ROMÂNIA
SENAT

Parlamentul României
Senat

PROIECT

H O T Ă R Â R E
referitoare la
Propunerea de Regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului UE (2019)881 (Regulamentul privind securitatea cibernetică 2) COM(2026) 11 final

În temeiul dispozițiilor art. 67 și art. 148 alin. (2) și alin. (3) din Constituția României, republicată, precum și ale *Protocolului (nr. 2) privind aplicarea principiilor subsidiarității și proporționalității*, anexat Tratatului de la Lisabona de modificare a Tratatului privind Uniunea Europeană și a Tratatului de instituire a Comunității Europene, semnat la Lisabona la 13 decembrie 2007, ratificat prin Legea nr. 13/2008,

În baza raportului Comisiei pentru Afaceri Europene nr. LXII/203/20.05.2026,
Senatul adoptă prezenta h o t ă r â r e.

Art. 1.- Senatul României constată că Propunerea de Regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului UE (2019)881(Regulamentul privind securitatea cibernetică 2) - COM(2026) 11 final - respectă principiul subsidiarității și principiul proporționalității.

Art. 2.- Senatul României consideră că:
a) inițiativa este una binevenită având în vedere creșterea amenințărilor cibernetice, al elementelor de extraneitate pe care le implică multe dintre aceste amenințări, precum și al fragmentării cadrelor, mijloacelor și modalităților de gestionare a acestora între statele membre;
b) consolidarea cadrului de cooperare în materie la nivel european, inclusiv prin activitățile și rolul ENISA, prin simplificarea Cadrului european de certificare și prin măsuri vizând creșterea securității lanțurilor de aprovizionare în domeniul TIC, reprezintă un deziderat deopotrivă util și oportun în măsura în care va conduce efectiv la o eficientizare a prevenirii și combaterii riscurilor și amenințărilor cibernetice, facilitând cooperarea între Statele Membre ca deținătoare ale competenței și responsabilității primordiale în acest domeniu, în complementaritate cu acțiunile instituțiilor și structurilor comunitare, cu respectarea mandatului fiecăreia dintre părțile implicate și a principiului subsidiarității, fiind important ca forma finală a CSA2 să reflecte toate aceste obiective.

Art. 3. - Prezenta hotărâre se publică în Monitorul Oficial al României, Partea I.

Această hotărâre a fost adoptată de Senat în ședința din ... mai 2026, cu respectarea prevederilor art. 76 alin(2) din Constituția României, republicată.

Președintele Senatului
Mircea ABRUDEAN

București, ... mai 2026
Nr. .

XX V4/750/21.05.2026

Parlamentul României
Senat

Comisia pentru Afaceri Europene

RAPORT
la
Propunerea de Regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului UE (2019)881 (Regulamentul privind securitatea cibernetică 2) COM (2026) 11 final

Comisia pentru afaceri europene a fost sesizată, în temeiul Protocolului nr. 2, privind aplicarea principiilor subsidiarității și proporționalității, anexat Tratatului de la Lisabona de modificare a Tratatului privind Uniunea Europeană și a Tratatului de instituire a Comunității Europene, semnat la Lisabona la 13 decembrie 2007, ratificat prin Legea nr. 13/2008, în vederea examinării Propunerii de Regulament al Parlamentului European și al Consiliului privind Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA), cadrul european de certificare a securității cibernetice și securitatea lanțului de aprovizionare TIC și de abrogare a Regulamentului UE (2019)881 (Regulamentul privind securitatea cibernetică 2) - **COM (2026) 11 final.**

Ședința comisiei a avut loc în data de 19 mai, în format fizic, în conformitate cu art. 63 din Regulamentul Senatului, cu modificările și completările ulterioare. La dezbateri a participat un reprezentant din partea Ministerului Afacerilor Externe.

A fost analizat punctul de vedere al Ministerului Afacerilor Externe și al Serviciului pentru Afaceri Europene.

Comisiile permanente sesizate, respectiv Comisia juridică, de numiri, disciplină, imunități și validări și Comisia pentru comunicații, tehnologia informației și inteligență artificială nu au transmis observații.

Descrierea documentului european:

Propunerea COM(2026)11 a fost elaborată de Comisia Europeană într-un context marcat de evoluția amenințărilor la adresa securității cibernetice, de la adoptarea Regulamentului privind securitatea cibernetică în 2019, într-o realitate geopolitică din ce în ce mai complexă. Atacurile cibernetice s-au intensificat și au devenit mai sofisticate, vizând infrastructura critică, întreprinderile și publicul larg, în centrul acestora aflându-se activitatea de tip ransomware. Tehnologiile emergente, cum ar fi inteligența artificială (IA) și informatica cuantică, remodelează instrumentele de apărare și tacticile adversarilor. Atât Strategia europeană privind o Uniune a pregătirii, cât și Strategia europeană de securitate internă (ProtectEU) au plasat securitatea cibernetică în centrul agendei Uniunii privind reziliența. Aceste strategii recunosc că amenințările persistente la adresa securității cibernetice nu sunt doar provocări tehnice, ci și riscuri strategice pentru democrația, economia și modul european de viață.

În acest context, există patru probleme principale pe care prezenta propunere urmărește să le abordeze: (i) neconcordanța dintre cadrul de politică al Uniunii în materie de securitate cibernetică și nevoile părților interesate într-un peisaj al amenințărilor din ce în ce mai ostil; (ii) stagnarea punerii în aplicare a Cadrului european de certificare a securității cibernetice (ECCF); (iii) complexitatea și diversitatea politicilor legate de securitatea cibernetică care au un impact asupra posturii de securitate cibernetică a Uniunii și (iv) creșterea riscurilor la adresa securității lanțurilor de aprovizionare în materia tehnologiei informației și comunicațiilor (TIC).

Pe baza principalelor probleme identificate, propunerea urmărește două obiective generale, anume de a spori capacitățile și reziliența în materie de securitate cibernetică și de a preveni fragmentarea pe piața unică prin: contribuția la consolidarea guvernanței Uniunii în materie de securitate cibernetică și contribuția la asigurarea faptului că instituțiile, autoritățile și alte părți interesate relevante sunt mai bine pregătite pentru a preveni, a detecta amenințările la adresa securității cibernetice și a răspunde la acestea într-un mod coordonat și eficace; sprijinirea dezvoltării, a punerii în aplicare și a adoptării unor instrumente comune ale Uniunii în materie de securitate cibernetică, cum ar fi sistemele de certificare, și furnizarea unor cadre armonizate care să consolideze încrederea și interoperabilitatea în toate statele membre.

Propunerea de nou Regulament privind securitatea cibernetică (CSA2) se sprijină pe trei piloni: securitatea lanțurilor de aprovizionare în domeniul tehnologiilor informației și comunicațiilor (TIC) în UE; simplificarea și consolidarea Cadrului european de certificare a securității cibernetice; consolidarea mandatului ENISA pentru a spori reziliența Europei în materie de securitate cibernetică.
COM a lansat această propunere ca parte a unui nou pachet de măsuri legislative care include și amendarea Directivei NIS2, în contextul în care Europa se confruntă cu atacuri hibride din ce în ce mai sofisticate, cu o dimensiune cibernetică sistematică, care pot perturba sectoare critice precum energia, transporturile, sănătatea, sistemul bancar și apa. CSA2 va permite UE să abordeze aceste riscuri de securitate, consolidându-și în același timp securitatea cibernetică. Costurile globale ale criminalității cibernetice au depășit 9 trilioane de euro în 2025, iar ransomware este cea mai mare amenințare cibernetică, fiind estimate atacuri la fiecare 2 secunde, până în 2031. Atacurile cibernetice asupra lanțurilor de aprovizionare se află printre primele șapte amenințări cibernetice.

Propunerea clarifică rolul ENISA și îi încredințează sarcini concrete de sprijinire a părților sale interesate, în primul rând a statelor membre, în special în ceea ce privește sprijinul pentru punerea în aplicare a politicii și a legislației Uniunii, cooperarea operațională, consolidarea capacităților, certificarea și standardizarea în materie de securitate cibernetică și îmbunătățirea forței de muncă din domeniul securității cibernetice și a mobilității acesteia în întreaga Uniune. Propunerea urmărește, de asemenea, creșterea eficienței și a eficacității Cadrului european de certificare a securității cibernetice (ECCF) pentru a îmbunătăți nivelul de securitate cibernetică în Uniune și pentru a le permite clienților să facă alegeri în cunoștință de cauză atunci când achiziționează produse, servicii, procese și servicii de securitate gestionate în cadrul pieței interne. În plus, în tandem cu propunerea de directivă de introducere a unor modificări specifice ale Directivei NIS 2, prezenta propunere urmărește să faciliteze respectarea obligațiilor în materie de securitate cibernetică și să deblocheze resurse pentru a consolida pregătirea operațională în materie de securitate cibernetică a entităților din sectoarele critice ale Uniunii. În cele din urmă, propunerea abordează necesitatea de a spori reziliența economiei Uniunii și a lanțului de aprovizionare TIC pentru a-și promova propria securitate și competitivitate.

În urma examinării, membrii comisiei:

- **constată că:**

- Temeiul juridic al propunerii îl constituie articolul 114 din Tratatul privind funcționarea Uniunii Europene (TFUE). Articolul 114 din TFUE prevede adoptarea de măsuri pentru a asigura instituirea și funcționarea pieței interne. Regulamentul (UE) 2019/881 privind ENISA și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor, cunoscut sub denumirea de CSA18, a fost adoptat inițial în temeiul acestei dispoziții. În

domeniul securității cibernetice a securității lanțurilor de aprovizionare TIC, fragmentarea cadrelor naționale care abordează factorii de risc non-tehnic are efecte negative asupra funcționării pieței interne, deoarece divergențele dintre abordările naționale ar putea conduce, în cele din urmă, la o vulnerabilitate mai mare a unor state membre, cu potențiale efecte de propagare în întreaga Uniune, afectând reziliența generală și, de asemenea, credibilitatea. Având în vedere caracterul evolutiv al amenințărilor la adresa securității cibernetice și interdependența tot mai mare a sistemelor digitale ale statelor membre, articolul 114 din TFUE rămâne temeiul juridic justificat pentru revizuirea Regulamentului privind securitatea cibernetică. Regulamentul propus reflectă cele mai recente evoluții din peisajul legislativ al securității cibernetice, în special având în vedere responsabilitățile tot mai mari ale ENISA și extinderea domeniului de aplicare al certificărilor și al gestionării riscurilor;

- prezenta propunere de regulament respectă principiul subsidiarității și principiul proporționalității, conform Protocolul nr. 2 privind aplicarea principiilor subsidiarității și proporționalității, art. 5 din Tratatul privind Uniunea Europeană.

• **consideră că:**

- inițiativa este una binevenită având în vedere creșterea amenințărilor cibernetice, al elementelor de extraneitate pe care le implică multe dintre aceste amenințări, precum și al fragmentării cadrelor, mijloacelor și modalităților de gestionare a acestora între statele membre;
- consolidarea cadrului de cooperare în materie la nivel european, inclusiv prin activitățile și rolul ENISA, prin simplificarea Cadrului european de certificare și prin măsuri vizând creșterea securității lanțurilor de aprovizionare în domeniul TIC, reprezintă un deziderat deopotrivă util și oportun în măsura în care va conduce efectiv la o eficientizare a prevenirii și combaterii riscurilor și amenințărilor cibernetice, facilitând cooperarea între Statele Membre ca

deținătoare ale competenței și responsabilității primordiale în acest domeniu, în complementaritate cu acțiunile instituțiilor și structurilor comunitare, cu respectarea mandatului fiecăreia dintre părțile implicate și a principiului subsidiarității, fiind important ca forma finală a CSA2 să reflecte toate aceste obiective.

În urma dezbaterii, membrii Comisiei pentru afaceri europene au hotărât, cu majoritatea voturilor membrilor prezenți, formularea unui Raport **la COM (2026) 11 final.**

Comisia pentru afaceri europene supune Plenului Senatului, spre dezbatere și adoptare, proiectul de hotărâre privind adoptarea prezentului Raport, în conformitate cu art. 34 din Anexa la Regulamentul Senatului aprobat prin Hotărârea Senatului nr. 28/2005, cu modificările și completările ulterioare.

PREȘEDINTE,	**SECRETAR,**
Senator Rodica CUȘNIR	**Senator DÎRLĂU Andrei-Emil**

Întocmit: Diana-Denisa Mocan, consilier parlamentar, CAE