EXPUNERE DE MOTIVE

Digitalizarea administraţiei publice a făcut ca furnizarea unor servicii esenţiale pentru cetăţeni şi mediul economic să depindă direct de disponibilitatea şi securitatea sistemelor informatice ale statului. Exploatarea unei singure vulnerabilităţi poate întrerupe servicii publice, poate bloca activitatea unei instituţii, poate compromite date şi poate genera cheltuieli importante pentru investigarea incidentului, refacerea infrastructurii şi reluarea activităţii. În acest context, existenţa unor mecanisme eficiente de identificare şi remediere timpurie a vulnerabilităţilor reprezintă o necesitate imediată pentru protejarea interesului public.

Ordonanţa de urgenţă a Guvernului nr. 155/2024 desemnează Directoratul Naţional de Securitate Cibernetică, denumit în continuare DNSC, drept autoritate competentă la nivel naţional şi coordonator al procesului de divulgare coordonată a vulnerabilităţilor. DNSC poate primi şi evalua raportări, poate verifica vulnerabilităţi şi poate intermedia relaţia dintre raportor şi entitatea afectată. Legea nr. 124/2025 a consolidat obligaţiile de raportare şi remediere, însă cadrul în vigoare nu conferă DNSC competenţa expresă de a organiza programe publice de identificare recompensată a vulnerabilităţilor şi nu prevede temeiul bugetar necesar pentru plata recompenselor. În prezent, DNSC poate gestiona o vulnerabilitate care îi este raportată, dar nu poate invita în mod organizat cercetători în securitate cibernetică să testeze, în limite stabilite în prealabil, sisteme informatice publice şi să îi recompenseze pentru vulnerabilităţile validate. Această lacună legislativă limitează capacitatea statului de a preveni incidente de securitate înainte ca acestea să producă efecte.

Necesitatea intervenţiei legislative trebuie analizată şi în contextul geopolitic actual. Conflictul armat din proximitatea României a fost însoţit de folosirea atacurilor cibernetice ca instrument de perturbare, presiune şi sabotaj. Chiar preambulul OUG nr. 155/2024 menţionează atacul asupra reţelei KA-SAT, acţiunile grupării Killnet împotriva unor infrastructuri din România şi incidentul care a afectat 26 de spitale prin compromiterea unui furnizor de servicii. Potrivit ENISA Threat Landscape 2025, administraţia publică a reprezentat 38,2% dintre incidentele analizate la nivelul Uniunii Europene, fiind sectorul cel mai vizat de atacuri. Persistenţa acestui nivel ridicat de risc impune adoptarea cu celeritate a unor instrumente suplimentare de prevenţie.

Atacul cibernetic asupra ANCPI a scos din funcţiune sistemul e-Terra şi serviciile de cadastru, blocând tranzacţii imobiliare, credite şi activitatea notarială. Pentru un singur cumpărător, amânarea tranzacţiei înaintea modificării TVA putea genera un cost suplimentar considerabil. Statul a suportat, în paralel, costurile izolării sistemelor, intervenţiei tehnice, migrării aplicaţiilor şi reluării serviciilor. Prin comparaţie, programul „Hack the Pentagon" a

costat 150.000 de dolari şi a identificat 138 de vulnerabilităţi, în timp ce o testare convenţională similară fusese estimată la peste un milion de dolari. Un program Bug Bounty are un buget plafonat, dar indisponibilitatea unui sistem public produce costuri în lanţ, considerabil mai mari. În lipsa unui cadru legal care să permită organizarea unor astfel de programe, vulnerabilităţile pot rămâne neidentificate până la exploatarea lor de către actori rău intenţionaţi.

Programele de tip Bug Bounty reprezintă mecanisme controlate prin care cercetătorii în securitate cibernetică sunt autorizaţi să testeze numai sistemele incluse expres în program şi pot primi recompense pentru vulnerabilităţile reale, raportate responsabil şi validate. Astfel de programe sunt utilizate de autorităţi publice din Statele Unite ale Americii, Singapore, Franţa, Elveţia, Olanda, Belgia, Regatul Unit şi Coreea de Sud.

Programele propuse nu înlocuiesc auditurile de securitate, testele de penetrare, monitorizarea continuă, copiile de rezervă sau planurile de continuitate. Ele completează aceste măsuri prin implicarea unui număr mai mare şi mai divers de specialişti. Recompensa se acordă numai pentru o vulnerabilitate validată, iar valoarea maximă a recompensei şi fondul total al programului se stabilesc înaintea lansării. Cheltuiala publică este astfel previzibilă, plafonată şi condiţionată de rezultat.

Propunerea legislativă conferă DNSC competenţa de a iniţia, organiza şi administra programe de identificare şi raportare recompensată a vulnerabilităţilor pentru reţelele şi sistemele informatice deţinute, administrate ori utilizate de autorităţi, instituţii publice şi alte entităţi de drept public. Pentru sistemele care nu aparţin DNSC, programul va putea fi organizat numai cu acordul prealabil, expres şi scris al entităţii competente. Totodată, se creează temeiul necesar pentru includerea în bugetul DNSC a cheltuielilor privind organizarea programelor şi plata recompenselor, în limita creditelor bugetare aprobate cu această destinaţie în bugetul de venituri şi cheltuieli al DNSC.

Activităţile de testare vor fi autorizate numai în prealabil, expres, limitat şi condiţionat, exclusiv pentru sistemele, perioada şi metodele prevăzute de regulile programului. Nu vor putea fi autorizate atacurile brute-force, phishingul, ingineria socială, utilizarea de malware, afectarea disponibilităţii serviciilor, ştergerea sau modificarea datelor, menţinerea accesului ori extinderea acestuia către alte sisteme sau conturi. Depăşirea limitelor programului va determina pierderea dreptului la recompensă, fără a înlătura răspunderea civilă, contravenţională sau penală.

Detaliile privind iniţierea programelor, selectarea sistemelor, condiţiile de participare, validarea vulnerabilităţilor, stabilirea şi plata recompenselor, protecţia datelor, confidenţialitatea, controlul şi suspendarea programelor vor fi reglementate prin hotărâre a Guvernului, la propunerea DNSC.

Având în vedere necesitatea consolidării fără întârziere a capacității de prevenire a incidentelor de securitate cibernetică și eliminării vidului normativ existent, adoptarea prezentei propuneri legislative în procedură de urgență este justificată de interesul public major privind asigurarea continuității serviciilor publice și protejarea infrastructurilor digitale ale statului.

Prin această intervenție punctuală, statul român va putea utiliza, într-un cadru legal, controlat și transparent, competențele cercetătorilor în securitate cibernetică pentru a descoperi vulnerabilitățile înainte ca acestea să fie exploatate de actori rău intenționați.

Având în vedere argumentele prezentate mai sus, înaintăm Parlamentului României, spre dezbatere și adoptare, prezenta propunere legislativă, în procedură de urgență.

Pentru inițiatori,

Oprea Octavian, deputat PNL

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătura
1.	Oprea Octavian	PNL	
2.	ȚIPLEA DUMITRU	PNL	
3	COZMA ADRIAN	PNL	
4	CĂDAR RĂZVAN	PNL	
5	Crușoveanu Marian	PNL	
6	Teșelariu Andrei - Ionuț	PNL	
7	Mircea Fechet	PNL	
8	Bogdan Huțucă	PNL	
9	Pardea Cyprian	PNL	

ROMANIA

PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAŢILOR SENATUL

LEGE

pentru completarea Ordonanţei de urgenţă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil

Parlamentul României adoptă prezenta lege.

Articol unic – Ordonanţa de urgenţă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil, publicată în Monitorul Oficial al României, Partea I, nr. 1332 din 31 decembrie 2024, aprobată cu modificări şi completări prin Legea nr. 124/2025, cu modificările şi 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 şi gestionarea programelor de identificare şi raportare a vulnerabilităţilor cu recompensarea persoanelor respective, conform art. 36^1, inclusiv prin acordarea de recompense băneşti pentru vulnerabilităţile validate."

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

„ **Art. 36^1 - (1)** DNSC poate iniţia şi gestiona programe de identificare şi raportare recompensată a vulnerabilităţilor pentru reţelele şi sistemele informatice proprii, precum şi pentru cele deţinute, administrate ori utilizate de autorităţi şi instituţii publice sau de alte entităţi de drept public din spaţiul cibernetic naţional civil, cu respectarea excluderilor şi regimurilor speciale prevăzute la art. 2.

(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.

(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) 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.

(5) 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."

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (2) din Constituția României, republicată.

PREȘEDINTELE	**PREȘEDINTELE**
CAMEREI DEPUTAȚILOR	**SENATULUI**