EXPUNERE DE MOTIVE

LEGE

pentru modificarea articolului 3 din Legea nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei

Secţiunea 1. Titlul proiectului de act normativ

Lege pentru modificarea articolului 3 din Legea nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei.

Secţiunea a 2-a. Motivul emiterii actului normativ

2.1. Descrierea situaţiei actuale

Legea nr. 354/2022 a interzis autorităţilor şi instituţiilor publice achiziţionarea, instalarea şi utilizarea produselor şi serviciilor software de tip antivirus şi a celorlalte produse de securitate prevăzute la art. 2, provenind, direct sau indirect, din Federaţia Rusă ori de la entităţi aflate sub control rusesc. Potrivit art. 3, interdicţia se aplică până la data de 31 decembrie 2026.

Federaţia Rusă conduce, de la 24 februarie 2022, un război de agresiune împotriva Ucrainei, cu încălcarea gravă a Cartei Organizaţiei Naţiunilor Unite, a suveranităţii şi a integrităţii teritoriale a unui stat vecin. Adunarea Generală a ONU a condamnat agresiunea şi a cerut retragerea necondiţionată a trupelor ruse, prin Rezoluţia ES-11/1 din 2 martie 2022, adoptată cu 141 de voturi pentru.[1]

Parlamentul European a recunoscut Federaţia Rusă drept stat sponsor al terorismului şi stat care foloseşte mijloace teroriste.[2] Curtea Penală Internaţională a emis, la 17 martie 2023, mandat de arestare pe numele preşedintelui Federaţiei Ruse, pentru deportarea ilegală de copii ucraineni.[3] Federaţia Rusă este principala ameninţare la adresa securităţii naţionale a României, a Uniunii Europene şi a Alianţei Nord-Atlantice. Ea încalcă sistematic dreptul internaţional şi trebuie sancţionată prin toate mijloacele legale şi izolată economic, politic, diplomatic şi tehnologic de comunitatea statelor democratice.

Agresiunea rusă se desfăşoară constant şi în spaţiul cibernetic, unde autorităţile statelor membre ale Uniunii Europene şi ale NATO, infrastructurile lor critice şi sectoarele de apărare sunt ţinte permanente. Exemplele documentate public arată amploarea, persistenţa şi gravitatea acestor operaţiuni.

---

[1]Adunarea Generală a Organizaţiei Naţiunilor Unite, Rezoluţia ES-11/1 din 2 martie 2022, adoptată cu 141 de voturi pentru, 5 împotrivă şi 35 de abţineri. Disponibilă la: https://docs.un.org/en/A/RES/ES-11/1

[2]Parlamentul European, Rezoluţia din 23 noiembrie 2022 privind recunoaşterea Federaţiei 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

[3]Curtea Penală Internaţională, mandate de arestare emise la 17 martie 2023 în situaţia 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 reţeaua de comunicaţii prin satelit KA-SAT, operată de Viasat. Atacul a afectat zeci de mii de utilizatori din Ucraina şi din Europa şi a întrerupt monitorizarea la distanţă a circa 5.800 de turbine eoliene Enercon din Germania. Uniunea Europeană, Statele Unite şi Regatul Unit au atribuit oficial atacul Federaţiei Ruse.[4]

În octombrie 2022, gruparea Sandworm, atribuită Direcţiei Principale de Informaţii a Statului Major al forţelor armate ruse (GRU), a desfăşurat atacuri cu programul de tip ransomware „Prestige" împotriva companiilor din sectorul transporturilor şi logisticii din Polonia şi Ucraina, urmărind blocarea fluxului de aprovizionare către Ucraina.[5]

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

România este ţintă directă. În perioada 29 aprilie - 1 mai 2022, gruparea pro-rusă Killnet a desfăşurat atacuri de tip DDoS care au scos din funcţiune site-urile Ministerului Apărării Naţionale, Poliţiei de Frontieră, Guvernului României şi ale companiei CFR, precum şi ale unor aeroporturi şi ale companiei TAROM, ca represalii pentru sprijinul acordat Ucrainei.[7]

În toamna anului 2024, infrastructura electorală a României a fost ţinta a peste 85.000 de atacuri cibernetice în perioada premergătoare alegerilor prezidenţiale. Atacurile, evaluate de autorităţi drept operaţiunea unui actor statal cu legături cu Federaţia Rusă, au vizat sistemele Autorităţii Electorale Permanente, iar date de acces au fost publicate pe platforme ruseşti. Documentele Consiliului Suprem de Apărare a Ţării au fost declasificate, iar Curtea Constituţională a anulat procesul electoral prezidenţial 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 interdicţiei de la 31 decembrie 2026 la 31 decembrie 2035.

---

[4]Consiliul Uniunii Europene, declaraţia Înaltului Reprezentant din 10 mai 2022 privind operaţiunile cibernetice ruse împotriva Ucrainei, inclusiv atacul asupra reţelei 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/

[5]Microsoft 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/

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

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

[8]Atacuri cibernetice asupra infrastructurii electorale a României în 2024 şi anularea procesului electoral prezidenţial de către Curtea Constituţională 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.

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

Nu este cazul.

Secţiunea a 7-a. Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ

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

Secţiunea a 8-a. Măsuri privind implementarea, monitorizarea şi evaluarea proiectului de act normativ

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

În numele iniţiatorilor,

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	Semnătura
1	Ciprian Dobre	PNL	
2	CIOBANU ADRIAN	PNL	
3	Oprea Octavian	PNL	
4	Cusoveanu Marian	PNL	
5	CIMPEAN OVIDIU	PNL	
6.	Gal Călin	P.N.L.	
7	Cotnescu Aurelian	PNL	
8	CADAR RAZVAN	PNL	
9.	PISTRU-POPA OEANINA	PNL.	
10	Petru Florin Manole	PSD	
11	BEJINARIU EUGEN	PSD	
12	PRUNĂ CRISTINA	USR	
13	Radu Mihai	USR	
14	GABRIEL ANDRONACHE	PNL	
15	Vela Ion Marcel	PNL	
16	ZICOPOL DRAGOS	MINORITATI	
17	COLEȘA ILIE-NIN	AUR	
18	MIRCEA FECHET	PNL	

CAMERA DEPUTAȚILOR **SENAT**

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

Parlamentul României adoptă prezenta lege.

Articol unic. Articolul 3 din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei, publicată în Monitorul Oficial al României, Partea I, nr. 1200 din 14 decembrie 2022, se modifică și va avea următorul cuprins:

„Art. 3

Interdicția prevăzută la art. 2 se aplică până la data de 31 decembrie 2035.„

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