C/2026/3549

22.7.2026

Avizul Comitetului Economic și Social European

a) 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 din 2)

[COM(2026) 11 final – 2026/11 (COD)]

și

b) Propunerea de directivă a Parlamentului European și a Consiliului de modificare a Directivei (UE) 2022/2555 în ceea ce privește măsurile de simplificare și alinierea la (Propunerea de regulament privind securitatea cibernetică 2)

[COM(2026) 13 final – 2026/12 (COD)]

(C/2026/3549)

Raportor: **Miroslav HAJNOŠ**

Consilieră	Pavlina PAVLOVA (pentru raportor)
Procedura legislativă	EU Law Tracker EU Law Tracker
Sesizări	(a) Parlamentul European, 5.2.2026 Consiliul Uniunii Europene, 23.3.2026 (b) Parlamentul European, 6.2.2026 Consiliul Uniunii Europene, 23.3.2026
Temei juridic	Articolul 114 din Tratatul privind funcționarea Uniunii Europene
Documentele Comisiei Europene	COM(2026) 11 final – 2026/11 (COD) COM(2026) 13 final – 2026/12 (COD) Rezumat
Obiectivele de dezvoltare durabilă (ODD) relevante	ODD 8 – Condiții de muncă decente și creștere economică ODD 9 – Industrie, inovare și infrastructură ODD 12 – Consum și producție responsabile ODD 17 – Parteneriate pentru obiective
Secțiunea competentă	Secțiunea pentru piața unică, producție și consum
Data adoptării în secțiune	15.4.2026
Data adoptării în sesiunea plenară	29.4.2026
Sesiunea plenară nr.	605
Rezultatul votului (pentru/împotrivă/abțineri)	193/0/0

1. RECOMANDĂRI

COMITETUL ECONOMIC ȘI SOCIAL EUROPEAN (CESE):

1.1. **salută** inițiativa Comisiei de a revizui Regulamentul privind securitatea cibernetică (CSA) și de a introduce modificări la Directiva NIS 2 și **sprijină** obiectivele pe care și le propune acest pachet, și anume de a consolida reziliența UE la amenințări cibernetice, de a îmbunătăți claritatea juridică și coordonarea instituțională, de a simplifica cadrele de

conformitate și de a reduce sarcina administrativă asupra entităților reglementate, menținând în același timp competitivitatea și capacitatea de inovare a pieței europene; **subliniază** că securitatea cibernetică și securitatea lanțului de aprovizionare din domeniul TIC trebuie tratate ca aspecte legate de securitatea economică și de reziliența geopolitică, și nu doar ca provocări de natură tehnică sau normativă;

1.2. **subliniază** că mandatul Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) contribuie în mod semnificativ la consolidarea rezilienței cibernetice a Uniunii. Propunerea de clarificare a rolului ENISA ar trebui să vizeze, înainte de toate, consolidarea mandatului agenției și preluarea noilor sarcini care decurg din cerințele cadrului de reglementare extins al Uniunii;

1.3. **avertizează** că, în cazul în care propunerea extinde responsabilitățile agenției, trebuie asigurată o creștere corespunzătoare a resurselor și a personalului specializat pentru a sprijini punerea în aplicare eficientă a acestor responsabilități. Orice sarcini suplimentare atribuite ENISA ar trebui să fie condiționate în mod explicit de stabilirea unui plan obligatoriu privind personalul;

1.4. **subliniază** că reziliența în materie de securitate cibernetică depinde de competențele, formarea și capacitatea organizatorică a personalului. Rolul propus pentru ENISA în ceea ce privește cadrul european de competențe în materie de securitate cibernetică și autorizațiile pentru atestatele de competențe, care este transferabil între statele membre, este un pas binevenit, cu condiția ca sarcinile instituțiilor și autorităților relevante să fie clar definite, să se consolideze reciproc și să nu se suprapună cu certificarea existentă;

1.5. **subliniază** că securitatea cibernetică este, de asemenea, o componentă fundamentală a rezilienței democratice în lumina riscurilor din ce în ce mai mari de amenințări cibernetice care vizează procesele democratice, inclusiv alegerile, prin campanii de dezinformare, manipularea infrastructurii digitale și ingerințe străine, și **solicită** o coordonare consolidată la nivelul UE pentru a proteja sistemele electorale, inclusiv pentru monitorizarea riscurilor, schimbul de informații și sprijinul pentru cadrele statelor membre în materie de securitate a alegerilor;

1.6. **sprijină** dezvoltarea, punerea în aplicare și adoptarea sistemelor de certificare ca mijloc de consolidare a încrederii la nivelul întregii piețe unice, subliniind – în același timp – angajamentul său de lungă durată față de un cadru armonizat de securitate cibernetică al Uniunii, bazat pe securitate juridică, transparență și proporționalitate, și față de promovarea coerenței și utilizabilității în detrimentul acumulării de reglementări;

1.7. **subliniază** că certificarea trebuie să funcționeze ca un factor real de asigurare a conformității, în special pentru operatorii transfrontalieri și multinaționali care fac obiectul suprapunerilor cauzate de obligațiile în materie de securitate cibernetică. Cadrul de certificare revizuit trebuie să includă dispoziții solide privind întreținerea sistemelor, transparența, claritatea guvernanței și protecția consumatorilor;

1.8. **remarcă** propunerea de a se institui un cadru structurat la nivelul UE pentru identificarea activelor TIC esențiale și pentru elaborarea unor măsuri proporționale de atenuare a riscurilor, printre care se numără, în cazuri justificate, măsuri privind furnizorii cu risc ridicat, în concordanță cu reducerea riscurilor la nivelul lanțurilor de aprovizionare TIC pentru a diminua dependențele de furnizori cu sediul în țări care suscită preocupări în materie de securitate cibernetică sau controlați de astfel de țări; **subliniază** că orice măsură privind securitatea lanțurilor de aprovizionare TIC trebuie să se bazeze pe cerințe clare, previzibile și transparente;

1.9. **solicită** să se ia pe deplin în considerare impactul economic și impactul în aval al intervenției propuse asupra lanțului de aprovizionare, inclusiv fezabilitatea, disponibilitatea alternativelor, constrângerile legate de ciclul de viață, riscul de perturbare operațională, costurile operaționale, efectele asupra prețurilor și a calității serviciilor pentru utilizatorii finali, impactul asupra pieței forței de muncă și inovarea;

1.10. **subliniază** necesitatea de a garanta că obligațiile prevăzute în cadrul revizuit sunt aplicate în mod proporțional și nu conduc la transfer indirect sau nejustificat de sarcini de asigurare a conformității către actori din afara domeniului lor de aplicare, că evită „dumpingul” în materie de conformitate și că rămân consecvente cu obiectivele de simplificare, claritate juridică și sensibilitate la nevoile IMM-urilor, care stau la baza agendei de simplificare din Regulamentul privind reziliența cibernetică și din Directiva NIS 2;

1.11. **solicită** implicarea sistematică a partenerilor sociali, a IMM-urilor, a organizațiilor de consumatori, a organizațiilor relevante ale societății civile, a mediului academic și a grupurilor de reflecție, în dezvoltarea, punerea în aplicare și monitorizarea sistemelor, pentru a garanta că acest cadru este echitabil din punct de vedere operațional, inteligibil din punct de vedere democratic și fezabil din punctul de vedere al punerii în practică și că sprijină suveranitatea tehnologică și avantajul competitiv ale Uniunii.

2. **NOTE EXPLICATIVE**

Argument în sprijinul recomandării 1.1

2.1. Regulamentul privind securitatea cibernetică [Regulamentul (UE) 2019/881] ([1]) este în curs de revizuire în conformitate cu cerința privind o evaluare cuprinzătoare a ENISA și a cadrului european de certificare în domeniul securității cibernetice (ECCF), având în vedere complexitatea și diversitatea crescândă a politicilor legate de securitatea cibernetică, stagnarea punerii în aplicare a ECCF și riscurile tot mai mari asociate lanțului de aprovizionare din domeniul TIC.

Argumente în sprijinul recomandării 1.2

2.2. Revizuirea extinde și reorganizează sarcinile ENISA. CESE consideră că prioritatea propunerii ar trebui să constea în consolidarea și raționalizarea mandatului ENISA și absorbția noilor sarcini în strictă conformitate cu Regulamentul privind reziliența cibernetică și cu Directiva NIS 2.

2.3. **CESE sprijină instituirea unui punct unic de intrare pentru raportarea incidentelor – în scopul de a raționaliza obligațiile paralele de raportare în temeiul Directivei NIS 2, al Regulamentului privind DORA și al normelor sectoriale, cu modele de raportare interoperabile și standardizate și cu definirea clară a termenelor de raportare și a cerințelor privind conținutul rapoartelor. O astfel de simplificare trebuie să fie operațională, nu doar formală: un raport cuprinzător ar trebui să fie suficient pentru toate regimurile de reglementare relevante.**

Argumente în sprijinul recomandării 1.3

2.4. Este posibil ca bugetul propus să nu fie suficient pentru a acoperi toate sarcinile. Orice extindere sau reorganizare a sarcinilor trebuie să fie însoțită de resurse financiare adecvate și durabile și de personal specializat, pentru a evita crearea unui mandat nefinanțat în mod corespunzător, ceea ce ar putea submina eficacitatea ENISA și capacitatea sa de a-și demonstra valoarea adăugată ([2]). CESE ar saluta, de asemenea, includerea resurselor suplimentare și a acordurilor de contribuție în bugetul oficial, precum și reflectarea lor în cadrul acestuia.

2.5. Propunerea precizează că bugetul agenției ar urma să fie acoperit parțial de mecanisme de autofinanțare prin taxe percepute pentru sprijinirea întreținerii sistemelor europene de certificare a securității cibernetice și pentru eliberarea autorizațiilor de atestare a competențelor. Această estimare se bazează pe perspectivele de adoptare a certificării în întreaga Uniune și este posibil să nu reflecte pe deplin adoptarea efectivă în practică.

([1]) Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (JO L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([2]) În avizul său pe tema „Legea privind securitatea cibernetică” (JO C 227, 28.6.2018, p. 86), CESE considera că noul mandat permanent al ENISA va contribui semnificativ la consolidarea rezilienței sistemelor europene. Această direcție a fost recunoscută și în avizul CESE pe tema „Regulamentul privind reziliența cibernetică” (JO C 100, 16.3.2023, p. 101), în care se afirmă că va fi important ca ENISA să dispună de resursele necesare pentru a îndeplini cu eficacitate și promptitudine sarcinile importante și sensibile care i-au fost încredințate.

2.6. **Un plan obligatoriu privind personalul ar trebui să abordeze dezvoltarea competențelor, nevoile de formare și realocarea volumului de muncă, fiind însoțit de măsuri adecvate pentru a preveni orele suplimentare excesive și epuizarea profesională, precum și de garanții privind capacitatea minimă, care să asigure că rezultatele esențiale pot fi în continuare realizate în mod eficace.** Numirea planificată a doi ofițeri de legătură pentru fiecare stat membru s-ar putea dovedi nerealistă, în special pentru statele membre mai mici și cu resurse limitate.

Argumente în sprijinul recomandării 1.4

2.7. CESE reiterează că reziliența în materie de securitate cibernetică depinde de competențele, formarea și capacitatea organizatorică a personalului. Sistemele propuse de atestare a competențelor pot contribui la acest obiectiv, cu condiția ca acestea să rămână practice, proporționale și accesibile.

2.8. Îmbunătățirea alfabetizării în materie de securitate cibernetică în rândul publicului larg este o completare necesară a dezvoltării competențelor profesionale și ar trebui încurajată pe deplin în întreaga UE. O populație mai bine informată cu privire la riscurile cibernetice, dezinformare și un comportament digital sigur contribuie în mod direct la reducerea vulnerabilităților la nivel societal. O astfel de conștientizare este deosebit de importantă într-o economie din ce în ce mai digitalizată, în care factorul uman rămâne un vector principal al incidentelor de securitate cibernetică.

Argumente în sprijinul recomandării 1.5

2.9. Amenințările cibernetice vizează din ce în ce mai mult instituțiile și procesele democratice, inclusiv alegerile, prin tactici hibride, cum ar fi dezinformarea, atacurile cibernetice asupra infrastructurii electorale și manipularea discursului public. Aceste riscuri au implicații sistemice pentru încrederea în instituțiile publice și pentru funcționarea sistemelor democratice. Prin urmare, CESE consideră că este esențial să se consolideze coordonarea la nivelul UE și să se sprijine statele membre în protejarea proceselor electorale, respectând în același timp competențele naționale. Consolidarea atât a rezilienței instituționale, cât și a sensibilizării publicului este o componentă-cheie a protejării democrației în era digitală.

Argumente în sprijinul recomandării 1.6

2.10. CESE susține sistemele de certificare, inclusiv certificarea posturii de securitate cibernetică a entităților, ca mijloc de simplificare a conformității în practică, de consolidare a securității cibernetice și de consolidare a încrederii în cadrul pieței unice. CESE sprijină alinierea la Directiva NIS 2 prin modificările specifice propuse în directiva care o însoțește, având scopul de a reduce complexitatea reglementărilor, de a îmbunătăți coerența în întreaga legislație a Uniunii în materie de securitate cibernetică, de a facilita conformitatea pentru entitățile reglementate și de a consolida sprijinul pentru supravegherea transfrontalieră.

Argumente în sprijinul recomandării 1.7

2.11. Certificarea ar trebui să reducă auditurile și procedurile de conformitate. Acest lucru necesită sisteme proporționale, bazate pe riscuri, aliniate la standardele internaționale (ISO/IEC) printr-o recunoaștere reciprocă semnificativă și abordări interoperabile, menținând deschiderea pieței globale și permițând produselor și serviciilor certificate de UE să concureze în mod eficient.

2.12. Termenele previzibile, procedurile clare și costurile proporționale sunt esențiale pentru a garanta că IMM-urile și furnizorii de servicii mai mici nu sunt dezavantajați. O abordare de tip „certificare unică, valabilă pretutindeni” trebuie să devină standardul operațional.

2.13. ENISA ar trebui să asigure o gestionare eficientă a sistemelor europene de certificare în domeniul securității cibernetice și o guvernanță clară, ținând seama de lecțiile desprinse din cadrul existent, a cărui eficacitate a fost compromisă de adoptarea sa limitată, procedurile sale îndelungate și lipsa sa de claritate operațională. Pentru a consolida încrederea și adoptarea pe piață, ENISA va pune la dispoziția publicului informații clare și comparabile privind nivelurile de securitate cibernetică ale produselor și serviciilor certificate.

Argumente în sprijinul recomandării 1.8

2.14. Propunerea abordează necesitatea de a spori reziliența la nivelul economiei Uniunii și al lanțului de aprovizionare TIC pentru a promova securitatea și competitivitatea în UE. CESE salută inițiativa Comisiei ([3]) de a da curs opiniei potrivit căreia UE nu ar trebui să achiziționeze sau să integreze componente TIC critice din țări implicate activ în subminarea intereselor europene în materie de securitate.

2.15. În cazul în care măsurile de atenuare a riscurilor duc la restricționarea sau la eliminarea treptată a furnizorilor considerați a prezenta riscuri ridicate în materie de securitate cibernetică, planificarea tranziției către alți furnizori este esențială. Planurile de tranziție ar trebui să includă inventare ale activelor, cartografierea dependențelor, termene realiste de înlocuire și garanții care să asigure continuitatea serviciilor. Aceste condiții sunt necesare pentru a se asigura că UE poate consolida securitatea lanțului de aprovizionare, evitând în același timp perturbările operaționale și șocurile costurilor pentru operatori și utilizatorii finali.

Argumente în sprijinul recomandării 1.9

2.16. Evaluările privind impactul economic trebuie să ia pe deplin în considerare aplicarea practică a cadrului, în special în cazurile în care se preconizează că măsurile de eliminare treptată sau alte măsuri restrictive vor fi luate împotriva unor furnizori esențiali și a unor entități critice. Controalele la nivelul lanțului de aprovizionare TIC pot avea efecte operaționale și economice semnificative și este necesară o evaluare sistematică a acestor efecte pentru a susține proporționalitatea, securitatea juridică și acceptarea socială. Măsurile propuse riscă să limiteze libertatea contractuală a societăților comerciale și pot avea un impact substanțial asupra furnizorilor de telecomunicații, a centrelor de cloud și de date și a oricărei societăți care utilizează tehnologii TIC și intră sub incidența Directivei NIS 2. Prin urmare, societățile se pot confrunta cu costuri mai mari legate de schimbarea echipamentelor și a furnizorilor, o situație care poate fi deosebit de dificilă pentru IMM-uri și poate reduce posibilitățile de alegere prin excluderea sau restricționarea anumitor furnizori.

2.17. CESE solicită recunoașterea faptului că reziliența în materie de securitate cibernetică depinde de dezvoltarea forței de muncă și de condițiile de muncă sigure pentru specialiștii în domeniul cibernetic, inclusiv pentru cei din sectoarele infrastructurilor critice, acolo unde acest lucru este relevant pentru reziliența operațională în materie de securitate cibernetică.

2.18. Evaluările impactului economic și social ar trebui să includă indicatori relevanți privind piața muncii. Printre acești indicatori ar trebui să se numere cerințele în materie de recalificare și perfecționare, volumul acțiunilor de formare și costurile asociate, implicațiile volumului de muncă asupra unor funcții-cheie precum IT, securitate cibernetică, achiziții publice și conformitate, precum și eventualele necesități de restructurare și măsurile de tranziție menite să prevină efectele relocărilor subite.

Argumente în sprijinul recomandării 1.10

2.19. Având în vedere potențialul impact al propunerii asupra opțiunilor în materie de achiziții publice, procesul necesită criterii clare, obiective și revizuibile, proceduri previzibile și o justificare transparentă pentru orice măsură adoptată. Normele care vizează furnizorii trebuie să se bazeze strict pe riscuri și dovezi, pentru a proteja continuitatea serviciilor și a asigura previzibilitatea investițiilor; în caz contrar, acestea riscă să genereze incertitudine, costuri suplimentare, perturbări pe piața Uniunii și transferul obligațiilor către nivelurile inferioare ale lanțului valoric, în special către furnizorii și subcontractanții mai mici. Entitățile nu ar trebui să se confrunte cu obligații de conformitate disproporționate față de dimensiunea și capacitatea lor.

Argumente în sprijinul recomandării 1.11

2.20. Măsurile de securitate cibernetică cu implicații semnificative pentru lanțurile de aprovizionare și pentru achizițiile publice și private trebuie elaborate și puse în aplicare prin implicarea structurată a părților interesate în evaluarea impactului economic și social, cu scopul de a stabili care dintre măsurile bazate pe riscuri sunt necesare, adecvate, solide juridicește și fezabile operațional. Consultarea cu partenerii sociali ar trebui să constituie un element structural al unor astfel de evaluări, mai degrabă decât să fie tratată doar ca o bună practică opțională.

([3]) JO C 227, 28.6.2018, p. 86.

3. **PROPUNERI DE AMENDAMENTE LA PROPUNEREA LEGISLATIVĂ A COMISIEI EUROPENE**

Amendamentul 1

legat de recomandările 1.4 și 1.5

Textul propus de Comisia Europeană	Amendamentul CESE
	Articolul 7 bis ***Sensibilizarea cu privire la securitatea cibernetică și reziliența democratică*** ***1. ENISA sprijină statele membre și instituțiile Uniunii în consolidarea sensibilizării cu privire la securitatea cibernetică și a rezilienței proceselor democratice, inclusiv a alegerilor, la amenințările cibernetice și la ingerințele hibride.*** ***2. ENISA contribuie la elaborarea unor inițiative la nivelul Uniunii menite să îmbunătățească cunoștințele publicului larg în materie de securitate cibernetică, inclusiv conștientizarea dezinformării, comportamentul digital sigur și riscurile legate de procesele democratice.***

Expunere de motive

Amenințările cibernetice vizează din ce în ce mai mult instituțiile democratice și procesele electorale. Consolidarea atât a garanțiilor instituționale, cât și a alfabetizării digitale a cetățenilor este esențială pentru a asigura reziliența democratică și încrederea în mediul digital.

Amendamentul 2

legat de recomandările 1.8, 1.9, 1.10 și 1.11

Textul propus de Comisia Europeană	Amendamentul CESE
	Articolul 103 bis ***Planificarea tranziției și punerea în aplicare proporțională*** ***1. În cazul în care măsurile de atenuare prevăzute la articolul 103 includ restricții, eliminări treptate sau obligații de înlocuire, Comisia se asigură că aceste măsuri sunt însoțite de planuri de tranziție structurate obligatorii, în plus față de perioadele de tranziție prevăzute la articolul 103 alineatul (1).*** ***2. Planurile de tranziție includ cel puțin: (a) inventarele activelor și cartografierea dependenței componentelor TIC afectate; (b) termene realiste pentru înlocuire sau atenuare; (c) garanții care să asigure continuitatea serviciilor în sectoarele cu o importanță critică ridicată.***

Textul propus de Comisia Europeană	Amendamentul CESE
	3. Măsurile luate în temeiul prezentului titlu evită perturbările operaționale nejustificate, nu impun costuri disproporționate în raport cu dimensiunea entității și cu expunerea la risc și previn transferul indirect al obligațiilor de conformitate către entități care nu intră în domeniul de aplicare al prezentului regulament. ***4. Comisia asigură implicarea sistematică a industriei, a IMM-urilor, a partenerilor sociali și a societății civile în pregătirea și evaluarea măsurilor.***

Expunere de motive

Prezentul amendament solicită planuri de tranziție structurate și măsuri de protecție împotriva efectelor în cascadă, asigurându-se că măsurile privind lanțul de aprovizionare sunt proporționale și nu transferă sarcinile de asigurare a conformității asupra unor actori din afara domeniului de aplicare al regulamentului.

Bruxelles, 29 aprilie 2026.

Președintele
Comitetului Economic și Social European
Séamus BOLAND