

EXPUNERE DE MOTIVE

LEGE

pentru modificarea articolului 3 din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei

Secțiunea 1. Titlul proiectului de act normativ

Lege pentru modificarea articolului 3 din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei.

Secțiunea a 2-a. Motivul emiterii actului normativ

2.1. Descrierea situației actuale

Legea nr. 354/2022 a interzis autorităților și instituțiilor publice achiziționarea, instalarea și utilizarea produselor și serviciilor software de tip antivirus și a celorlalte produse de securitate prevăzute la art. 2, provenind, direct sau indirect, din Federația Rusă ori de la entități aflate sub control rusesc. Potrivit art. 3, interdicția se aplică până la data de 31 decembrie 2026.

Federația Rusă conduce, de la 24 februarie 2022, un război de agresiune împotriva Ucrainei, cu încălcarea gravă a Cartei Organizației Națiunilor Unite, a suveranității și a integrității teritoriale a unui stat vecin. Adunarea Generală a ONU a condamnat agresiunea și a cerut retragerea necondiționată a trupelor ruse, prin Rezoluția ES-11/1 din 2 martie 2022, adoptată cu 141 de voturi pentru.¹

Parlamentul European a recunoscut Federația Rusă drept stat sponsor al terorismului și stat care folosește mijloace teroriste.² Curtea Penală Internațională a emis, la 17 martie 2023, mandat de arestare pe numele președintelui Federației Ruse, pentru deportarea ilegală de copii ucraineni.³ Federația Rusă este principala amenințare la adresa securității naționale a României, a Uniunii Europene și a Alianței Nord-Atlantice. Ea încalcă sistematic dreptul internațional și trebuie sancționată prin toate mijloacele legale și izolată economic, politic, diplomatic și tehnologic de comunitatea statelor democratice.

Agresiunea rusă se desfășoară constant și în spațiul cibernetic, unde autoritățile statelor membre ale Uniunii Europene și ale NATO, infrastructurile lor critice și sectoarele de apărare sunt ținte permanente. Exemplele documentate public arată amploarea, persistența și gravitatea acestor operațiuni.

¹Adunarea Generală a Organizației Națiunilor Unite, Rezoluția ES-11/1 din 2 martie 2022, adoptată cu 141 de voturi pentru, 5 împotriva și 35 de abțineri. Disponibilă la: <https://docs.un.org/en/A/RES/ES-11/1>

²Parlamentul European, Rezoluția din 23 noiembrie 2022 privind recunoașterea Federației Ruse drept stat sponsor al terorismului, adoptată cu 494 de voturi pentru. Disponibilă la: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0405_EN.html

³Curtea Penală Internațională, mandate de arestare emise la 17 martie 2023 în situația din Ucraina. Disponibil la: <https://www.icc-cpi.int/news/situation-ukraine-icc-judges-issue-arrest-warrants-against-vladimir-vladimirovich-putin-and>

La 24 februarie 2022, cu o oră înainte de invazie, un atac cibernetic cu programul distructiv AcidRain a lovit rețeaua de comunicații prin satelit KA-SAT, operată de Viasat. Atacul a afectat zeci de mii de utilizatori din Ucraina și din Europa și a întrerupt monitorizarea la distanță a circa 5.800 de turbine eoliene Enercon din Germania. Uniunea Europeană, Statele Unite și Regatul Unit au atribuit oficial atacul Federației Ruse.⁴

În octombrie 2022, gruparea Sandworm, atribuită Direcției Principale de Informații a Statului Major al forțelor armate ruse (GRU), a desfășurat atacuri cu programul de tip ransomware „Prestige” împotriva companiilor din sectorul transporturilor și logisticii din Polonia și Ucraina, urmărind blocarea fluxului de aprovizionare către Ucraina.⁵

În mai 2024, Uniunea Europeană, NATO și statele afectate au condamnat campania grupării APT28, controlată de GRU, îndreptată împotriva Germaniei, inclusiv a partidului cancelarului federal, și a Cehiei, precum și împotriva unor instituții guvernamentale și operatori de infrastructură critică din Lituania, Polonia, Slovacia și Suedia.⁶

România este țintă directă. În perioada 29 aprilie - 1 mai 2022, gruparea pro-rusă Killnet a desfășurat atacuri de tip DDoS care au scos din funcțiune site-urile Ministerului Apărării Naționale, Poliției de Frontieră, Guvernului României și ale companiei CFR, precum și ale unor aeroporturi și ale companiei TAROM, ca represalii pentru sprijinul acordat Ucrainei.⁷

În toamna anului 2024, infrastructura electorală a României a fost ținta a peste 85.000 de atacuri cibernetice în perioada premergătoare alegerilor prezidențiale. Atacurile, evaluate de autorități drept operațiunea unui actor statal cu legături cu Federația Rusă, au vizat sistemele Autorității Electorale Permanente, iar date de acces au fost publicate pe platforme rusești. Documentele Consiliului Suprem de Apărare a Țării au fost declassificate, iar Curtea Constituțională a anulat procesul electoral prezidențial la 6 decembrie 2024.⁸

2.2. Schimbări preconizate

Prezenta propunere legislativă modifică articolul 3 din Legea nr. 354/2022, prelungind termenul de aplicare a interdicției de la 31 decembrie 2026 la 31 decembrie 2035.

⁴Consiliul Uniunii Europene, declarația Înaltului Reprezentant din 10 mai 2022 privind operațiunile cibernetice ruse împotriva Ucrainei, inclusiv atacul asupra rețelei KA-SAT. Disponibilă la: <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/>

⁵Microsoft Security, „New Prestige ransomware impacts organizations in Ukraine and Poland”, 14 octombrie 2022. Disponibil la: <https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/>

⁶Condamnarea campaniei grupării APT28 (GRU) împotriva Germaniei și Cehiei de către Uniunea Europeană, NATO și statele afectate, mai 2024. A se vedea: <https://www.aljazeera.com/news/2024/5/3/germany-accuses-russia-of-intolerable-cyberattack-warns-of-consequences>

⁷Atacuri de tip DDoS revendicate de gruparea pro-rusă Killnet împotriva instituțiilor publice din România, 29 aprilie - 1 mai 2022. A se vedea: <https://www.romania-insider.com/romania-cyberattack-russia-killnet-2022>

⁸Atacuri cibernetice asupra infrastructurii electorale a României în 2024 și anularea procesului electoral prezidențial de către Curtea Constituțională la 6 decembrie 2024. A se vedea: <https://www.rferl.org/a/romania-russia-election-interference-tiktok/33227010.html>

Prelungirea este necesară și proporțională. Cauzele care au justificat adoptarea legii nu numai că persistă, ci s-au agravat. La împlinirea termenului actual, interdicția ar înceta, iar autoritățile și instituțiile publice ar putea reintroduce în sistemele lor informatice produse și servicii controlate de un stat agresor, contrar scopului prevăzut la art. 1 alin. (5). Termenul de 31 decembrie 2035 asigură un orizont de protecție stabil, pe durata previzibilă a amenințării.

2.3. Alte informații

Întrucât termenul prevăzut la art. 3 expiră la 31 decembrie 2026, adoptarea propunerii are caracter urgent, pentru a se asigura continuitatea protecției înainte de ieșirea din vigoare a interdicției.

Secțiunea a 3-a. Impactul socioeconomic al proiectului de act normativ

Impactul macroeconomic: menținerea interdicției reduce riscul de compromitere a sistemelor informatice ale statului și de întrerupere a serviciilor publice esențiale.

Impactul asupra mediului de afaceri: propunerea nu produce efecte asupra mediului de afaceri, întrucât se adresează exclusiv autorităților și instituțiilor publice.

Impactul social: propunerea protejează datele cetățenilor gestionate de autoritățile și instituțiile publice.

Impactul asupra mediului înconjurător: propunerea nu are impact asupra mediului.

Secțiunea a 4-a. Impactul financiar asupra bugetului general consolidat

Propunerea nu generează cheltuieli suplimentare față de bugetul general consolidat, nici pe termen scurt, pentru anul curent, nici pe termen lung, pe următorii 5 ani. Propunerea menține un regim juridic deja aplicat de autoritățile și instituțiile publice, fără a institui obligații noi de cheltuială.

Secțiunea a 5-a. Efectele proiectului de act normativ asupra legislației în vigoare

Propunerea modifică un singur articol, art. 3, din Legea nr. 354/2022 și nu produce efecte asupra altor acte normative.

Menținerea măsurii este compatibilă cu dreptul Uniunii Europene. Ea se întemeiază pe protejarea intereselor esențiale de securitate ale statului, în sensul art. 4 alin. (2) din Tratatul privind Uniunea Europeană și al art. 36 și 346 din Tratatul privind funcționarea Uniunii Europene, în coordonare cu măsurile restrictive ale Uniunii adoptate prin Regulamentul (UE) nr. 833/2014.

Propunerea se supune avizului Consiliului Legislativ.

Secțiunea a 6-a. Consultările efectuate în vederea elaborării proiectului de act normativ

Nu este cazul.

Secțiunea a 7-a. Activități de informare publică privind elaborarea și implementarea proiectului de act normativ

Propunerea legislativă urmează procedura de dezbatere și adoptare din Parlamentul României, care asigură informarea publică.

Secțiunea a 8-a. Măsuri privind implementarea, monitorizarea și evaluarea proiectului de act normativ

Propunerea nu necesită structuri noi de implementare. Aplicarea și monitorizarea se realizează prin mecanismele existente, prevăzute de Legea nr. 354/2022, de către Ministerul Economiei, Digitalizării, Antreprenoriatului și Turismului și Directoratul Național de Securitate Cibernetică.

În numele inițiatorilor,

Sebastian-Ioan Burduja

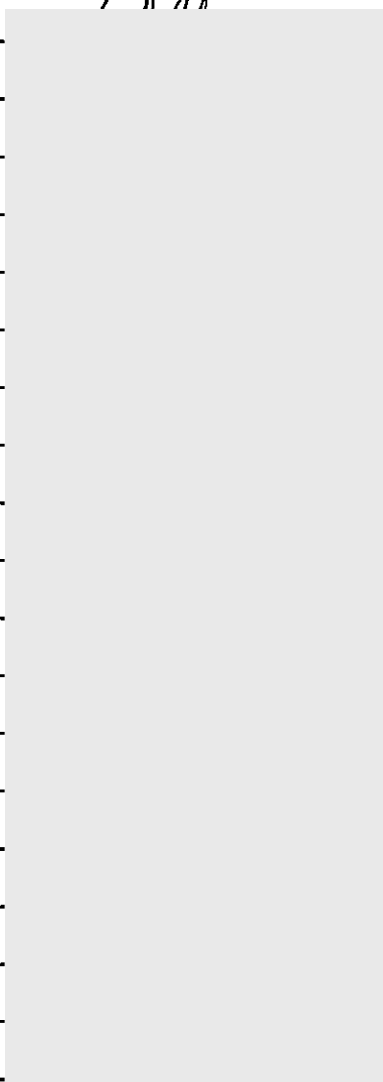
Deputat PNL.



Tabel susținători

LEGE

pentru modificarea articolului 3 din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei

Nr. crt.	Nume și prenume	Grup parlamentar	Semnătură
1	Ciprian Zobre	PNL	
2	CIOBANU ADRIAN	PNL	
3	OPREA OCTAVIAN	PNL	
4	CRUSOVEANU HARIAN	PNL	
5	CIMPEAN OVIDIU	PNL	
6	GEAM CALIN	P.N.L.	
7	COTINESCU AURELIAN	PNL	
8	CADAR RAZVAN	PNL	
9	PISTRU POPA OCEANINA	PNL	
10	PELU MARIU MANOLE	PSD	
11	DETINARIU EUGEN	PSD	
12	PRUNA CRISTINA	USR	
13	RADU MIHAIL	USR	
14	GABRIEL ANDRONACHE	PNL	
15	VELA ION MARCEL	PNL	
16	ZICOPOL DRAGOS	MIȚOPRITAI	
17	COLEȘA IULIAN	AUR	
18	MIRCEA FECHET	PNL	
			/