CONSILIUL LEGISLATIV

AVIZ

referitor la propunerea legislativă pentru modificarea și completarea Ordonanței de Urgență 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, precum și pentru completarea Legii nr. 286/2009 privind Codul Penal

Analizând **propunerea legislativă pentru modificarea și completarea Ordonanței de Urgență 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, precum și pentru completarea Legii nr. 286/2009 privind Codul Penal** (b53/11.02.2026), transmisă de Secretarul General al Senatului cu adresa nr. XXXV/681/16.02.2026 și înregistrată la Consiliul Legislativ cu nr. D80/16.02.2026,

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 şi funcţionare a Consiliului Legislativ,

Avizează negativ propunerea legislativă, din următoarele considerente:

1. Propunerea legislativă are ca obiect de reglementare „completarea art. 36 din Ordonanţa de urgenţă nr. 155/2024 prin introducerea unui nou alineat, care stabileşte ***obligaţia*** *Directoratului Național privind Securitatea Cibernetică(DNSC) de a se consulta cu un comitet interinstituțional*, constituit din autorităţile relevante în domeniul securităţii şi apărării cibernetice, reglementarea funcţionării acestui comitet în baza unui statut elalorat de DNSC și avizat de autorităţile membre, asigurând flexibilitate administrativă şi

adaptabilitate la evoluţiile tehnologice, precum şi *completarea Codului Penal cu o prevedere, prin care faptele săvârşite în cadrul activităţilor de cercetare şi raportare a vulnerabilităţilor, realizate în condiţiile prevăzute de O.U.G. nr. 155/2024,* ***nu constituie infracţiune***".

Potrivit **Expunerii de motive** *„Prin instituirea unui mecanism de consultare interinstituţională şi prin clarificarea regimului juridic al cercetării şi raportării vulnerabilităţilor, proiectul de lege contribuie la consolidarea rezilienţei cibernetice a României, în deplină concordanţă cu cadrul european existent şi fără suprapunerea instrumentelor deja funcţionale la nivelul Uniunii Europene".*

Totodată, se mai precizează că *„Din punct de vedere juridic, se asigură o mai bună corelare între legislaţia specială în domeniul securităţii cibernetice şi normele de drept penal, contribuind la eliminarea riscului interpretărilor neunitare".*

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 organice, fiind incidente prevederile art. 73 lit. h) din Constituția României, republicată, iar în aplicarea art. 75 alin. (1) din Legea fundamentală, prima Cameră sesizată este Senatul.

4. Ca observație de fond, la art. I, semnalăm că, prin folosirea expresiei ***„(...) în îndeplinirea prevederilor alin. (1), DNSC se consultă cu un comitet format din autoritățile de la art. 11 - 12 și art. 14 - 17 din Legea nr. 58/2023 (...)"***, norma propusă devine lipsită de claritate, precizie şi previzibilitate, **fiind susceptibilă de a aduce atingere principiului legalității, consacrat de art. 1 alin. (5) din Legea fundamentală**, deoarece se intenționează crearea, în fapt, a unui cadru instituțional - **„comitet"** - dar fără să precizeze dacă acest comitet are un caracter consultativ sau decizional, dacă este un organism cu sau fără personalitate juridică, dacă organizarea și funcționarea acestuia se stabilesc prin regulament aprobat prin **Ordin al directorului DNSC** care se publică în monitorul Oficial al României sau este nepublic, cu avizul autorităților membre, dacă există o regulă privind cvorumul, periodicitatea consultării, termenul de răspuns, precum și a unui regim juridic neclar al **„statutului".**

Precizăm că, **obiectul de reglementare al 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 îl reprezintă cadrul de **securitate cibernetică în spațiul cibernetic național civil**.

Or, prin norma propusă la **alin. (1[1])** se includ, în mod formal, în acest mecanism - comitet - **autorități și instituții publice din domeniul securității naționale: Ministerul Apărării Naționale și Ministerul Afacerilor Interne; Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale, Serviciul de Protecție și Pază, fără ca acest fapt să fie justificat și delimitat normativ:** consultarea este în scopul identificării vulnerabilităților cu potențial impact asupra securității naționale, asupra infrastructurilor critice, sau asupra sistemelor guvernamentale.

Totodată, se impune și o delimitare a situațiilor în care DNSC consultă un comitet, respectiv doar în cazul vulnerabilităților a căror exploatare poate afecta **securitatea națională**, infrastructuri critice ori sisteme informatice de interes guvernamental, sau al întregului **spațiu cibernetic național.**

În forma actuală, **art. 36 din Ordonanța de urgență a Guvernului nr. 155/2024** stabilește că Directoratul Național de Securitate Cibernetică, ca **CSIRT național**, gestionează divulgarea coordonată a vulnerabilităților fiind ***„coordonator care acționează ca intermediar de încredere"***.

Ca atare, norma propusă nu se corelează cu prevederile **art. 36 alin. (2)** care enumeră atribuții concrete, inclusiv faptul că ***DNSC „emite proceduri, norme tehnice și ghiduri"*** cu cerințe minime sau recomandări pentru raportare, conduită, programe private, iar ***alin. (5) - (6)*** fixează condiții de bună-credință și conduită a raportorului, cum ar fi de exemplu: fără copiere neautorizată, fără ocolirea barierelor tehnice, fără divulgare publică fără acord, precum și regula de raportare în 48 de ore.

Totodată, semnalăm că norma este susceptibilă de a crea un paralelism legislativ, prin suprapunere cu mecanisme sau organisme deja prevăzute în **Legea nr. 58/2023** care are conține dispoziții privind **Consiliul Operativ de Securitate Cibernetică (COSC)**, de la care se solicită aviz prealabil și consultativ în anumite situații excepționale **și în componența căruia intră și Directoratului Național privind Securitatea Cibernetică.**

Referitor la „comitetul" ce se intenționează a fi instituit prin norma preconizată la Art. I. din proiect, menționăm că aceasta nu se corelează cu prevederile **art. 10 alin. (1)** din Legea nr. 58/2023:

„Sunt autorități competente în sensul prezentei legi:

***a) DNSC, pentru spațiul cibernetic național civil**, conform prevederilor prezentei legi și ale Ordonanței de urgență a Guvernului*

nr. 104/2021, aprobată cu modificări și completări prin Legea nr. 11/2022, cu modificările ulterioare;", în timp ce

***b) la alin. (3)** se prevede că „Autoritățile prevăzute la alin. (1) **pot elabora strategii și norme proprii, prin acte administrative ale conducătorilor autorităților, pentru reglementarea activităților de securitate cibernetică**, la nivel instituțional".*

De asemenea, constatăm că proiectul de act normativ indică autoritățile de la art. 11 - 12 și 14 - 17 din Legea nr. 58/2023, care sunt, în esență: Ministerul Apărării Naționale și Ministerul Afacerilor Interne; Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale, Serviciul de Protecție și Pază, **fără a exista justificarea de ce sunt incluse doar acestea și nu și alte autorități relevante din arhitectura Legii nr. 58/2023**, dacă intenția este una de guvernanță extinsă, ori de ce consultarea nu este limitată doar la cazurile cu impact pentru securitatea națională.

În concluzie, **norma propusă nu se corelează nici cu prevederile art. 39 din Ordonanța de urgență a Guvernului nr. 155/2024** care dispune faptul că **pentru asigurarea unui nivel comun ridicat de securitate cibernetică la nivel național, DNSC se consultă și cooperează cu Serviciul Român de Informații**, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale a căror afectare aduce atingere securității naționale, cu **Ministerul Apărării Naționale**, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în sprijinul activităților privind apărarea națională, cu **Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază,** pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale în domeniul lor de activitate și responsabilitate.

De asemenea, se instituie și faptul că DNSC se consultă și cooperează, după caz, și cu: **organele de urmărire penală**, dar și cu **Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal**, în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii.

5. La **art. II**, referitor la norma propusă pentru **art. 365[1] din Codul penal**, semnalăm că, prin conținutul lor, condițiile prevăzute la art. 36 alin. (5) și (6) din Ordonanța de urgență a Guvernului nr. 155/2024, **care trebuie îndeplinite cumulativ**, **nu pot constitui ipoteze de excludere a răspunderii penale pentru toate infracțiunile prevăzute la art. 360 - 365 din Codul penal**.

Avem în vedere faptul că unele dintre condiții se referă tocmai la faptele incriminate drept infracțiuni.

Astfel, întrucât **art. 36 alin. (5) lit. b) stabilește condiția** ca activitatea de cercetare să se desfășoare fără accesarea sau copierea neautorizată a conținutului fișierelor din sistemele informatice care fac obiectul activității de cercetare, **nu poate fi exclusă răspunderea penală pentru fapta prevăzută la art. 360 alin. (2) din Codul penal**, normă care incriminează accesul fără drept la un sistem informatic săvârșit în scopul obținerii de date informatice, și nici pentru fapta prevăzută la **art. 364** din același act normativ, normă care incriminează transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice.

Totodată, întrucât **art. 36 alin. (5) lit. c) stabilește condiția** ca în cadrul activității de cercetare să nu fie șterse sau modificate date din sistemele informatice care fac obiectul activității de cercetare, **nu poate fi exclusă răspunderea penală pentru fapta prevăzută la art. 362 teza întâi din Codul penal**, constând în modificarea, ștergerea sau deteriorarea, fără drept, a datelor informatice.

În ceea ce privește condiția prevăzută la **art. 36 alin. (5) lit. d)** referitoare la desfășurarea activității de cercetare fără încălcarea sau ocolirea unor bariere tehnice precum parole sau detalii de identificare, prin tehnici precum atacuri brute-force, prin phishing sau alte procedee de inginerie socială, **apreciem că aceasta este incompatibilă cu excluderea răspunderii penale pentru fapta prevăzută la art. 360 alin. (3) din Codul penal,** normă care incriminează accesul fără drept la un sistem informatic la care, prin intermediul unor proceduri, dispozitive sau programe specializate, accesul este restricționat sau interzis pentru anumite categorii de utilizatori.

În plus, condițiile prevăzute la **art. 36 alin. (5) lit. e) și f)**, care impun ca prin activitatea de cercetare să nu se cauzeze nicio întrerupere sau deteriorare a produselor sau serviciilor TIC ale terților și ca aceasta să nu se desfășoare pentru a derula atacuri sau a produce prejudicii și să nu utilizeze produse de tip malware sau tehnici de natură să afecteze disponibilitatea serviciilor TIC, **sunt incompatibile, cel puțin în parte, cu excluderea răspunderii penale pentru fapta incriminată la art. 363**, constând în perturbarea gravă, fără drept, a unui sistem informatic.

Pe de altă parte, din motivare nu rezultă rațiunea pentru care desfășurarea activității de cercetare în condițiile stabilite la **art. 36 alin. (5) și (6)** ar putea justifica excluderea răspunderii penale în cazul săvârșirii faptei constând în restricționarea, fără drept, a accesului la date, prevăzută la art. 362 teza a doua din Codul penal sau efectuarea

de operațiuni ilegale cu dispozitive sau programe informatice, incriminată în cuprinsul art. 365 din Codul penal.

În concluzie, toate aceste aspecte contravin exigențelor de redactare **clară, precisă și coerentă** și de **integrare sistematică** a intervențiilor legislative, normele propuse prin prezentul proiect sunt de natură să încalce normele de tehnică legislativă, **cerințele de calitate a legii, subsumate art. 1 alin. (5) din Constituție**, motiv pentru care **se impune reanalizarea în totalitate soluției legislative.**

Referitor la cele menționate ***supra***, prin **Decizia nr. 619/2016**, Curtea Constituțională a reținut că *„legea trebuie să întrunească cele **trei cerințe de calitate care rezultă din art. 1 alin. (5) din Constituție** - claritate, precizie și previzibilitate. Curtea a statuat că respectarea legilor este obligatorie, însă nu se poate pretinde unui subiect de drept să respecte o lege care nu este clară, precisă și previzibilă, întrucât acesta nu își poate adapta conduita în funcție de ipoteza normativă a legii. De aceea, una dintre cerințele principiului respectării legilor vizează calitatea actelor normative. Așadar, orice act normativ trebuie să îndeplinească anumite condiții calitative, respectiv să fie clar, precis și previzibil (...).*

Curtea a stabilit că cerința de claritate a legii vizează caracterul neechivoc al obiectului reglementării, cea de precizie se referă la exactitatea soluției legislative alese și a limbajului folosit, în timp ce previzibilitatea legii privește scopul și consecințele pe care le antrenează".

De asemenea, prin **Decizia nr. 242/2020**, Curtea Constituțională a statuat că *„(...) există paralelism legislativ atât în situația în care se reglementează identic într-o anumită sferă a relațiilor sociale, cât și atunci când aceeași problemă este reglementată diferit. (...)".*

Prin urmare, propunerea legislativă, în ansamblul său, **încalcă prevederile art. 1 alin. (5) din Constituție, care consacră principiul legalității, în componenta privind calitatea legii.**

Față de cele prezentate mai sus, propunerea legislativă nu poate fi promovată în forma propusă.

PREȘEDINTE,

Florin IORDACHE

București
Nr. 152/23.02.2026