



Biroul permanent al Senatului

L593 / 27.10.2026

Parlamentul României *Senat*

Comisia pentru comunicații, tehnologia informației și inteligență artificială
Nr. LXIX/279/27.10.2026

RAPORT

asupra **Propunerii legislative pentru completarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil**
L593/2026

În conformitate cu prevederile art. 70 din Regulamentul Senatului, republicat, în vigoare, Comisia pentru comunicații, tehnologia informației și inteligență artificială, prin adresa nr. **L593/2026**, a fost sesizată de Biroul permanent al Senatului în vederea dezbaterii și elaborării **raportului** asupra **Propunerii legislative pentru completarea Ordonanței de urgență a Guvernului nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil**, având ca inițiatori: *Cadar Răzvan-Olimpiu - deputat PNL; Cozma Adrian-Felician - deputat PNL; Crușoveanu Marian - deputat PNL; Fechet Mircea - deputat PNL; Huțucă Bogdan-Iulian - deputat PNL; Oprea Octavian - deputat PNL; Pandea Ciprian - deputat PNL; Teslariu Andrei-Ionuț - deputat PNL; Țiplea Dumitru - deputat PNL.*

Propunerea legislativă are ca obiect de reglementare completarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil,

aprobată cu modificări și completări prin Legea nr. 124/2025, cu modificările și completările ulterioare, în sensul instituirii unor programe de identificare și raportare recompensată a vulnerabilităților rețelelor și sistemelor informatice din spațiul cibernetic național civil.

Potrivit Expunerii de motive „*propunerea legislativă conferă Directoratului Național pentru Securitate Cibernetică (DNSC) dreptul de a iniția, organiza și administra programe de identificare și raportare recompensată a vulnerabilităților pentru rețelele și sistemele informatice deținute, administrate ori utilizate de autorități, instituții publice și alte entități de drept public.(...) Totodată, se creează temeiul necesar pentru includerea în bugetul DNSC a cheltuielilor privind organizarea programelor și plata recompenselor, în limita creditelor bugetare aprobate cu această destinație în bugetul de venituri și cheltuieli al DNSC*”.

Consiliul Legislativ a avizat negativ propunerea legislativă, conform avizului nr. 831 din 01 octombrie 2026. Conform avizului adoptat, propunerea legislativă prezintă deficiențe de claritate și predictibilitate privind autorizarea testării sistemelor informatice, nu delimitează suficient mecanismul propus de procedurile existente de divulgare coordonată a vulnerabilităților, nu stabilește clar limitele testării și consecințele depășirii acestora și conține necorelări între expunerea de motive și textul normativ, inclusiv în ceea ce privește măsurile de protecție și normele de aplicare; totodată, nu este fundamentat suficient impactul financiar și nu este identificată sursa de finanțare a recompenselor.

Consiliul Economic și Social (CES) a avizat nefavorabil inițiativa legislativă, conform avizului cu nr. 6270 din 23 septembrie 2026. Propunerea legislativă nu stabilește suficient de clar și predictibil condițiile de funcționare a programelor de identificare și raportare a vulnerabilităților, criteriile de validare și limitele recompenselor, nu fundamentează impactul financiar și nu precizează sursa de finanțare a cheltuielilor bugetare, inclusiv a celor administrative; totodată, CES consideră că activitățile ar trebui desfășurate cu personalul propriu al DNSC, pentru a evita riscurile de securitate asociate externalizării, semnalând și posibile probleme de conformitate cu art. 138 alin. (5) din Constituție.

Consiliul Concurenței, conform avizului nr. 15284/13.10.2026, apreciază că propunerea legislativă privind instituirea unor programe de tip Bug Bounty, gestionate și finanțate de DNSC, nu contravine prevederilor legislației naționale și europene în domeniul concurenței și al ajutorului de stat.

Conform opiniei nr. 66/06.10.2026 de la **Consiliul Fiscal**, propunerea legislativă nu întrunește cerințele prevăzute la art. 15 alin. (1) din Legea nr. 69/2010 a responsabilității fiscal-bugetare republicate (LRFB), care reglementează propunerile de acte normative care conduc la majorarea cheltuielilor bugetare.

Directoratul Național de Securitate Cibernetică susține adoptarea inițiativei legislative, conform avizului nr. D1764/28.09.2026.

Ministerul Finanțelor nu susține adoptarea inițiativei legislative, întrucât aceasta ar genera presiuni suplimentare asupra deficitului bugetar, conform avizului nr. 183460-10/15.10.2026.

Comisia pentru buget, finanțe, activitate bancară și piață de capital a avizat **favorabil** propunerea legislativă, cu majoritate de voturi.

În cadrul dezbaterilor au fost formulate amendamente de către domnul senator Glad-Aurel Varga și domnul deputat Octavian Oprea, care, supuse votului, au fost **admise** cu unanimitate de voturi și se regăsesc în anexa care face parte integrantă din prezentul raport comun.

În ședința din data de 27.10.2026, membrii Comisiei pentru comunicații, tehnologia informației și inteligență artificială au examinat propunerea legislativă, avizele și punctele de vedere primite și au hotărât, cu **unanimitate de voturi**, să adopte un **raport de admitere, cu amendamente admise**.

Comisia pentru comunicații, tehnologia informației și inteligență artificială supune spre dezbateră și adoptare, Plenului Senatului, **raportul de admitere, cu amendamente admise**, precum și **propunerea legislativă**.

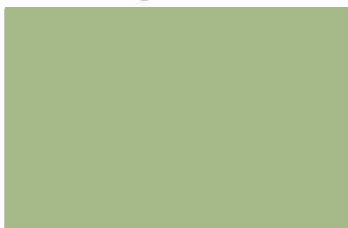
În raport cu obiectul de reglementare, proiectul legislativ face parte din categoria **legilor ordinare** și urmează a fi adoptat în conformitate cu prevederile art. 76 alin. (2) din Constituția României, republicată.

Potrivit art. 75 alin. (1) din Constituția României, republicată, și art. 92 alin. (7), pct. 1 din Regulamentul Senatului, republicat, în vigoare, **Senatul** este **prima Cameră sesizată**.

PREȘEDINTE

Senator,

Vasile-Ciprian RUS



SECRETAR

Senator,

Grigore-Adrian PEIU



AMENDAMENTE ADMISE

la Propunerea legislativă pentru completarea Ordonanței de urgență a Guvernului nr. 155/2024 privind instituirea unui
cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil
(L593/2026)

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
1	Articolul unic	Articolul unic se renumerează și devine Articolul I, și va avea următorul cuprins: <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	
2	Art. I 1. Art. 24 h) organizarea și gestionarea programelor de identificare și raportare a vulnerabilităților cu recompensarea persoanelor respective, conform art. 36 ¹ , inclusiv prin acordarea de recompense bănești pentru vulnerabilitățile validate."	Art. I. 1. La art. 24, alin. (4), lit. h) se modifică și va avea următorul cuprins: h) organizarea și gestionarea programelor de identificare și raportare a vulnerabilităților, cu acordarea de recompense bănești pentru vulnerabilitățile validate, în condițiile prevăzute la art. 36¹ și în limita creditelor bugetare aprobate cu această destinație. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	<u>Răspunde observației Consiliului Legislativ privind necesitatea corelării normei cu regimul bugetar al DNSC.</u> Clarifică obiectul atribuției DNSC, corelează acordarea recompenselor cu condițiile stabilite la art. 36 ¹ și precizează limita bugetară aplicabilă. Totodată, păstrează distincția dintre organizarea programelor și acordarea efectivă a recompenselor. <i>Amendament admis cu unanimitate de voturi.</i>

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
3	Art. I. 2.Art. 36¹ (1) DNSC poate iniția și gestiona programe de identificare și raportare recompensată a vulnerabilităților pentru rețelele și sistemele informatice proprii, precum și pentru cele deținute, administrate ori utilizate de autorități și instituții publice sau de alte entități de drept public din spațiul cibernetic național civil, cu respectarea excluderilor și regimurilor speciale prevăzute la art. 2.	Art. I. La art. 36¹, alin. (1) se modifică și va avea următorul cuprins: (1) DNSC poate iniția și gestiona programe de identificare și raportare a vulnerabilităților, cu acordarea de recompense bănești pentru vulnerabilitățile validate, pentru rețelele și sistemele informatice proprii, precum și pentru cele deținute, administrate sau utilizate de autorități și instituții publice ori de alte entități de drept public din spațiul cibernetic național civil, cu respectarea domeniului de aplicare, a excluderilor și a regimurilor speciale prevăzute la art. 2, precum și a competențelor și drepturilor titularilor rețelelor și sistemelor informatice vizate. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	<u>Răspunde observației Consiliului Legislativ privind competența autorizării.</u> Simplul fapt că DNSC administrează sau utilizează un sistem nu înseamnă că poate autoriza testarea tuturor componentelor acestuia. Se menține obiectul inițial al reglementării, dar se introduce expres obligația respectării competențelor și drepturilor titularilor. Trimiterea la art. 2 trebuie să producă efecte reale, inclusiv în cazul infrastructurilor comune, externalizate sau interconectate. <i>Amendament admis cu unanimitate de voturi.</i>
4	Art. I. Art. 36¹ (2) Pentru rețelele și sistemele informatice care nu sunt deținute sau administrate de DNSC, programul se organizează numai cu acordul prealabil, expres și scris al entității în cauză și, după caz, al oricărui alt titular al dreptului de a autoriza testarea.	Art. I. La art. 36¹, alineatul (2) se modifică și va avea următorul cuprins: (2) Includerea unei rețele sau a unui sistem informatic într-un program prevăzut la alin. (1) este condiționată de acordul prealabil, expres și scris al tuturor titularilor dreptului de a autoriza testarea asupra rețelei, sistemului informatic sau componentelor vizate. Acordul identifică rețeaua, sistemul informatic sau componentele asupra cărora se poate	<u>Răspunde observației Consiliului Legislativ privind competența autorizării.</u> Se elimină diferența nejustificată dintre sistemele administrate de DNSC și celelalte sisteme. Acordul trebuie să provină de la persoanele sau entitățile care au efectiv dreptul de a autoriza testarea. DNSC poate administra un sistem fără a deține dreptul de a autoriza testarea tuturor componentelor sale. Prin urmare, acordurile trebuie să fie

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
		efectua testarea și precizează limitele acesteia. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	determinate de drepturile efective asupra sistemului și de competența legală de autorizare, nu doar de calitatea de proprietar sau administrator.
5	Art. I. Art. 36¹	Art. I. La art. 36¹, după alin. (2) se adaugă un nou alineat, alin. (3), cu următorul cuprins: (3) Programele prevăzute la alin. (1) constituie un mecanism complementar procesului de divulgare coordonată a vulnerabilităților reglementat la art. 36. Vulnerabilitățile identificate în cadrul acestor programe se raportează și se gestionează cu respectarea dispozițiilor art. 36. În măsura în care activitățile desfășurate în cadrul programelor intră în sfera atribuțiilor prevăzute la art. 36 alin. (1), se aplică și dispozițiile art. 36 alin. (1¹) privind consultarea comitetului consultativ. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	<u>Raspunde observației Consiliului Legislativ care cere să se precizeze dacă programele recompensate fac parte din procesul de divulgare coordonată a vulnerabilităților reglementat la art. 36 sau reprezintă o activitate separată.</u> Se stabilește expres caracterul complementar al programelor și se clarifică aplicarea mecanismului de divulgare coordonată și a consultării comitetului consultativ. <i>Amendament admis cu unanimitate de voturi.</i>
6	Art. I. Art. 36¹	Art. I. La art. 36¹, alin (3) din textul propunerii legislative se renumerează și devine alin. (4), se modifică și va avea următorul cuprins:	<u>Răspunde observației Consiliului Legislativ potrivit căreia DNSC este finanțat integral de la bugetul de stat, prin bugetul Secretariatului General al Guvernului, iar sintagma „bugetul de</u>

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
	(3) În cadrul programelor prevăzute la alin. (1), DNSC poate acorda recompense bănești persoanelor fizice sau juridice pentru vulnerabilitățile raportate și validate, potrivit regulilor programului și în limita creditelor bugetare aprobate cu această destinație în bugetul de venituri și cheltuieli al DNSC. Valoarea maximă a recompensei pentru o vulnerabilitate și valoarea totală a fondului de recompense se stabilesc și se aduc la cunoștința participanților înaintea începerii programului.	(4) În cadrul programelor prevăzute la alin. (1), DNSC poate acorda recompense bănești persoanelor fizice sau juridice pentru vulnerabilitățile raportate și validate, în conformitate cu criteriile de eligibilitate și validare stabilite pentru program și în limita creditelor bugetare aprobate cu această destinație. Valoarea maximă a recompensei pentru o vulnerabilitate și valoarea totală a fondului de recompense se stabilesc și se aduc la cunoștința participanților înaintea începerii programului. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	<u>venituri și cheltuieli al DNSC” trebuie reconsiderată.</u> <i>Amendament admis cu unanimitate de voturi.</i>
7	Art. I. Art. 36¹ (4) Aprobarea de către DNSC a programului și, după caz, acordul prevăzut de dispozițiile alin. (2), împreună cu acceptarea regulilor programului de către participant, constituie o autorizare prealabilă, expresă, limitată și condiționată pentru activitățile de testare permise. Autorizarea operează exclusiv asupra rețelelor și sistemelor informatice incluse în program, în perioada și prin metodele prevăzute de regulile acestuia.	Art. I. La articolul 36¹, alineatul (4) din textul propunerii legislative se renumerează și devine alin. (5), se modifică și va avea următorul cuprins: (5) Activitățile de testare în cadrul programelor prevăzute la alin. (1) pot fi desfășurate numai după aprobarea programului de către DNSC, obținerea acordurilor prevăzute la alin. (2) și acceptarea expresă de către participant a condițiilor programului. Autorizarea este limitată la rețelele, sistemele și componentele identificate în program, la metodele de testare permise și la perioada stabilită pentru desfășurarea activităților. Programul și condițiile	Se identifică actele și condițiile cumulative necesare pentru desfășurarea testării și se precizează elementele minime ale autorizării. <u>Acest lucru răspunde cerințelor de claritate și predictibilitate invocate de Consiliul Legislativ, care critică în mod expres faptul că aprobarea programului, acordurile și acceptarea regulilor programului sunt calificate drept „autorizare prealabilă, expresă, limitată și condiționată”, fără să fie precizate suficient conținutul și efectele juridice ale autorizării.</u>

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
		acceptate de participant stabilesc, în mod clar și verificabil, cel puțin obiectul testării, metodele permise, durata, limitele tehnice și operaționale, modalitatea de raportare a vulnerabilităților și condițiile de suspendare sau încetare a autorizării. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	<i>Amendament admis cu unanimitate de voturi.</i>
8		Art. I. După noul alineat (5), se adaugă patru noi alineate, alin. (6), (7), (8) și (9) cu următorul cuprins: (6) În cadrul programelor prevăzute la alin. (1) sunt interzise: a) accesarea, copierea, ștergerea sau modificarea neautorizată a datelor; b) utilizarea atacurilor de tip brute-force, a tehnicilor de phishing ori a altor tehnici de inginerie socială; c) utilizarea de programe de tip malware sau a altor tehnici care afectează ori pot afecta disponibilitatea, integritatea sau funcționarea rețelelor și sistemelor informatice; d) menținerea accesului la rețelele și sistemele informatice după încetarea autorizării sau extinderea accesului la alte rețele, sisteme, componente ori conturi care nu sunt incluse în program;	<u>Conform observației Consiliului Legislativ.</u> Se introduc în corpul legii interdicțiile operaționale prezentate în expunerea de motive, dar absente din textul inițial.

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
Art. I. Art. 36¹ (5) Participarea la programele prevăzute la alin. (1) este voluntară și nu creează obligația participantului de a		e) divulgarea publică a vulnerabilităților cu încălcarea condițiilor legale aplicabile procesului de divulgare coordonată; f) orice altă activitate care depășește limitele autorizării sau contravine prevederilor legale aplicabile. (7) Nerespectarea condițiilor programului ori depășirea limitelor autorizării atrage încetarea autorizării pentru activitățile respective și pierderea dreptului la recompensă pentru vulnerabilitatea în cauză, fără a aduce atingere răspunderii civile, contravenționale sau penale, după caz. (8) Desfășurarea activităților în cadrul programelor prevăzute la alin. (1) se realizează cu respectarea condițiilor prevăzute la art. 36 alin. (5) și (6). Aprobarea programului, acordurile prevăzute la alin. (2) și acceptarea condițiilor programului nu înlătură și nu modifică regimul răspunderii juridice stabilit prin lege și nu conferă imunitate pentru faptele săvârșite cu depășirea limitelor autorizării. Art. I. La art. 36¹, alin. (5) din textul propunerii legislative se renumerează și devine alin. (9) și va avea următorul cuprins: (9) Participarea la programele prevăzute la alin. (1) este voluntară și nu creează obligația	Se reglementează expres consecințele depășirii limitelor autorizării, în concordanță cu soluția anunțată în expunerea de motive. Se clarifică raportul dintre autorizarea în cadrul programului și condițiile legale privind cercetarea și raportarea vulnerabilităților. Amendamentul ține seama de art. 365¹ din Codul penal, introdus prin Legea nr. 123/2026 și de condițiile cumulative prevăzute de lege pentru aplicarea cauzei de înlăturare a caracterului penal. Amendament admis cu unanimitate de voturi.

Nr. crt.	Text propunere legislativă	Amendamente admise	Motivare inițiator amendament/Observații
	efectua activități de testare ori de a obține un anumit rezultat.	participantului de a efectua activități de testare ori de a obține un anumit rezultat. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	
9		Se adaugă un nou articol, Articolul II, cu următorul cuprins: În termen de 90 de zile de la data intrării în vigoare a prezentei legi, Guvernul aprobă, prin hotărâre, normele metodologice de aplicare a art. 36¹ din Ordonanța de urgență a Guvernului 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, care stabilesc cel puțin procedura de inițiere și aprobare a programelor, criteriile de selectare a rețelelor și sistemelor informatice, condițiile de participare, procedura de raportare și validare a vulnerabilităților, criteriile de stabilire și procedura de acordare a recompenselor, măsurile privind protecția datelor și confidențialitatea, precum și condițiile de monitorizare, suspendare și încetare a programelor. <i>Autori amendamente:</i> <i>Glad-Aurel Varga, senator PNL</i> <i>Octavian Oprea, deputat PNL</i>	Se introduce temeiul normativ expres pentru adoptarea hotărârii Guvernului anunțate în expunerea de motive. Se precizează obiectul reglementării subsecvente, astfel încât să nu existe incertitudine cu privire la procedurile care urmează să fie detaliate. Normele metodologice vor pune în aplicare legea, fără a putea modifica limitele autorizării, regimul răspunderii juridice sau alte elemente esențiale stabilite prin actul normativ primar. <i>Amendament admis cu unanimitate de voturi.</i>