PARLAMENTUL ROMÂNIEI

S E N A T

L E G E

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

Senatul adoptă prezentul proiect de lege

Art.I.- 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, cu completările ulterioare, se completează după cum urmează:

1. La articolul 24 alineatul (4), după litera g) se introduce o nouă literă, lit.h), cu 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. 36^1 și în limita creditelor bugetare aprobate cu această destinație."

2. După articolul 36 se introduce un nou articol, art.36^1, cu următorul cuprins:

„Art.36^1.- (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.

(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 efectua testarea și precizează limitele acesteia.

(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.(1^1) privind consultarea comitetului consultativ.

(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.

(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 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.

(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;

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.

(9) Participarea la programele prevăzute la alin.(1) este voluntară și nu creează obligația participantului de a efectua activități de testare ori de a obține un anumit rezultat."

Art.II.- 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.36[1] 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, cu completările ulterioare, 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.

Acest proiect de lege a fost adoptat de Senat în şedinţa din 2 noiembrie 2026, cu respectarea prevederilor articolului 76 alineatul (2) din Constituţia României, republicată.

PREŞEDINTELE SENATULUI

MIRCEA ABRUDEAN