



CONSILIUL LEGISLATIV

Biroul permanent al Senatului

Bp. 489 / 5 Octombrie 2026

AVIZ

referitor 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

Analizând 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 (b489/02.09.2026), transmisă de Secretarul General al Senatului cu adresa nr. XXXV/4143/08.09.2026 și înregistrată la Consiliul Legislativ cu nr. D769/09.09.2026,

CONSILIUL LEGISLATIV

În temeiul art. 2 alin. (1) lit. a) din Legea nr. 73/1993, republicată, și al art. 29 alin. (4) din Regulamentul de organizare și funcționare a Consiliului Legislativ,

Avizează negativ propunerea legislativă, pentru următoarele considerente:

1. 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, administrare 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”.

2. Menționăm că, prin avizul pe care îl emite, Consiliul Legislativ nu se pronunță asupra oportunității soluțiilor legislative preconizate.

3. Prin conținutul său normativ, propunerea legislativă face parte din categoria **legilor ordinare**, iar în aplicarea art. 75 alin. (1) din Constituția României, republicată, prima Cameră sesizată este Senatul.

4. **Ca observație de fond**, în considerarea dispozițiilor art. 6 alin. (1) și art. 13 lit. a) din Legea nr. 24/2000, semnalăm că normele propuse la art. 36¹ alin. (1), (2) și (4) din proiect **sunt lipsite de claritate, precizie și predictibilitate, deoarece nu delimitează competența de autorizare a testării în raport cu drepturile asupra sistemelor vizate, precum și cu regimul legal al cercetării și raportării vulnerabilităților**. Astfel, art. 36¹ alin. (2) impune acordul entității și al celorlalți titulari **numai pentru sistemele care nu sunt deținute sau administrate de DNSC**. În consecință, pentru un sistem administrat de DNSC, dar asupra căruia o altă entitate își rezervă dreptul de a autoriza testarea, **alin. (4) permite calificarea aprobării programului drept autorizare fără a cere expres toate acordurile necesare, deși calitatea de administrator nu probează, prin ea însăși, întinderea dreptului de autorizare**.

Menționăm că deficiența semnalată privește chiar **mecanismul juridic prin care programul recompensat ar urma să permită accesul și testarea și rezultă din coroborarea normelor propuse la alin. (1), (2) și (4) ale art. 36¹ din proiect, raportată la art. 5 lit. a) și b) din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, fiind susceptibilă să genereze dificultăți de aplicare și de a aduce atingere prevederilor art. 1 alin. (5) din Constituția României, republicată, în componenta privind calitatea legii**.

Dispozițiile art. 36 alin. (1) - (3) din Ordonanța de urgență a Guvernului nr. 155/2024 - actul normativ de bază - consacră deja **rolul DNSC de coordonator al divulgării coordonate a vulnerabilităților și atribuțiile de primire, evaluare, verificare și intermediere a**

raportărilor, iar **art. 36 alin. (2) lit. i)** permite emiterea de proceduri, norme tehnice și ghiduri inclusiv pentru programele private de divulgare a vulnerabilităților.

Prin urmare, nu se poate susține - vezi expunerea de motive - că activitatea de raportare și gestionare a vulnerabilităților este lipsită de reglementare. Elementul de noutate pe care îl aduce propunerea legislativă constă în **competența expresă de organizare a unor programe publice de testare recompensată și în instituirea unei categorii determinate de cheltuieli.**

Apreciem că, în considerarea prevederilor **art. 6 alin. (1), art. 13 și art. 31 din Legea nr. 24/2000** privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată, cu modificările și completările ulterioare, **expunerea de motive ar fi trebuit să delimiteze această noutate de instrumentele deja existente.**

Totodată, avem în vedere și **insuficienta determinare a regimului juridic aplicabil programelor de identificare și raportare recompensată a vulnerabilităților și, mai cu seamă, a efectelor juridice ale „autorizării”** activităților de testare preconizate la norma propusă pentru **art. 36¹ alin. (4) din proiect.** Potrivit acesteia, aprobarea programului de către Directoratul Național de Securitate Cibernetică, acordul entității în cauză și, după caz, al oricărui alt titular al dreptului de a autoriza testarea, împreună cu acceptarea regulilor programului de către participant, constituie o **„autorizare prealabilă, expresă, limitată și condiționată”** pentru activitățile de testare permise. Precizăm că, în actuala redactare, **norma nu stabilește cu suficientă claritate conținutul și întinderea juridică a acestei autorizări, raportul său cu condițiile aplicabile activităților de cercetare și raportare a vulnerabilităților care sunt prevăzute deja la art. 36 alin. (5) și (6) din Ordonanța de urgență a Guvernului nr. 155/2024 și nici consecințele juridice ale depășirii limitelor autorizării.** Or, aceste aspecte prezintă o relevanță deosebită inclusiv sub aspectul răspunderii penale, având în vedere că **art. 365¹ din Legea nr. 286/2009 privind Codul penal, introdus prin Legea nr. 123/2026, instituie o cauză de înlăturare a caracterului penal numai pentru faptele expres prevăzute de această normă și numai în cazul îndeplinirii cumulative a condițiilor stabilite la art. 36 alin. (5) și (6) din Ordonanța de urgență a Guvernului nr. 155/2024.**

Prin urmare, considerăm că simpla calificare, prin proiect, a participării la program drept „autorizare” nu poate avea semnificația unei exonerări generale de răspundere și nici nu poate modifica, implicit, condițiile stabilite de legea penală.

Deși, în forma propusă, **art. 36¹ alin. (4)** asimilează aprobarea DNSC, acordurile titularilor și acceptarea regulilor programului unei **autorizări prealabile, exprese, limitate și condiționate**, totuși, nu determină suficient elementele minime ale autorizării și nu indică raportul dintre aceasta și interdicțiile prevăzute la art. 36 alin. (5) și obligația de raportare de la alin. (6) din actul normativ de bază.

În considerarea **art. 1 alin. (5) din Constituție și a art. 6, art. 36 și art. 37 din Legea nr. 24/2000**, norma trebuie să permită identificarea prealabilă a sistemelor, metodelor, duratei și limitelor relevante, fără a transfera integral configurarea condițiilor esențiale către regulile fiecărui program.

Mai mult, precizăm că prin **Legea nr. 123 din 3 iulie 2026** pentru completarea art. 36 din Ordonanța de urgență a Guvernului nr. 155/2024 și pentru completarea Legii nr. 286/2009 privind Codul penal s-a introdus un nou articol, **art. 36 alin. (1¹)**, care prevede **consultarea de către DNSC a unui comitet consultativ alcătuit din autoritățile indicate la art. 11, 12 și 14 - 17 din Legea nr. 58/2023**, tocmai pentru îndeplinirea dispozițiilor art. 36 alin. (1).

Ca atare, **apreciem că este necesar a se clarifica dacă programele vizate de noul art. 36¹ din proiectul propus intră în sfera procesului de divulgare coordonată, astfel încât consultarea să fie incidentă, sau să reprezinte o activitate separată.** În lipsa acestei precizări există riscul de a genera aplicări divergente cu privire la circuitul avizării și la cooperarea dintre autoritățile competente.

Semnalăm și faptul că, trimiterea din norma propusă la art. 36¹ alin. (1) din proiect la art. 2 din actul normativ de bază trebuie aplicată efectiv, iar nu numai declarativ deoarece art. 2 stabilește domeniul de aplicare, excluderile pentru anumite autorități ori activități și regimurile speciale. Menționăm că, **potrivit dispozițiilor art. 3 alin. (1) și art. 5 lit. a) - b) din Legea nr. 58/2023** privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, **competențele și responsabilitatea deținătorilor, administratorilor și utilizatorilor de sisteme sunt distincte.** În cazul unor infrastructuri comune, externalizate sau interconectate, acordul unei instituții care utilizează sistemul nu este, prin el însuși, suficient pentru a autoriza testarea altor componente ori a infrastructurilor exceptate.

Din acest punct de vedere, **semnalăm și existența unei neconcordanțe evidente între soluțiile prezentate în expunerea de motive și cele consacrate în partea dispozitivă a propunerii legislative.** Astfel, în expunerea de motive se precizează că nu vor putea

fi autorizate atacurile de tip brute-force, phishingul, ingineria socială, utilizarea de programe de tip malware, afectarea disponibilității serviciilor, ștergerea sau modificarea datelor, menținerea accesului ori extinderea acestuia către alte sisteme sau conturi. De asemenea, se arată că depășirea limitelor programului va determina pierderea dreptului la recompensă, fără a înlătura răspunderea civilă, contravențională sau penală, precum și că detaliile referitoare la inițierea programelor, selectarea sistemelor, condițiile de participare, validarea vulnerabilităților, stabilirea și plata recompenselor, protecția datelor, confidențialitatea, controlul și suspendarea programelor vor fi reglementate prin hotărâre a Guvernului.

Or, constatăm că nici interdicțiile menționate, nici consecințele depășirii limitelor programului și nici soluția privind adoptarea unei hotărâri a Guvernului nu se regăsesc în textul normativ propus.

Precizăm că **normele propuse la art. 36¹ alin. (1) - (5) se limitează**, în esență, la stabilirea posibilității organizării programelor, obținerii acordurilor necesare, acordării recompenselor și constituirii autorizării prin acceptarea „**regulilor programului**”, fără ca legea să determine elementele esențiale ale acestor reguli ori să prevadă expres cadrul normativ subsecvent prin care acestea ar urma să fie dezvoltate.

Ca atare, constatăm că **expunerea de motive** prezintă o soluție normativă mult mai amplă decât aceea care rezultă din dispozitivul propunerii legislative, fiind descrise garanții, interdicții, consecințe juridice și mecanisme de punere în aplicare care nu au corespondent în norma preconizată.

O asemenea necorelare este susceptibilă să afecteze claritatea, precizia și previzibilitatea reglementării, exigențe care decurg din **prevederile art. 1 alin. (5) din Constituția României, republicată**, și care trebuie avute în vedere și prin raportare la art. 6 alin. (1), art. 31 alin. (1) și art. 32 alin. (1) și (2) din Legea nr. 24/2000. Potrivit art. 32 alin. (2) din această lege, motivarea trebuie să se refere la forma finală a proiectului de act normativ, iar modificările intervenite asupra proiectului impun reconsiderarea corespunzătoare a motivării.

Față de cele de mai sus, apreciem că este necesară reanalizarea soluției legislative și completarea acesteia astfel încât chiar norma de nivel primar să stabilească, într-o manieră neechivocă, **raportul dintre programele de identificare și raportare recompensată și mecanismul de divulgare coordonată a vulnerabilităților** reglementat la art. 36 din actul normativ de bază, condițiile și limitele esențiale ale autorizării activităților de testare, consecințele nerespectării acestor limite, raportul cu regimul răspunderii juridice,

precum și, dacă se menține soluția anunțată în expunerea de motive, temeiul și limitele reglementării prin hotărâre a Guvernului.

În mod corespunzător, **expunerea de motive va trebui reanalizată, reformulată și corelată cu soluțiile normative efectiv reținute în cuprinsul propunerii legislative**, în concordanță cu prevederile art. 31 din Legea nr. 24/2000, care stabilește în mod imperativ secțiunile pe care trebuie să le cuprindă un asemenea document, și cu prevederile art. 32 alin. (2) din același act normativ, care prevede că **motivarea trebuie să se refere la forma finală a proiectului de act normativ**.

De altfel, semnalăm că, **la pagina a doua a expunerii de motive**, sunt anunțate interdicții operaționale, pierderea dreptului la recompensă în cazul depășirii regulilor și **adoptarea unei hotărâri a Guvernului pentru punerea în aplicare**, însă niciunul dintre aceste trei elemente nu este reglementat expres în articolul unic al proiectului propus. Precizăm că, pe de altă parte, unele interdicții propuse se regăsesc deja la art. 36 alin. (5) din actul normativ de bază, dar proiectul nu face trimitere la ele, iar celelalte soluții așa-zis noi nu au suport în dispozitiv. În considerarea dispozițiilor art. 30 - 32 și art. 61 alin. (2) din Legea nr. 24/2000, apreciem că documentul de prezentare și motivare trebuie corelat cu soluțiile efectiv supuse adoptării.

Formulăm observația întrucât există riscul ca proiectul de act normativ să fie lovit de viciul de neconstituționalitate referitor la fundamentarea actului normativ, la paragrafele 80 și 81 din Decizia nr. 139 din 13 martie 2019, Curtea Constituțională pronunțându-se cu privire la acest aspect, astfel: *„Lipsa unei fundamentări temeinice a actului normativ în discuție determină, pentru motivele arătate, încălcarea prevederilor din Constituție cuprinse în art. 1 alin. (5) potrivit cărora, «În România, respectarea Constituției, a supremației sale și a legilor este obligatorie», precum și ale art. 147 alin. (4) potrivit cărora deciziile Curții Constituționale sunt general obligatorii”¹, dar și a „dispozițiilor art. 1 alin. (3) din Constituție, care consacră statul de drept și principiul dreptății”*.

De asemenea, s-a reținut că *„Fundamentarea temeinică a inițiativelor legislative reprezintă o exigență impusă de dispozițiile constituționale menționate, întrucât previne arbitrarul în activitatea de legiferare, asigurând că legile propuse și adoptate răspund unor nevoi sociale reale și dreptății sociale (...)”*.

¹ Citând pct. 2.21 și 2.22 din Decizia nr. 682 din 27 iunie 2012.

În ceea ce privește regimul bugetar și fișa financiară, introducerea art. 24 alin. (4) lit. h) și a art. 36¹ alin. (3) presupune efectuarea unor cheltuieli pentru plata unor programe și recompense și creează o categorie de cheltuieli din fonduri publice. Mențiunea din art. 36¹ alin. (3) privind limita creditelor aprobate și plafonarea fondului fiecărui program constituie reguli de execuție, dar nu înlocuiește analiza impactului financiar și identificarea sursei de finanțare, fiind incidente prevederile art. 111 alin. (1) și art. 138 alin. (5) din Constituție, art. 14 alin. (2) - (3) și art. 15 alin. (1) - (2) din Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, precum și art. 15 alin. (1) lit. a) din Legea responsabilității fiscal-bugetare nr. 69/2010, republicată, cu modificările și completările ulterioare.

În Decizia Curții Constituționale nr. 681 din 30 septembrie 2020, paragrafele 28 - 30, se distinge între solicitarea fișei financiare, întocmirea ei de către Guvern și solicitarea punctului de vedere al acestuia; paragrafele 31 - 33 privesc caracterul real al sursei de finanțare.

Art. 1 alin. (1) și art. 11 alin. (1) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022, cu modificările și completările ulterioare, prevăd finanțarea integrală a DNSC de la bugetul de stat, prin bugetul Secretariatului General al Guvernului. Ca atare, norma propusă pentru art. 36¹ alin. (3), care conține sintagma „**bugetul de venituri și cheltuieli al DNSC**”, trebuie confruntată cu acest regim, precum și cu terminologia folosită de art. 24 alin. (4) din actul normativ sus-menționat, care se referă la „**bugetul DNSC**”.

*

* *

Față de cele expuse mai sus, apreciem că propunerea legislativă nu poate fi promovată în forma prezentată, fiind necesară revederea și reformularea acesteia.

PRESEDINTE
Florin IORDACHE



București
Nr. 831/01.10.2026