**PARLAMENTUL ROMÂNIEI**
**CAMERA DEPUTAŢILOR**
**COMISIA PENTRU TEHNOLOGIA INFORMAȚIEI ȘI COMUNICAȚIILOR**

**Nr. 7c-18/73/2026**

**Plx 350/2026**

**Către:**

**BIROUL PERMANENT AL CAMEREI DEPUTAŢILOR**

Vă înaintăm alăturat, **Raportul** asupra **propunerii legislative 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,** trimisă Comisiei pentru tehnologia informației și comunicațiilor pentru dezbatere în fond, cu adresa nr. **Plx 350/2026** din 29 aprilie 2026.

În raport cu obiectul și conținutul său, inițiativa legislativă face parte din categoria legilor **organice.**

**PREŞEDINTE,**

**RADU –NICOLAE MIHAIU**

**PARLAMENTUL ROMÂNIEI**
**CAMERA DEPUTAŢILOR**
**COMISIA PENTRU TEHNOLOGIA INFORMAȚIEI ȘI COMUNICAȚIILOR**

**Nr. 7c-18/73/2026**

**Plx 350/2026**

# RAPORT

asupra

**propunerii legislative 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**

În conformitate cu prevederile art.95 din Regulamentul Camerei Deputaților, Comisia pentru tehnologia informației și comunicațiilor a fost sesizată spre dezbatere în fond, cu **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**, transmisă cu adresa nr. **Pl-x 350/2026.**

**Consiliul Legislativ** a avizat **negativ** propunerea legislativă, conform avizului nr.152/3.02.2026.

**Consiliului Economic și Social** a avizat **favorabil** proiectul de act normativ**,** conform avizului nr. 1450/25.02.2026.

**Senatul,** în calitate de primă Cameră sesizată, **a respins** inițiativa legislativă, în ședința din data de 27 aprilie 2026.

**Comisia pentru muncă şi protecţie socială a avizat favorabil** propunerea legislativă, confom avizului nr. 7c-9/423/11.05.2026.

**Comisia pentru administrație publică și amenajarea teritorilui** a **avizat favorabil** inițiativa legislativă, confom avizului nr. 4c-7/395/2026.

**Camera Deputaților** este **Camera decizională**, potrivit prevederilor art.75 alin. (1) din Constituția României, republicată.

Propunerea legislativă are ca obiect de reglementare completarea art.36 din Ordonanţa de urgenţă a Guvernului nr.155/2024, prin introducerea unui nou alineat, care stabileşte obligaţia Directoratului Naţional privind Securitatea Cibernetică (DNSC) de a se consulta cu un comitet inter instituţional, constituit din autorităţile relevante în domeniul securităţii şi apărării cibernetice, reglementarea funcţionării acestui comitet în baza unui statut elaborat de DNSC şi 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 Ordonanţa de urgenţă a Guvernului nr.155/2024, nu constituie infracţiune.

În conformitate cu prevederile **art.62** și **133** din Regulamentul Camerei Deputaţilor, republicat, membrii Comisiei pentru tehnologia informației și comunicațiilor au examinat proiectul de act normativ în şedinţa din 19 mai 2026**.** La ședințele comisiei deputații au fost prezenți conform listelor de prezență.

În urma dezbaterilor și a opiniilor exprimate, membrii Comisiei pentru tehnologia informației și comunicațiilor au hotărât **cu unanimitate de voturi** să propună plenului Camerei Deputaților **adoptarea propunerii legislative 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**, cu **amendamente admise** redactate în **Anexă** care face parte integrantă din prezentul raport.

În raport cu obiectul și conținutul reglementării, inițiativa legislativă face parte din categoria legilor **organice**.

| | |
|---|---|
| **PREŞEDINTE,** | **SECRETAR,** |
| **RADU – NICOLAE MIHAIU** | **SORIN NĂCUȚĂ** |

**ANEXĂ**

**AMENDAMENTE ADMISE**

**Plx 350/2026**

| Nr.crt. | Forma inițiatori | Amendamente | Motivare |
|---|---|---|---|
| **1.** | Lege 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 | Lege pentru **completarea art. 36 din Ordonanța** de **urgență a Guvernului** nr.155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, precum și pentru completarea Legii nr.286/2009 privind Codul penal | Tehnică legislativă |
| **2.** | **Art. I.** La articolul 36 din Ordonanța de urgență nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, publicată în Monitorul Oficial, Partea I, nr. 1332 din 31 decembrie 2024, aprobată cu modificări și completări prin Legea nr. 124/2025, după alineatul (1) se introduce un nou alineat, alin. $(1)^1$, cu următorul cuprins: | **Art. I.** La articolul 36 din Ordonanța de urgență **a Guvernului** nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, publicată în Monitorul Oficial **al României**, Partea I, nr. 1332 din 31 decembrie 2024, aprobată cu modificări și completări prin Legea nr. 124/2025, după alineatul (1) se introduce un nou alineat, **alin. ($1^1$)**, cu următorul cuprins: | Tehnică legislativă |

| | | | |
|---|---|---|---|
| | (1)[1] În îndeplinirea prevederilor alin. (l), DNSC se consultă cu un comitet format din autoritățile de la art. 11 — 12 și art. 14 — 17 din Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, care funcționează în baza unui statut elaborat de către DNSC și avizat de autoritățile membre. | (1[1]) În îndeplinirea prevederilor alin. (1), DNSC se consultă cu un comitet **consultativ, fără personalitate juridică,** format din autoritățile **prevăzute** la art. 11, 12, 14 — 17 din Legea nr. 58/2023, care funcționează în baza unui statut elaborat de către DNSC și avizat de autoritățile membre. | Preluare observații Consiliul legislativ |
| **3.** | **Art. II.** După art. 365 din Legea nr. 286/2009 privind Codul Penal, publicată în Monitorul Oficial, Partea I, nr. 510 din 24 iulie 2009, se introduce un nou articol 365[1], cu următorul cuprins:<br><br>**Art. 365[1]** Faptele prevăzute în art. 360 — 365 nu constituie infracțiune atunci când sunt săvârșite de o persoană fizică sau juridică, dacă sunt îndeplinite cumulativ condițiile privind cercetarea și raportarea vulnerabilităților unor produse sau servicii ale tehnologiei informațiilor și comunicațiilor | **Art. II.** După **articolul** 365 din Legea nr. 286/2009 privind Codul penal, publicată în Monitorul Oficial **al României**, Partea I, nr. 510 din 24 iulie 2009, **cu modificările și completările ulterioare,** se introduce un nou articol, **articolul** 365[1], cu următorul cuprins:<br><br>Art. 365[1] **Cauză de înlăturare a caracterului penal**<br><br>Faptele prevăzute **la art. 360 alin. (1) și (3), art. 361 și art. 364** nu constituie infracțiune atunci când sunt săvârșite de o persoană fizică sau juridică, dacă sunt îndeplinite cumulativ condițiile privind cercetarea și raportarea vulnerabilităților unor produse sau servicii ale | În vederea implementării observațiilor Consiliului Legislativ privind compatibilitatea tuturor ipotezelor descrise de art. 360-365 cu cauza de înlăturare a răspunderii prevăzută în proiect, în sensul excluderii faptelor a căror consumare nu poate face obiectul cercetării și raportării vulnerabilităților unor produse sau servicii ale tehnologiei informațiilor și comunicațiilor prevăzute la art. 36 alin. (5) și (6) din Ordonanța de urgență a Guvernului nr. 155/2024.<br><br>În ceea ce privește faptele prevăzute la art. 360 alin. (2), art. 360 alin. (3) și art. 364, se apreciază că acestea nu pot fi excluse în mod absolut din sfera cauzei de înlăturare a răspunderii penale, întrucât, în anumite situații, pot interveni în mod inevitabil și incidental |

| | | | |
|---|---|---|---|
| | prevăzute la art. 36 alin. (5) și (6) din Ordonanța de urgentă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, publicată în Monitorul Oficial, Partea I, nr. 1332 din 31 decembrie 2024, aprobată cu modificări și completări de Legea nr. 124/2025. | tehnologiei informațiilor și comunicațiilor prevăzute la art. 36 alin. (5) și (6) din Ordonanța 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. | în cadrul activităților legitime de cercetare a vulnerabilităților.<br><br>Astfel, în practică, stabilirea existenței unei vulnerabilități poate presupune realizarea unor conexiuni la sisteme informatice și interacțiunea cu acestea, ceea ce poate conduce, în mod automat, la recepționarea sau transferul unor date, fără ca aceste acțiuni să constituie scopul în sine al activității desfășurate.<br><br>De asemenea, identificarea și testarea vulnerabilităților implică utilizarea unor proceduri și programe specializate, fără de care detectarea acestora nu este posibilă, aceste activități fiind inerente domeniului securității cibernetice.<br><br>În aceste condiții, incriminarea acestor conduite, în absența unei delimitări bazate pe scopul legitim al cercetării și pe respectarea condițiilor legale privind raportarea vulnerabilităților, ar avea ca efect descurajarea activităților de securitate cibernetică desfășurate cu bună-credință. |