EXPUNERE DE MOTIVE

1. Contextul și situația actuală

La nivelul Uniunii Europene există deja mecanisme și instrumente dedicate raportării și gestionării vulnerabilităților de securitate cibernetică, inclusiv în cadrul implementării Directivei (UE) 2022/2555 (NIS 2), care stabilesc obligații clare pentru operatori și autorități competente. Un astfel de instrument este **European Union Vulnerability Database**, care oferă un cadru comun pentru colectarea și analiza informațiilor privind vulnerabilitățile cibernetice.

În plan național, Ordonanța de urgență a Guvernului nr. 155/2024 creează cadrul general pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, stabilind atribuțiile Directoratului Național de Securitate Cibernetică (DNSC), în calitate de autoritate competentă responsabilă cu securitatea cibernetică, precum și cu sarcinile de supraveghere și asigurare a respectării măsurilor necesare pentru atingerea unui nivel comun ridicat de securitate cibernetică. Totodată, actul normativ stabilește competențe și responsabilități pentru alte entități de drept public sau privat implicate în aplicarea dispozițiilor ordonanței.

Cu toate acestea, legislația în vigoare nu reglementează în mod expres un **mecanism structurat de consultare interinstituțională**, care să permită:

- analiza coordonată a vulnerabilităților raportate de instituții publice, operatori sau persoane terțe;
- facilitarea comunicării între autoritățile cu atribuții în domeniul securității și apărării cibernetice;
- asigurarea unei abordări unitare și coerente în aplicarea obligațiilor prevăzute de lege.

De asemenea, persistă o **incertitudine juridică** în ceea ce privește activitățile de cercetare și raportare a vulnerabilităților realizate cu bună-credință, în raport cu dispozițiile Codului penal referitoare la accesul neautorizat la sisteme informatice.

La nivelul Uniunii Europene, există câteva țări, precum Belgia, Portugalia sau Franța, care au introdus dispoziții legale de protecție de tip "safe harbour" pentru cercetători în securitate IT, care pot reduce sau elimina răspunderea penală pentru hacking în scop de cercetare dacă sunt respectate condiții stricte.

2. Scopul și obiectivele proiectului de lege

Proiectul de lege are ca obiectiv principal **îmbunătățirea mecanismelor de cooperare, analiză și comunicare** în domeniul securității cibernetice, fără a dubla sau suprapune instrumentele existente la nivel european.

În acest sens, proiectul urmărește:

- instituționalizarea unui **comitet de consultare**, coordonat de DNSC, format din autoritățile prevăzute la art. 11–12 și art. 14–17 din Legea nr. 58/2023 privind

securitatea şi apărarea cibernetică a României, care să sprijine DNSC în îndeplinirea atribuţiilor sale legale;

- asigurarea unui cadru organizat pentru:
  - analiza vulnerabilităţilor transmise de instituţii publice, operatori sau persoane terţe;
  - schimbul de informaţii relevante între autorităţile competente;
  - facilitarea comunicării necesare aplicării coerente a prevederilor legii;
- clarificarea cadrului juridic aplicabil cercetării şi raportării vulnerabilităţilor produselor sau serviciilor TIC, prin introducerea unei prevederi în Codul penal, în condiţiile strict reglementate de legislaţia specială.

3. Descrierea soluţiilor propuse

Proiectul de lege propune:

- completarea art. 36 din Ordonanţa de urgenţă nr. 155/2024 prin introducerea unui nou alineat, care stabileşte obligaţia DNSC de a se consulta cu un **comitet interinstituţional**, 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;
- 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.

Prin proiectul propus faptele prevăzute în art. 360 – 365 din Codul Penal nu constituie infracţiune dacă persoana fizică sau juridică care raportează respectă cel puţin următoarele:

a) activitatea de cercetare pentru descoperirea de vulnerabilităţii raportate se efectuează cu bună-credinţă, exclusiv cu scopul de a contribui la îmbunătăţirea securităţii cibernetice şi cu respectarea prevederilor legale;
b) activitatea de cercetare se desfăşoară fără accesarea sau copierea neautorizată a conţinutului fişierelor din sistemele informatice care fac obiectul activităţii de cercetare;
c) în cadrul activităţii de cercetare nu sunt şterse sau modificate date din sistemele informatice care fac obiectul activităţii de cercetare;
d) activitatea de cercetare se desfăşoară 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;
e) nu se cauzează nicio întrerupere sau deteriorare a produselor sau serviciilor TIC ale terţilor;
f) activitatea de cercetare nu se desfăşoară pentru a derula atacuri, nu produce prejudicii şi nu utilizează produse de tip malware sau tehnici de natură să afecteze disponibilitatea serviciilor TIC;
g) nu a dezvăluit public informaţii cu privire la vulnerabilitatea identificată, anterior sau ulterior momentului raportării, fără acordul DNSC.

De asemenea, raportarea trebuie să fie realizată în termen de cel mult 48 de ore de la identificarea vulnerabilităţii.

4. Impactul asupra sistemului de securitate cibernetică

Adoptarea proiectului de lege va conduce la:

- consolidarea cooperării interinstituționale în domeniul securității cibernetice;
- creșterea capacității de analiză și reacție la vulnerabilități complexe;
- reducerea riscurilor generate de fragmentarea informațiilor și de lipsa coordonării;
- încurajarea raportării responsabile a vulnerabilităților de către specialiști și terți, în condiții de predictibilitate juridică.

5. Impactul asupra sistemului juridic și bugetar

Proiectul de lege nu generează impact bugetar suplimentar, întrucât comitetul funcționează în cadrul instituțional existent, fără crearea unor structuri permanente noi sau alocări bugetare distincte.

Din punct de vedere juridic, se asigură o mai bună corelare între legislația specială în domeniul securității cibernetice și normele de drept penal, contribuind la eliminarea riscului interpretărilor neunitare.

6. Concluzii

Prin instituirea unui mecanism de consultare interinstituțională și prin clarificarea regimului juridic al cercetării și raportării vulnerabilităților, proiectul de lege contribuie la consolidarea rezilienței cibernetice a României, în deplină concordanță cu cadrul european existent și fără suprapunerea instrumentelor deja funcționale la nivelul Uniunii Europene.

Pentru inițiatori,
PRUNĂ Cristina-Mădălina, deputat USR
MITITELU Eduard-Tatian, deputat PNL

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

Nr. crt.	Nume Prenume	Grup parlamentar	Semnătura
1	MITITELU EDUARD-TATIAN	PNL	
2	Raluca Turcan	PNL	
3	MĂCUȚĂ SORIN	PNL	
4	CIOBOTARIU DRAGOȘ	PNL	
5	MATEI ANETA.	PNL.	
6	STĂNESCU VICTOR	PNL	
7	GEORGE SCARLAT	PNL	
8	RUSU SEBASTIAN	PNL	
9	Oprea Octavian	PNL	
10	BORȘ MĂDĂLIN	PSD	
11	Sebastian Burduja	PNL	
12	LONGHER GHERVASEN	MIN	
13	LAZĂR TEODOR	USR	
14	ALECSANDRU HARIUS-NICOLAE	USR	
15	TAIMOSĂ ȘTEFAN	USR	
16	WIENER ADRIAN	USR	
17	DRĂGOESCU CEZAR	USR	
18	NASUI CĂUNIU	USR	
19	PRUNĂ CRISTINA	USR	

20	Constantinescu Sergiu	PNL	
21	TOMA ILIE	PSD	
22	Manta Claudiu	PSD	
23	COLESNICHE-TZIU	PUR	
24	BARSTAN TIBERIU	PUR	
25	Cav Ilyes Florin	AUR	
26	Bende Sandor	UDMR	
27	JITARU OVIDIU	PNL	
28	PRISCA RAZVAN	PNL	
29	Paraschivescu Catalin	USR	
30	Radu Mihai	USR	
31	GIURGIU ADRIAN	USR	
32	GAL KAROLY	UDMR	
33			
34			
35			
36			
37			
38			
39			
40			
41			
42			
43			
44			
45			