii obiectivelor prezentului regulament și pentru a se evita fragmentarea pieței interne, sistemele sau procedurile naționale de certificare de securitate ***informatică*** pentru produsele și serviciile TIC care fac obiectul unui sistem european de certificare de securitate ***informatică*** ar trebui să înceteze să mai producă efecte de la data stabilită de

	Comisie în actul de punere în aplicare. În plus, statele membre ar trebui să nu introducă noi sisteme naționale de certificare ***de securitate informatică*** pentru produse și servicii TIC care fac deja obiectul unui sistem european de certificare de securitate ***informatică*** existent.

Amendamentul 24

Propunere de regulament
Considerentul 58 a (nou)

Textul propus de Comisie	*Amendamentul*
	(58a) Agenția ar trebui să elaboreze cerințe de referință clare în materie de securitate informatică și ar trebui să le propună Comisiei ca acte de punere în aplicare, după caz, pentru toate dispozitivele informatice vândute în Uniune sau exportate din aceasta. Aceste cerințe ar trebui să fie revizuite ulterior o dată la doi ani, pentru a se asigura îmbunătățiri continue. Aceste cerințe de referință în materie de securitate informatică ar trebui să solicite, printre altele, ca dispozitivele să nu conțină nicio vulnerabilitate de securitate cunoscută și exploatabilă, să fie capabile să accepte actualizările fiabile de securitate, ca vânzătorul să comunice autorităților competente vulnerabilitățile cunoscute și să repare sau să înlocuiască dispozitivele afectate până în momentul, precizat de producător, în care suportul tehnic în materie de securitate pentru dispozitivul respectiv se încheie.

Amendamentul 25

Propunere de regulament
Articolul 1 – paragraful 1 – litera b

Textul propus de Comisie	*Amendamentul*
(b) stabilește un cadru pentru	(b) stabilește un cadru pentru

instituirea de sisteme europene de certificare de securitate ***cibernetică***, cu scopul de a asigura un nivel adecvat de securitate ***cibernetică*** a produselor și serviciilor TIC în Uniune. Acest cadru se aplică fără a aduce atingere dispozițiilor specifice privind certificarea voluntară sau obligatorie din alte acte ale Uniunii.	instituirea de sisteme europene de certificare de securitate ***informatică***, cu scopul de a asigura un nivel adecvat de securitate ***informatică*** a produselor și serviciilor TIC în Uniune. Acest cadru se aplică fără a aduce atingere dispozițiilor specifice privind certificarea voluntară sau obligatorie din alte acte ale Uniunii.

Justificare

Modificare de natură pur lingvistică, pentru a elimina pleonasmul prezent în textul COM.

Amendamentul 26

Propunere de regulament
Articolul 2 – paragraful 1 – punctul 8

Textul propus de Comisie	*Amendamentul*
(8) „amenințare cibernetică” înseamnă orice circumstanță potențială sau orice eveniment potențial care poate avea un impact negativ asupra rețelelor și a sistemelor informatice, precum și asupra utilizatorilor acestora și a persoanelor afectate;	(8) „amenințare cibernetică” înseamnă orice circumstanță ***sau capabilitate*** potențială sau orice eveniment potențial care poate avea un impact negativ asupra rețelelor și a sistemelor informatice, precum și asupra utilizatorilor acestora și a persoanelor afectate;

Justificare

Adăugarea unui aspect important, în special în ceea ce privește evaluarea amenințărilor.

Amendamentul 27

Propunere de regulament
Articolul 4 – alineatul 3 – paragraful 1 a (nou)

Textul propus de Comisie	*Amendamentul*
	Agenția urmărește să identifice vulnerabilitățile critice ale rețelei de securitate informatică a Uniunii în ansamblul său, precum și ale statelor membre individuale. În cazul în care agenția consideră că este necesar, aceste vulnerabilități ar trebui raportate

Parlamentului European.

Amendamentul 28

Propunere de regulament
Articolul 4 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. Agenția sporește capabilitățile de securitate ***cibernetică*** la nivelul Uniunii pentru a completa acțiunea statelor membre în materie de prevenire a amenințărilor cibernetice și de reacție la acestea, în special în cazul incidentelor transfrontaliere.	5. Agenția sporește capabilitățile de securitate ***informatică*** la nivelul Uniunii pentru a completa ***și a sprijini*** acțiunea statelor membre în materie de prevenire a amenințărilor cibernetice și de reacție la acestea, în special în cazul incidentelor transfrontaliere.

Amendamentul 29

Propunere de regulament
Articolul 4 – alineatul 6

Textul propus de Comisie	*Amendamentul*
6. Agenția promovează recurgerea la certificare, inclusiv prin contribuția ***pe care și-o aduce la*** instituirea și întreținerea unui cadru de certificare de securitate ***cibernetică*** la nivelul Uniunii în conformitate cu titlul III din prezentul regulament, astfel încât asigurarea securității ***cibernetice*** a produselor și serviciilor TIC să devină mai transparentă, iar piața internă digitală să se bucure, astfel, de o mai mare încredere.	6. Agenția promovează recurgerea la certificare, inclusiv prin contribuția ***la dezvoltarea de standarde ale Uniunii și internaționale privind securitatea informatică,*** instituirea și întreținerea unui cadru de certificare de securitate ***informatică*** la nivelul Uniunii în conformitate cu titlul III din prezentul regulament, astfel încât asigurarea securității ***informatice*** a produselor și serviciilor TIC să devină mai transparentă, iar piața internă digitală să se bucure, astfel, de o mai mare încredere.

Amendamentul 30

Propunere de regulament
Articolul 4 – alineatul 7

Textul propus de Comisie	*Amendamentul*
7. Agenția promovează un nivel	7. Agenția promovează un nivel

ridicat de sensibilizare ***a cetățenilor și întreprinderilor*** cu privire la aspectele legate de securitatea ***cibernetică***.	ridicat de sensibilizare cu privire la aspectele legate de securitatea ***informatică***.

Justificare

Sensibilizarea nu ar trebui să vizeze numai cetățenii și întreprinderile, ci și toți actorii relevanți din societate, inclusiv autoritățile și legiuitorii. Acest amendament lasă în mod deliberat deschisă lista destinatarilor acestui tip de activitate.

Amendamentul 31

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2

Textul propus de Comisie	*Amendamentul*
2. acordând asistență statelor membre pentru punerea în aplicare în mod coerent a politicii și dreptului Uniunii privind securitatea ***cibernetică***, în special în ceea ce privește Directiva (UE) 2016/1148, inclusiv prin intermediul avizelor, orientărilor, consilierii și bunelor practici referitoare la teme precum gestionarea riscurilor, raportarea incidentelor și schimbul de informații, precum și facilitând schimbul de bune practici între autoritățile competente în această privință;	2. acordând asistență statelor membre pentru punerea în aplicare în mod coerent a politicii și dreptului Uniunii privind securitatea ***informatică***, în special în ceea ce privește Directiva (UE) 2016/1148***, Directiva.../... [de instituire a Codului european al comunicațiilor electronice], Regulamentul (UE) 2016/679 și Directiva 2002/58/CE***, inclusiv prin intermediul avizelor, orientărilor, consilierii și bunelor practici referitoare la teme precum gestionarea riscurilor, raportarea incidentelor și schimbul de informații, precum și facilitând schimbul de bune practici între autoritățile competente în această privință;

Amendamentul 32

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. acordând asistență Comitetului european pentru protecția datelor instituit prin Regulamentul (UE) 2016/679 în ceea

ce privește elaborarea de orientări cu scopul de a preciza, la nivel tehnic, condițiile care permit utilizarea licită a datelor cu caracter personal de către operatorii de date pentru scopuri de securitate informatică, cu obiectivul de a proteja infrastructura lor, prin detectarea și blocarea atacurilor împotriva sistemelor lor informatice în contextul:

(i) Regulamentului (UE) 2016/679;

(ii) Directivei (UE) 2016/1148; și

(iii) al directivei 2002/58/CE;

Amendamentul 33

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 b (nou)

Textul propus de Comisie	*Amendamentul*
	2b. propunând orientări cu obiectivul de a asigura că vânzătorii TIC acționează cu diligența necesară pentru a asigura soluționarea în timp util a vulnerabilităților de securitate informatică din produsele și serviciile lor, pentru a evita expunerea utilizatorilor la amenințări cibernetice;

Amendamentul 34

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 c (nou)

Textul propus de Comisie	*Amendamentul*
	2c. propunând orientări de stabilire a responsabilităților și obligațiilor juridice pentru toate părțile interesate (inclusiv utilizatorii finali) care participă la ecosistemele TIC;

Amendamentul 35

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 d (nou)

Textul propus de Comisie	*Amendamentul*
	2d. propunând orientări, în conformitate cu dreptul intern, referitoare la reglementările privind responsabilitățile operatorilor de infrastructuri în rețea de importanță critică în cazul unui atac împotriva sistemelor lor informatice, care afectează utilizatorii acestora, din cauza absenței diligenței necesare a unor utilizatori sau chiar a operatorului, în cazul în care acesta nu a luat măsuri rezonabile pentru a preveni incidentul sau pentru a atenua efectele acestuia asupra tuturor utilizatorilor;

Amendamentul 36

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 e (nou)

Textul propus de Comisie	*Amendamentul*
	2e. propunând orientări pentru a limita achiziționarea și utilizarea de „zile zero” de către autoritățile publice, cu scopul de a ataca sistemele informatice; promovând auditurile de software și finanțarea personalului specializat;

Amendamentul 37

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 f (nou)

Textul propus de Comisie	*Amendamentul*
	2f. propunând orientări privind

	publicarea de către autoritățile publice, întreprinderile private, cercetători, universități și alte părți interesate a tuturor vulnerabilităților de securitate de importanță critică, care nu sunt încă cunoscute în mod public, în cadrul unei comunicări responsabile;

Amendamentul 38

Propunere de regulament
Articolul 5 – alineatul 1 – punctul 2 g (nou)

Textul propus de Comisie	*Amendamentul*
	2g. propunând politici pentru extinderea utilizării „codului verificabil cu sursă deschisă” pentru soluții informatice în sectorul public, precum și pentru utilizarea aferentă a instrumentelor automatizate, în vederea facilitării revizuirii codului sursă și verificării cu ușurință a absenței ușilor secrete și a altor eventuale vulnerabilități în materie de securitate;

Amendamentul 39

Propunere de regulament
Articolul 6 – alineatul 1 – litera fa (nouă)

Textul propus de Comisie	*Amendamentul*
	(fa) și cooperează cu autoritățile naționale de supraveghere a protecției datelor, dacă este necesar;

Amendamentul 40

Propunere de regulament
Articolul 6 – alineatul 2 a (nou)

Textul propus de Comisie	*Amendamentul*
	2a. Agenția facilitează crearea și lansarea unui proiect european de securitate informatică pe termen lung, pentru a sprijini creșterea unei industrii independente a UE în materie de securitate informatică și pentru a integra securitatea informatică în toate evoluțiile din sectorul informatic la nivelul UE.

Justificare

ENISA ar trebui să consilieze legislatorii cu privire la pregătirea politicilor care să permită UE să ajungă la nivelul industriilor de securitate informatică din țările terțe. Proiectul ar trebui să fie la o scară comparabilă cu ceea ce a fost realizat anterior în sectorul aviatic (exemplul Airbus). Acesta este necesar pentru a dezvolta o industrie TIC mai puternică, independentă și de încredere la nivelul UE (vezi studiul STOA, PE 614.531).

Amendamentul 41

Propunere de regulament
Articolul 7 – alineatul 5

Textul propus de Comisie	*Amendamentul*
5. În urma unei cereri formulate de ***două sau mai multe state membre afectate*** și cu singurul scop de a furniza consiliere pentru prevenirea viitoarelor incidente, agenția acordă sprijin sau efectuează o anchetă tehnică ex post în urma notificărilor primite de întreprinderile afectate de incidente care au un impact semnificativ sau substanțial, în temeiul Directivei (UE) 2016/1148. De asemenea, agenția efectuează o astfel de anchetă numai în urma unei cereri justificate în mod corespunzător din partea Comisiei, cu acordul statelor membre în cauză, în situația în care astfel de incidente afectează mai mult de două state membre.	5. În urma unei cereri formulate de ***un stat membru*** și cu singurul scop de a furniza consiliere pentru prevenirea viitoarelor incidente, agenția acordă sprijin sau efectuează o anchetă tehnică ex post în urma notificărilor primite de întreprinderile afectate de incidente care au un impact semnificativ sau substanțial, în temeiul Directivei (UE) 2016/1148. De asemenea, agenția efectuează o astfel de anchetă numai în urma unei cereri justificate în mod corespunzător din partea Comisiei, cu acordul statelor membre în cauză, în situația în care astfel de incidente afectează mai mult de două state membre.
Domeniul de aplicare al anchetei și procedura care trebuie să fie urmată pentru efectuarea acesteia sunt stabilite de comun acord de către statele membre în cauză și	Domeniul de aplicare al anchetei și procedura care trebuie să fie urmată pentru efectuarea acesteia sunt stabilite de comun acord de către statele membre în cauză și

de agenție și nu aduc atingere niciunei investigații penale în curs privind același incident. La încheierea anchetei, agenția întocmește un raport tehnic final, în special pe baza informațiilor și observațiilor transmise de către statele membre și întreprinderea (întreprinderile) în cauză și de comun acord cu statele membre respective. Un rezumat al raportului, care se concentrează pe recomandările formulate în vederea prevenirii unor viitoare incidente, va fi pus la dispoziția rețelei CSIRT.	de agenție și nu aduc atingere niciunei investigații penale în curs privind același incident ***sau măsurilor de securitate națională dintr-un stat membru***. La încheierea anchetei, agenția întocmește un raport tehnic final, în special pe baza informațiilor și observațiilor transmise de către statele membre și întreprinderea (întreprinderile) în cauză și de comun acord cu statele membre respective. Un rezumat al raportului, care se concentrează pe recomandările formulate în vederea prevenirii unor viitoare incidente, va fi pus la dispoziția rețelei CSIRT.

Amendamentul 42

Propunere de regulament
Articolul 7 – alineatul 8 a (nou)

Textul propus de Comisie	*Amendamentul*
	8a. La cererea unei instituții, a unui organ, a unui birou sau a unei agenții a Uniunii sau a unui stat membru, agenția efectuează audituri periodice și independente ale securității informatice a infrastructurilor de importanță critică, cu scopul de a identifica posibile recomandări în vederea consolidării rezilienței acestora.

Justificare

ENISA ar trebui împuternicită să efectueze audituri preventive de securitate informatică ale oricărui tip de infrastructură de importanță critică pentru autoritățile din statele membre sau din instituțiile, agențiile etc. ale UE)

Amendamentul 43

Propunere de regulament
Articolul 8 – paragraful 1 – litera a – punctul 1

Textul propus de Comisie	*Amendamentul*

(1) pregătirea propunerilor de sisteme europene de certificare de securitate ***cibernetică*** pentru produsele și serviciile TIC***,*** în conformitate cu articolul 44 din prezentul regulament;	(1) pregătirea propunerilor de sisteme europene de certificare de securitate ***informatică*** pentru produsele și serviciile TIC ***în cooperare cu întreprinderile din sector și*** în conformitate cu articolul 44 din prezentul regulament;

Justificare

Este importantă cooperarea cu întreprinderile din acest sector.

Amendamentul 44

Propunere de regulament
Articolul 8 – paragraful 1 – litera ca (nouă)

Textul propus de Comisie	*Amendamentul*
	(ca) instituie sisteme de certificare pentru a descuraja implementarea de către vânzătorii și furnizorii de servicii TIC a unor uși secrete care slăbesc în mod deliberat securitatea informatică a produselor și serviciilor comerciale și au un efect negativ asupra securității globale a internetului.

Justificare

Acesta ar trebui recunoscut ca unul dintre principalele obiective ale sistemelor de certificare.

Amendamentul 45

Propunere de regulament
Articolul 9 – paragraful 1 – litera d

Textul propus de Comisie	*Amendamentul*
(d) colectează, organizează și pune la dispoziția publicului, prin intermediul unui portal dedicat, informații privind securitatea ***cibernetică***, furnizate de instituțiile, agențiile și organele Uniunii;	(d) colectează, organizează și pune la dispoziția publicului, prin intermediul unui portal dedicat, informații privind securitatea ***informatică***, furnizate de instituțiile, agențiile și organele Uniunii ***și puse la dispoziție de statele membre și de părțile interesate din sectorul public și***

privat;

Amendamentul 46

Propunere de regulament
Articolul 9 – paragraful 1 – litera e

Textul propus de Comisie	*Amendamentul*
(e) sensibilizează publicul cu privire la riscurile de securitate ***cibernetică*** și furnizează orientări cu privire la bune practici pentru utilizatorii individuali, destinate cetățenilor și organizațiilor;	(e) sensibilizează publicul cu privire la riscurile de securitate ***informatică, diseminează măsuri adecvate pentru prevenirea incidentelor*** și furnizează orientări cu privire la bune practici pentru utilizatorii individuali, destinate cetățenilor și organizațiilor;

Amendamentul 47

Propunere de regulament
Articolul 9 – paragraful 1 – litera ea (nouă)

Textul propus de Comisie	*Amendamentul*
	(ea) creează o rețea de puncte naționale de contact în materie de educație pentru a sprijini o mai bună coordonare și schimbul de bune practici între statele membre privind educația și sensibilizarea în materie de securitate informatică;

Amendamentul 48

Propunere de regulament
Articolul 9 – paragraful 1 – litera g

Textul propus de Comisie	*Amendamentul*
(g) organizează, în cooperare cu statele membre și cu instituțiile, organele, oficiile și ***agențiile Uniunii***, campanii periodice de informare pentru sporirea securității ***ciberneticii*** și a vizibilității acesteia în Uniune***.***	(g) organizează, în cooperare cu statele membre și cu instituțiile, organele, oficiile***,*** ***agențiile Uniunii*** și ***alte părți interesate relevante***, campanii periodice de informare pentru sporirea securității ***informatice*** și a vizibilității acesteia în Uniune***;***

Amendamentul 49

Propunere de regulament
Articolul 9 – paragraful 1 – litera ga (nouă)

Textul propus de Comisie	*Amendamentul*
	(ga) promovează adoptarea la scară largă, de către toți actorii de pe piața unică digitală a UE, a unor măsuri preventive ferme de securitate informatică și a unor tehnologii fiabile de protecție a vieții private, ca primă linie de apărare împotriva atacurilor la adresa sistemelor informatice.

Justificare

Pe baza avizului AEPD (pentru PET). Rolul ENISA ar trebui, în mod clar, să treacă dincolo de acordarea unui sprijin statelor membre, CE și agențiilor UE și să fie, de asemenea, mai vizibil pentru întreprinderile din sector și pentru publicul larg.

Amendamentul 50

Propunere de regulament
Articolul 10 – paragraful 1 – litera a

Textul propus de Comisie	*Amendamentul*
(a) consiliază Uniunea și statele membre cu privire la necesitățile și prioritățile în materie de cercetare în ***domeniul*** securității ***cibernetice*** pentru a face posibile răspunsuri eficace la riscurile și amenințările actuale și emergente, inclusiv în privința tehnologiilor informației și comunicațiilor noi și emergente, și pentru o folosire eficace a tehnologiilor de prevenire a riscurilor;	(a) consiliază Uniunea și statele membre cu privire la necesitățile și prioritățile în materie de cercetare în ***domeniile*** securității ***informatice și ale protecției datelor și a vieții private,*** pentru a face posibile răspunsuri eficace la riscurile și amenințările actuale și emergente, inclusiv în privința tehnologiilor informației și comunicațiilor noi și emergente, și pentru o folosire eficace a tehnologiilor de prevenire a riscurilor;

Amendamentul 51

Propunere de regulament

Articolul 14 – alineatul 1 – litera m

Textul propus de Comisie	*Amendamentul*
(m) numește directorul executiv și, după caz, îi prelungește mandatul sau îl demite din funcție, în conformitate cu articolul 33 din prezentul regulament;	(m) numește directorul executiv ***printr-o procedură de selecție bazată pe criterii profesionale*** și, după caz, îi prelungește mandatul sau îl demite din funcție, în conformitate cu articolul 33 din prezentul regulament;

Amendamentul 52

Propunere de regulament
Articolul 20 – alineatul 1

Textul propus de Comisie	*Amendamentul*
1. La propunerea directorului executiv, consiliul de administrație instituie un grup permanent al părților interesate, alcătuit din experți recunoscuți care reprezintă părțile interesate relevante, cum ar fi sectorul TIC, furnizorii de rețele sau de servicii de comunicații electronice accesibile publicului, grupurile de consumatori, experții universitari în domeniul securității ***cibernetice*** și reprezentanți ai autorităților competente notificate în temeiul [Directivei de instituire a Codului European al Comunicațiilor Electronice], precum și autoritățile de aplicare a legii și cele de supraveghere a protecției datelor.	1. La propunerea directorului executiv, consiliul de administrație instituie un grup permanent al părților interesate, alcătuit din experți recunoscuți care reprezintă părțile interesate relevante, cum ar fi sectorul TIC, furnizorii de rețele sau de servicii de comunicații electronice accesibile publicului, grupurile de consumatori, ***organismele europene de standardizare,*** experții universitari în domeniul securității ***informatice*** și reprezentanți ai autorităților competente notificate în temeiul [Directivei de instituire a Codului European al Comunicațiilor Electronice], precum și autoritățile de aplicare a legii și cele de supraveghere a protecției datelor.

Amendamentul 53

Propunere de regulament
Articolul 30 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Curtea de Conturi are competența de a-i audita, pe bază de documente și la fața locului, pe toți beneficiarii de granturi, contractanții și subcontractanții care au	2. Curtea de Conturi are competența de a-i audita, pe bază de documente și ***de inspecții*** la fața locului, pe toți beneficiarii de granturi, contractanții și subcontractanții

primit fonduri ale Uniunii din partea agenției.	care au primit fonduri ale Uniunii din partea agenției.

Amendamentul 54

Propunere de regulament
Articolul 44 – alineatul 2

Textul propus de Comisie	*Amendamentul*
2. Atunci când pregătește propunerile de sisteme menționate la alineatul (1) din prezentul articol, ENISA consultă toate părțile interesate relevante și cooperează îndeaproape cu Grupul. Grupul furnizează pentru ENISA asistența și consilierea de specialitate solicitate de aceasta în ceea ce privește pregătirea propunerii de sistem, inclusiv prin furnizarea de avize atunci când este necesar.	2. Atunci când pregătește propunerile de sisteme menționate la alineatul (1) din prezentul articol, ENISA consultă toate părțile interesate relevante și cooperează îndeaproape cu Grupul ***și cu grupul permanent al părților interesate***. Grupul ***și grupul permanent al părților interesate*** furnizează pentru ENISA asistența și consilierea de specialitate solicitate de aceasta în ceea ce privește pregătirea propunerii de sistem, inclusiv prin furnizarea de avize atunci când este necesar. ***Dacă este cazul, ENISA poate, în plus, să înființeze un grup de lucru de certificare al părților interesate, alcătuit din membri ai grupului permanent al părților interesate și orice alte părți interesate relevante, pentru a oferi consiliere de specialitate în domeniile acoperite de o anumită propunere de sistem.***

Justificare

Întreprinderile din sector ar trebui să fie implicate printr-un proces de consultare în elaborarea și pregătirea propunerilor de sisteme, cu scopul de a oferi expertiză pentru a asigura conceperea eficientă a acestora.

Amendamentul 55

Propunere de regulament
Articolul 44 – alineatul 4

Textul propus de Comisie	*Amendamentul*
4. Comisia, pe baza propunerii de sistem prezentate de ENISA, poate adopta acte de punere în aplicare, în conformitate cu articolul 55 alineatul (1), care să prevadă sisteme europene de certificare de securitate ***cibernetică*** pentru produsele și serviciile TIC, care îndeplinesc cerințele prevăzute la articolele 45, 46 și 47 din prezentul regulament.	4. Comisia, pe baza propunerii de sistem prezentate de ENISA, poate adopta acte de punere în aplicare, în conformitate cu articolul 55 alineatul (1), care să prevadă sisteme europene de certificare de securitate ***informatică*** pentru produsele și serviciile TIC, care îndeplinesc cerințele prevăzute la articolele 45, 46 și 47 din prezentul regulament. ***Comisia poate consulta Comitetul european pentru protecția datelor și poate ține seama de opinia acestuia înainte de a adopta aceste acte de punere în aplicare.***

Justificare

Pe baza avizului AEPD. Prezentul amendament asigură coerența între certificările din cadrul european de certificare de securitate cibernetică și RGPD.

Amendamentul 56

Propunere de regulament
Articolul 46 – alineatul 2 – partea introductivă

Textul propus de Comisie	*Amendamentul*
2. Nivelurile de asigurare de bază, substanțial și ridicat ***îndeplinesc următoarele criterii:***	2. Nivelurile de asigurare de bază, substanțial și ridicat ***se referă la un certificat emis în contextul unui sistem european de certificare de securitate informatică ce asigură un grad corespunzător de încredere în calitățile pretinse sau declarate în ceea ce privește securitatea informatică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri referitoare la standardele, inclusiv la controalele tehnice, al căror scop este de a reduce riscul de incidente de securitate informatică;***

Amendamentul 57

Propunere de regulament
Articolul 46 – alineatul 2 – litera a

Textul propus de Comisie	*Amendamentul*
(a) nivelul de asigurare de bază se referă la un certificat emis în contextul unui sistem european de certificare de securitate cibernetică ce asigură un grad limitat de încredere în calitățile pretinse sau declarate în ceea ce privește securitatea cibernetică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri conexe, inclusiv la controale tehnice, al căror scop este de a reduce riscul de incidente de securitate cibernetică;	***eliminat***

Amendamentul 58

Propunere de regulament
Articolul 46 – alineatul 2 – litera b

Textul propus de Comisie	*Amendamentul*
(b) nivelul de asigurare substanțial se referă la un certificat emis în contextul unui sistem european de certificare de securitate cibernetică ce asigură un grad substanțial de încredere în calitățile pretinse sau declarate în ceea ce privește securitatea cibernetică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri conexe, inclusiv la controale tehnice, al căror scop este de a reduce substanțial riscul de incidente de securitate cibernetică;	***eliminat***

Amendamentul 59

Propunere de regulament
Articolul 46 – alineatul 2 – litera c

Textul propus de Comisie	*Amendamentul*

(c) nivelul de asigurare ridicat se referă la un certificat emis în contextul unui sistem european de certificare de securitate cibernetică ce asigură un grad mai ridicat de încredere, față de certificatele având un nivel de asigurare substanțial, în calitățile pretinse sau declarate în ceea ce privește securitatea cibernetică ale unui produs sau serviciu TIC și este caracterizat prin trimitere la specificații tehnice, la standarde și la proceduri conexe, inclusiv la controale tehnice, al căror scop este de a preveni riscul de incidente de securitate cibernetică;	***eliminat***

Amendamentul 60

Propunere de regulament
Articolul 47 – alineatul 1 – litera aa (nouă)

Textul propus de Comisie	*Amendamentul*
	(aa) organismele de evaluare a conformității și de audit;

Amendamentul 61

Propunere de regulament
Articolul 47 – alineatul 1 – litera l

Textul propus de Comisie	*Amendamentul*
(l) identificarea sistemelor naționale de certificare de securitate ***cibernetică*** care acoperă aceleași tipuri sau categorii de produse și servicii TIC;	(l) identificarea sistemelor naționale de certificare de securitate ***informatică, în temeiul articolului 49,*** care acoperă aceleași tipuri sau categorii de produse și servicii TIC;

Amendamentul 62

Propunere de regulament
Articolul 48 – alineatul 6

Textul propus de Comisie	*Amendamentul*

6. Certificatele se emit pentru o perioadă maximă de ***trei*** ani și pot fi reînnoite în aceleași condiții, numai dacă sunt îndeplinite în continuare cerințele relevante.	6. Certificatele se emit pentru o perioadă maximă ***stabilită*** de ***la caz la caz pentru fiecare sistem, dar care nu depășește cinci*** ani***,*** și pot fi reînnoite în aceleași condiții, numai dacă sunt îndeplinite în continuare cerințele relevante.

Amendamentul 63

Propunere de regulament
Articolul 48 a (nou)

Textul propus de Comisie	*Amendamentul*
	Articolul 48a
	Cerințele de referință în materie de securitate informatică
	1. Agenția, pe baza experienței sale privind cadrul de certificare de securitate informatică în temeiul titlului III al prezentului regulament, propune Comisiei cerințe minime clare în materie de securitate informatică pentru dispozitivele informatice vândute în Uniune sau exportate de aceasta, cum ar fi:
	(a) producătorul furnizează o certificare în scris a faptului că dispozitivul nu conține nicio componentă de hardware, software sau firmware care are o vulnerabilitate cunoscută și exploatabilă în materie de securitate;
	(b) dispozitivul se bazează pe componente de software sau firmware capabile să accepte actualizări autentificate adecvat și fiabile de la producător;
	(c) dispozitivul nu include nicio parolă sau cod de acces necriptate; producătorul documentează capacitățile de accesare la distanță a dispozitivului și îl securizează împotriva accesării neautorizate cel târziu în timpul instalării; producătorul nu prevede parole standard implicite cu codare fixă pentru dispozitiv; vânzătorul documentează posibilitățile

utilizatorului de actualizare a dispozitivelor și indică în mod clar cine poartă responsabilitatea în cazul în care utilizatorul nu actualizează dispozitivul;

(d) obligația producătorului, a distribuitorului și a importatorului dispozitivelor conectate la internet, al componentei de software sau al componentei de firmware de a comunica autorităților competente orice vulnerabilități cunoscute și exploatabile în materie de securitate;

(e) obligația producătorilor de dispozitive conectate la internet, de componente de software sau de componente de firmware de a garanta o reparație sau înlocuire în legătură cu orice nouă vulnerabilitate descoperită în materie de securitate;

(f) obligația producătorilor de dispozitive conectate la internet, de componente de software sau de componente de firmware de a furniza informații despre modul în care dispozitivul primește actualizări de securitate informatică, despre calendarul prevăzut pentru încheierea suportului tehnic în materie de securitate informatică și despre natura procesului de notificare a utilizatorului;

2. Agenția poate propune ca cerințele minime de securitate informatică menționate la alineatul 1 să se aplice dispozitivelor informatice din unul sau mai multe sectoare specifice.

3. Agenția revizuiește și, dacă este necesar, modifică cerințele de securitate informatică menționate la alineatul (1) din doi în doi ani și prezintă aceste modificări Comisiei sub formă de propuneri.

4. Comisia poate decide, prin intermediul unor acte de punere în aplicare și pe baza unei evaluări a impactului, ca cerințele de securitate informatică propuse sau modificate,

menționate la alineatul (1) și alineatul (2), să aibă valabilitate generală în Uniune. Actele de punere în aplicare respective se adoptă în conformitate cu procedura de examinare menționată la articolul 55 alineatul (2).

5. Comisia asigură o publicitate adecvată pentru cerințele de securitate informatică în privința cărora s-a decis că au valabilitate generală, în conformitate cu alineatul (3).

6. Agenția regrupează toate cerințele de securitate informatică propuse și modificările acestora într-un registru și le pune la dispoziția publicului prin mijloace corespunzătoare.

Justificare

Pentru a înlocui, din motive de claritate, litera (c) de la amendamentul 19 din proiectul de aviz. Este important să se asigure reziliența mediului informatic, pentru a combate criminalitatea cibernetică și a proteja drepturile fundamentale ale utilizatorilor informatici. Prin urmare, prezentul regulament ar trebui să prevadă obiective la un nivel ridicat în materie de securitate informatică, care să respecte o referință obligatorie de securitate în interiorul Uniunii.

Amendamentul 64

Propunere de regulament
Articolul 50 – alineatul 6 – litera d

Textul propus de Comisie	*Amendamentul*
(d) cooperează cu alte autorități naționale de supraveghere în materie de certificare sau cu alte autorități publice, inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor și serviciilor TIC cu cerințele prezentului regulament sau ale sistemului european de certificare de securitate ***cibernetică*** specific;	(d) cooperează cu alte autorități naționale de supraveghere în materie de certificare sau cu alte autorități publice, ***cum ar fi autoritățile naționale de supraveghere a protecției datelor,*** inclusiv prin schimbul de informații cu privire la o posibilă neconformitate a produselor și serviciilor TIC cu cerințele prezentului regulament sau ale sistemului european de certificare de securitate ***informatică*** specific;

Justificare

Din avizul AEPD.

PROCEDURA COMISIEI SESIZATE PENTRU AVIZ

Titlu	Regulamentul privind ENISA, „Agenția UE pentru securitate cibernetică”, și de abrogare a Regulamentului (UE) nr. 526/2013 și privind certificarea securității cibernetice a TIC („Cybersecurity Act”)
Referințe	COM(2017)0477 – C8-0310/2017 – 2017/0225(COD)
Comisie competentă Data anunțului în plen	ITRE 23.10.2017
Aviz emis de către Data anunțului în plen	LIBE 23.10.2017
Raportor/Raportoare pentru aviz: Data numirii	Jan Philipp Albrecht 20.11.2017
Examinare în comisie	25.1.2018 8.3.2018
Data adoptării	8.3.2018
Rezultatul votului final	+: 35 –: 2 0: 4
Membri titulari prezenți la votul final	Asim Ademov, Jan Philipp Albrecht, Heinz K. Becker, Caterina Chinnici, Rachida Dati, Cornelia Ernst, Kinga Gál, Sylvie Guillaume, Monika Hohlmeier, Filiz Hyusmenova, Dietmar Köster, Barbara Kudrycka, Monica Macovei, Péter Niedermüller, Ivari Padar, Judith Sargentini, Birgit Sippel, Branislav Škripek, Sergei Stanishev, Traian Ungureanu, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Auke Zijlstra
Membri supleanți prezenți la votul final	Maria Grapini, Sylvia-Yvonne Kaufmann, Jeroen Lenaers, Andrejs Mamikins, Maite Pagazaurtundúa Ruiz, John Procter, Jaromír Štětina, Josep-Maria Terricabras, Axel Voss, Elissavet Vozemberg-Vrionidi
Membri supleanți [articolul 200 alineatul (2)] prezenți la votul final	Andrea Bocskor, Reimer Böge, André Elissen, Ramón Jáuregui Atondo, Julia Reda, Rainer Wieland, Patricija Šulin

VOT FINAL PRIN APEL NOMINAL
ÎN COMISIA COMPETENTĂ

35	+
ALDE	Filiz Hyusmenova, Maite Pagazaurtundúa Ruiz, Cecilia Wikström
ECR	Monica Macovei, John Procter, Branislav Škripek
GUE/NGL	Cornelia Ernst
PPE	Asim Ademov, Heinz K. Becker, Andrea Bocskor, Rachida Dati, Kinga Gál, Barbara Kudrycka, Jeroen Lenaers, Jaromír Štětina, Patricija Šulin, Traian Ungureanu, Elissavet Vozemberg-Vrionidi, Rainer Wieland
S&D	Caterina Chinnici, Maria Grapini, Sylvie Guillaume, Ramón Jáuregui Atondo, Sylvia-Yvonne Kaufmann, Dietmar Köster, Andrejs Mamikins, Péter Niedermüller, Ivari Padar, Birgit Sippel, Sergei Stanishev, Josef Weidenholzer
VERTS/ALE	Jan Philipp Albrecht, Julia Reda, Judith Sargentini, Josep-Maria Terricabras

2	-
ENF	André Elissen, Auke Zijlstra

4	0
EFDD	Kristina Winberg
PPE	Reimer Böge, Monika Hohlmeier, Axel Voss

Legenda simbolurilor utilizate:
+ : pentru
- : împotrivă
0 : abțineri