



Lege

privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei

Parlamentul României adoptă prezenta lege.

Art. 1.

- (1) Prezenta lege stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare, în vederea interzicerii achiziționării și utilizării de către autoritățile și instituțiile publice, de la nivel central și local, a produselor și serviciilor privind securitatea dispozitivului (securitatea punctului final), aplicații și programe software de detecție antivirus, anti-malware, firewall pentru aplicații web (Web Application Firewall), rețele virtuale private (Virtual Private Network), precum și sisteme de detecție și răspuns pentru endpointuri (Endpoint Detection Response) provenind din Federația Rusă sau aflată sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă.
- (2) În aplicarea prevederilor alin. (1), ministrul cercetării, inovării și digitalizării adoptă o listă nominală privind produsele, serviciile și entitățile producătoare și furnizoare interzise.

Art. 2.

Interdicția prevăzută la art. 1 produce efecte pe întreaga durată a invaziei declanșată de Federația Rusă împotriva Ucrainei, până la data semnării unui tratat de pace sau a unui acord permanent de armistițiu care să consfințească integritatea teritorială a Ucrainei, reparații pentru prejudiciile suferite de țara invadată, precum și cooperarea Federației Ruse cu organismele naționale și internaționale competente pentru pedepsirea persoanelor care se fac vinovate de crime de război sau crime împotriva umanității.

Art. 3.

- (1) Nerespectarea de către autoritățile și instituțiile publice a prevederilor art. 1, alin. (1) art. 4, alin. (2) constituie contravenție și se sancționează cu amendă de la 50.000 și 200.000 lei.
- (2) Constatarea și aplicarea contravențiilor se face de către personal anume desemnat prin ordin al ministrului cercetării, inovării și digitalizării;

- (3) Dispozițiile prezentei legi se completează cu prevederile Ordonanței Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.

Art. 4.

- (1) În aplicarea prevederilor art. 1, alin. (2), ministrul cercetării, inovării și digitalizării adoptă un ordin în termen de maximum 15 zile de la intrarea în vigoare a prezentei legi.
- (2) În termen de 45 de zile de la intrarea în vigoare a prezentei legi, toate produsele și serviciile de tipul celor prevăzute la art. 1, alin. (1) sunt deconectate, respectiv dezinstalate de la rețelele și sistemele informatice ale autorităților și instituțiilor publice de la nivel central și local.
- (3) În aplicarea prevederilor art. 1, alin. (2), Ministerul Cercetării, Inovării și Digitalizării, cu sprijinul Autorității pentru Digitalizarea României, a Directoratului Național de Securitate Cibernetică, a Serviciului Român de Informații și a Serviciului de Telecomunicații Speciale, identifică produsele și serviciile prevăzute la art. 1, alin. (1) și sprijină autoritățile și instituțiile publice centrale și locale în vederea deconectării și dezinstalării acestora din rețelele și sistemele informatice.
- (4) În termen de 30 de zile de la adoptarea ordinului de ministru prevăzut la alin. (1), autoritățile și instituțiile publice demarează procedura de achiziționare a produselor și serviciilor de tipul celor prevăzute la art. 1, alin. (1) cu respectarea prevederilor prezentei legi.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (1) din Constituția României, republicată.

PRIM – MINISTRU

Nicolae-Ionel CIUCĂ

EXPUNERE DE MOTIVE

Secțiunea 1

Titlul proiectului de act normativ:

LEGE

privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei

1. Descrierea situației actuale

În contextul războiului de agresiune asupra Ucrainei, tot mai multe state membre ale Uniunii Europene au emis recomandări sau acte normative cu caracter imperativ prin care au impus propriilor lor autorități și instituții publice să schimbe soluțiile antivirus dacă le folosesc pe cele de la Kaspersky Lab, deoarece există riscul ca Rusia să exploateze aceste soft-uri într-un atac cibernetic.

Spre exemplu, Autoritatea germană BSI (Federal Office for Information Security) avertizează că riscul poate fi mai mare pentru companiile din domeniul infrastructurilor esențiale. BSI susține că ar fi bine ca toate companiile germane care folosesc soluții AV sau alte tipuri de soft-uri de la Kaspersky să renunțe la ele și să folosească programe de la alte companii. BSI explică faptul că soluțiile antivirus mențin o legătură permanentă, criptată și imposibil de verificat cu serverele vendor-ului, pentru o actualizare permanentă a definițiilor virușilor. Teama este că fișiere sensibile ar putea fi extrase de pe computerele care folosesc soluțiile companiei, pentru a fi trimise pe serverele Kaspersky și ale altor companii rusești¹.

În Italia, Franco Gabrielli, secretar de stat la președinția Consiliului de miniștri, a declarat în Senat că Guvernul de la Roma lucrează la un set de reguli care ar permite entităților de stat să înlăture programele software dezvoltate de firma rusă Kaspersky². Între timp, reglementările au fost adoptate astfel cum sunt descrise la secțiunea 5, pct. VI din prezenta expunere.

Potrivit unor informații publice apărute în presă³, Primăria municipiului București a organizat o licitație pentru achiziționarea unui antivirus Kaspersky Endpoint Security For Business-Select pentru 1.200 de echipamente, cu mentenanță inclusă 12 luni. Biroul de Presă al instituției primarului general a transmis că Primăria Capitalei folosește antivirusul Kaspersky din anul 2012 și nu a întâmpinat probleme din cauza acestui produs.

Există informații conform cărora foarte multe instituții publice și autorități ale administrației publice locale achiziționează programe software de antivirus rusești din cauza prețurilor mici și care au prevalență prin Sistemul informatic colaborativ pentru mediu performant de desfășurare al achizițiilor publice (SICAP).

Prezența software-urilor rusești de tip antivirus reprezintă o vulnerabilitate la adresa securității cibernetică a autorităților și instituțiilor românești, din cauză că aceste programe acaparează funcții importante ale rețelelor și sistemelor informatice, creând relații de interdependență. În contextul în care Federația Rusă utilizează inclusiv atacuri de tip cibernetic la adresa statelor occidentale și își folosește companiile naționale și cetățenii ruși, prin diverse metode, în războiul asupra Ucrainei, încălcând toate normele de drept internațional în materie, România nu poate să-și asume prezența unor produse și servicii IT rusești în infrastructura cibernetică națională.

Potrivit **Hotărârii Parlamentului României nr. nr. 22 din 30 iunie 2020 privind aprobarea Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024, obiectivele naționale de securitate vizează și ”asigurarea securității și protecției**

¹Disponibil la: <https://economie.hotnews.ro/stiri-it-25436103-germania-avertizeaza-software-kaspersky-lab-putea-exploatat-federatia-rusa-recomanda-companiilor-renunte.htm>; accesat la data de 10.05.2022.

²Disponibil la: <https://spotmedia.ro/stiri/it/italia-va-limita-utilizarea-antivirusului-kaspersky-in-sectorul-public-de-teama-ca-rusia-l-ar-folosi-pentru-atacuri-cibernetice>; accesat la data de 10.05.2022.

³Disponibil la: <https://stiripesurse.directorylib.com/primaria-capitaliei-vrea-antivirus-rusesc-declarat-amenintare-de-securitate-988775.html>; accesat la 10.05.2022.

infrastructurilor de comunicații și tehnologia informațiilor cu valențe critice pentru securitatea națională, precum și cunoașterea prevenirii și contracararea amenințărilor cibernetice derulate asupra acestora de către actori cu motivație strategică, de ideologie extremist-teroristă sau financiară. Redimensionarea și reconstrucția sistemului de comunicații, la nivel național, conform cerințelor de calitate internaționale, astfel încât zonele de eșec ale pieței (acolo unde operatorii consideră că nu este oportun să investească) să fie compensate prin infrastructuri de comunicații finanțate din fonduri publice”.

În aceeași strategie, la pct. 161, se reliefează ca **vulnerabilitate** ”nivelul redus de securitate cibernetică a infrastructurilor de comunicații și tehnologia informației din domenii strategice (inclusiv ca efect al vulnerabilităților tehnologice și procedurale ale infrastructurilor deținute de operatorii de comunicații) facilitează derularea de atacuri cibernetice de către actori statali sau non-statali”.

Din perspectiva **dimensiunii de informații, contrainformații și de securitate**, la pct. 179, Strategia își propune următoarele obiective:

”– Prevenirea și contracararea amenințărilor cibernetice - derulate de entități ostile, statale și nonstatale - asupra infrastructurilor de comunicații și tehnologia informației cu valențe critice pentru securitatea națională;

- Cresterea capacității instituțiilor publice, companiilor private și a organizațiilor neguvernamentale de a implementa norme de securitate cibernetică și de a-și forma personalul în vederea protecției datelor cu caracter personal, a datelor privind activitatea și rezultatele cercetării științifice și a altor date ce nu sunt de interes public;

– Prevenirea și contracararea amenințărilor hibride, concretizate în acțiuni conjugate ostile, derulate de actori statali sau nonstatali, în plan politico-administrativ, economic, militar, social, informațional, cibernetic sau al crimei organizate.”

În **Hotărârea Guvernului României nr. 1.321 din 30 decembrie 2021** privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027 se prevede, printre cele 5 obiective strategice, acela de a avea ”Rețele și sisteme informatice sigure și reziliente”.

Strategia prezintă o sinteză a tipurilor de atacuri cibernetice care au guvernat aparatul de stat în ultima perioadă, astfel:

„Atacurile cibernetice derulate de actori statali sunt de regulă de tip Advanced Persistent Threat (APT). Au un nivel tehnologic ridicat, atât în ceea ce privește modul de operare, cât și din punct de vedere al aplicațiilor malware folosite, actualizate permanent în vederea eludării mecanismelor de detecție și menținerii persistenței pentru o perioadă îndelungată de timp. Instrumentarul cibernetic folosit de atacatori este divers, adaptat scopurilor operaționale ale acestora.

Peisajul autohton a fost dominat în ultimii ani de atacuri cibernetice cu aplicații malware de tip ransomware, infostealer sau cryptojacking, care au vizat rețele și sisteme informatice aparținând unor autorități și instituții ale administrației publice sau entități private. De asemenea, se remarcă intensificarea atacurilor cibernetice din ce în ce mai complexe, inclusiv de tip APT, dedicate exploatării sistemelor informatice din domeniul financiar-bancar.”

Cu privire la obiectiv strategic de ”Rețele și sisteme informatice sigure și reziliente” acesta prevede o serie de măsuri, astfel: ”Pentru România este prioritară securitatea cibernetică a rețelilor și sistemelor informatice, îndeosebi a celor din domenii aferente serviciilor esențiale, precum și a celor cu valențe critice pentru securitatea națională. Menținerea în parametri optimi a disponibilității, continuității și integrității și asigurarea rezilienței acestora contribuie la susținerea în condiții optime a tuturor domeniilor vieții economice și sociale.

Autoritățile și instituțiile administrației publice și entitățile private trebuie să implementeze și să operationalizeze politici de securitate cibernetică adecvate. Acest deziderat presupune inclusiv realizarea de investiții în domeniul tehnologic și alocarea de resursă umană cu pregătire de specialitate. Totodată este necesară impunerea și respectarea unui set de standarde calitative pentru produsele și serviciile utilizate în cadrul acestor rețele și sisteme.

Măsuri:

4.1.1. Implementarea de politici și măsuri de securitate cibernetică

Pentru a putea avea rețele și sisteme informatice sigure este dezirabilă crearea și implementarea corectă, de către întregul personal al unei entități, a unui set minim de politici și măsuri de securitate cibernetică. Acestea trebuie să fie adaptabile, permanent corelate cu nivelul amenințării cibernetică și cu trendul rapid de dezvoltare al tehnologiilor.

De asemenea, aceste politici trebuie să fie însoțite de implementarea unor planuri de recuperare în caz de atac cibernetic și de măsuri tehnice și organizaționale, menite să contribuie la creșterea atât a capacității de reacție la atacuri și incidente de securitate cibernetică, cât și a rezilienței infrastructurilor.

În plus, este necesar ca fiecare operator de rețele și sisteme cu impact la adresa securității naționale, inclusiv cei desemnați prin legislația de transpunere a Directivelor NIS, să elaboreze proceduri de testare și auditare periodică a nivelului de securitate cibernetică, ca parte integrantă a procesului de evaluare a riscurilor, și să actualizeze permanent tehnologiile hardware și software folosite în cadrul infrastructurilor.

În același timp, autoritățile și instituțiile administrației publice cu responsabilități în asigurarea securității cibernetică trebuie să încurajeze și să susțină implementarea de politici și măsuri de securitate cibernetică prin crearea unui cadru de lucru unitar, oferirea pregătirii necesare și coagularea unei comunități de experți în domeniu.

4.1.2. Dezvoltarea capacităților naționale de detectare, investigare și contracarare a atacurilor cibernetică

Pentru a avea rețele și sisteme informatice sigure și reziliente este necesară dezvoltarea și adaptarea permanentă a capacităților de detecție și investigare. Acest lucru trebuie să fie făcut în concordanță atât cu evoluțiile tehnologice, cât și cu schimbările mediului de securitate cibernetică, printr-o cooperare între autorități și instituții ale administrației publice și entități private.

Cunoașterea obținută ca urmare a investigațiilor derulate reprezintă un element important în contracararea și, ulterior, în atribuirea atacurilor cibernetică.

4.1.3. Alocarea eficientă a resurselor financiare, tehnologice și umane

Având în vedere diversitatea domeniilor în care se regăsesc rețele și sisteme informatice și interconectarea dintre acestea, este importantă promovarea și conștientizarea în rândul operatorilor, autorități și instituții ale administrației publice sau entități private, a necesității realizării de investiții în tehnologii.

Aceste investiții trebuie să fie susținute prin demersuri de specializare a personalului din domeniu, care să fie pregătit pentru a:

- *înțelege amenințarea provenită din spațiul cibernetic;*
- *cunoaște evoluțiile din domeniul tehnologic;*
- *dobândi cunoștințele necesare pentru o reacție adecvată în cazul unui atac cibernetic sau a unui incident de securitate cibernetică.*

O cooperare permanentă între autoritățile și instituțiile administrației publice cu responsabilități în domeniul securității cibernetică, precum și între acestea și mediul de afaceri și industrie este dezirabilă în sensul partajării cunoașterii, de exemplu prin elaborarea de ghiduri de bune practici, recomandări pe domenii de activitate, identificării celor mai bune soluții de asigurare a protecției rețelelor și sistemelor informatice, precum și alocării eficiente și complementare a resurselor.

4.1.4. Consolidarea mecanismului de raportare a incidentelor de securitate cibernetică

Un sistem de management centralizat al incidentelor de securitate cibernetică oferă imaginea de ansamblu asupra amenințării cibernetică la adresa unei infrastructuri, a unui domeniu de activitate și chiar a securității naționale. Totodată, un mecanism de raportare eficient contribuie la asigurarea unui răspuns concret la amenințările provenite din spațiul cibernetic.

Este necesară elaborarea unui set de măsuri și mecanisme de raportare a incidentelor, îndeosebi la nivelul entităților care operează rețele și sisteme informatice din domenii aferente serviciilor esențiale sau cu valențe critice pentru securitatea națională. Operatorii

trebuie să înțeleagă și să își asume rolul de facto și atribuțiile care le revin și să optimizeze fluxul subsumat mecanismului de raportare a incidentelor de securitate cibernetică, în conformitate cu recomandările și reglementările UE și cu legislația națională.

4.1.5. Crearea unor mecanisme de certificare, conformitate și standardizare în domeniul securității cibernetice

Calitatea și nivelul de securitate cibernetică al produselor hardware și software folosite sunt deosebit de importante pentru menținerea unor rețele și sisteme informatice sigure și reziliente în fața amenințărilor cibernetice și trebuie să prevaleze aspectelor restrictive de ordin bugetar.

În acest sens, este necesară crearea unor mecanisme la nivel național de certificare, conformitate și standardizare în domeniul securității cibernetice, care să aibă în vedere un set strict de criterii (tehnice, non-tehnice, inclusiv prin raportare la aspecte ce țin de securitate națională) și care să permită identificarea riscurilor și vulnerabilităților de securitate cibernetică existente la nivelul produselor hardware și software.

De asemenea, este necesară crearea cadrului normativ și a mecanismelor necesare astfel încât în cadrul programelor și proiectelor să fie respectat principiul "securizare din etapa de proiectare", având în vedere că, produsele și capacitățile sunt proiectate pentru a corespunde standardelor din domeniul securității cibernetice

4.1.6. Securizarea lanțului de aprovizionare

Trebuie menținută în atenție securizarea lanțului de aprovizionare, prin impunerea implementării unor mecanisme de securitate cibernetică la toate componentele acestui ecosistem. Este necesară definirea criteriilor de încredere pentru furnizorii de echipamente hardware, software și servicii, în special pentru sistemele ce țin de securitatea națională.

2. Schimbări preconizate

Prezentul proiect legislativ își propune să interzică achiziționarea de produse și servicii de tip antivirus de la entități provenind din Federația Rusă sau aflate sub controlul Federației Ruse. Rațiunile pentru care se instituie această interdicție sunt legate, pe de-o parte, de contextul dat de războiul pornit de Federația Rusă asupra Ucrainei iar, pe de altă parte, de lipsa de independență a entităților rusești care furnizează soluții IT.

Măsura legislativă este inițiată într-un context european mai larg în care state membre UE au interzis expres produsele și serviciile „Kaspersky Lab” și ale companiei „Group-IB” deoarece există informații conform cărora cele două entități permit guvernului rus să penetreze sistemele și rețelele informatice în care le sunt instalate programele software.

Prezentul proiect de lege interzice autorităților și instituțiilor publice de la nivel central și local să achiziționeze și să utilizeze produse și servicii privind securitatea dispozitivului (securitatea punctului final), aplicații și programe software de detecție antivirus, anti-malware, firewall pentru aplicații web (Web Application Firewall), rețele virtuale private (Virtual Private Network), precum și sisteme de detecție și răspuns pentru endpointuri (Endpoint Detection Response) provenind din Federația Rusă sau aflată sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă.

În 45 de zile de la data intrării în vigoare a legii, toate produsele și serviciile de tipul celor prevăzute mai sus vor fi deconectate, respectiv dezinstalate de la rețelele și sistemele informatice ale autorităților și instituțiilor publice de la nivel central și local. Deconectarea, respectiv dezinstalarea se va face chiar de către autoritățile și instituțiile publice centrale și locale care au instalat pe rețelele și sistemele lor informatice astfel de programe. Având în vedere claritatea și calitatea textului, autoritățile pot aprecia în concret, încă de la data intrării în vigoare a prezentei legi, ce fel de produse

și servicii trebuie să dezinstateze. Deconectarea, respectiv deinstalarea se va realiza cu sprijinul Ministerului Cercetării, Inovării și Digitalizării, Autorității pentru Digitalizarea României, Directoratului Național de Securitate Cibernetică, Serviciului Român de Informații și Serviciului de Telecomunicații Speciale

Interdicția prevăzută la art. 1 este una temporară, în acord cu regulile prevăzute de art. 53 din Constituție, și produce efecte pe întreaga durată a invaziei declanșată de Federația Rusă împotriva Ucrainei, până la data semnării unui tratat de pace sau a unui acord permanent de armistițiu care să consfințească integritatea teritorială a Ucrainei, reparații pentru prejudiciile suferite de țara invadată, precum și cooperarea Federației Ruse cu organismele naționale și internaționale competente pentru pedepsirea persoanelor care se fac vinovate de crime de război sau crime împotriva umanității.

Pentru nerespectarea de către autoritățile și instituțiile publice a prevederilor art. 1, alin. (1) și (2) se instituie contravenție și se sancționează cu amendă de la 50.000 și 200.000 lei. Având în vedere că proiectul se adresează autorităților și instituțiilor publice nu am fi putut opta pentru instituirea unei sancțiuni penale din cauza prevederilor art. 135 C. pen. De asemenea, nu am considerat că o sancțiune penală aplicată instituțiilor publice în considerarea permisiilor prevăzute de art. 135, alin. (2) C. pen. ar fi proporțională și adecvată, având în vedere faptul că ne putem confrunta cu un adevărat fenomen de instituții care deja utilizează astfel de programe. Scopul legii este să elimine rapid aceste programe din rețelele și sistemele informatice ale instituțiilor, nu să creeze probleme de natură penală instituțiilor publice românești.

Constatarea și aplicarea contravențiilor se face de către personal anume desemnat prin ordin al ministrului cercetării, inovării și digitalizării;

Prevederile prezentului proiect nu se aplică autorităților publice cu atribuții în domeniul securității naționale, apărării naționale și ordinii publice, deoarece acestea au propriile reguli de protecție a securității cibernetice, congruente fiind cu regimul juridic de protecție al informațiilor clasificate. De asemenea, unele dintre aceste autorități, în exercitarea activității lor de culegere de informații și intelligence, pot folosi, în scopul exercitării atribuțiilor, unele dintre astfel de programe.

Apreciem că prezenta lege impune un regim de restrângere a exercițiului unor drepturi și libertăți fundamentale pentru rațiuni de securitate națională, astfel că soluția legislativă trebuie adoptată numai prin lege. În România, restrângerea exercițiului unor drepturi și libertăți fundamentale poate opera doar pentru una din ipotezele exhaustiv enumerate de art. 53⁴. Altfel spus, Constituția limitează posibilitatea de intervenție a legiuitorului în sensul restrângerii exercițiului unor drepturi fundamentale doar la acele situații în care concilierea unor interese deopotrivă imperative trebuie realizată fără a afecta substanța niciunui dintre ele. Este vorba fie de obiectivele ce vizează însăși supraviețuirea statului și a elementelor sale constitutive, fie de necesara armonizare între garanțiile oferite mai multor drepturi fundamentale în același timp. Măsurile de restrângere a exercițiului

⁴ Lidia Barac, "Inconsecvențe jurisprudențiale relative la posibilitatea restrângerii exercițiului unor drepturi sau libertăți fundamentale. Problematika limitării exercițiului unor drepturi și libertăți fundamentale în contextul instituirii stării de urgență sau a stării de alertă (I)", Juridice.ro, 19.05.2020, disponibil la: <https://www.juridice.ro/683898/inconsecvente-jurisprudentiale-relative-la-posibilitatea-restrangerii-exercitiului-unor-drepturi-sau-libertati-fundamentale-problematika-limitarii-exercitiului-unor-drepturi-si-libertati-fundamentale.html>; accesat la data de 07.05.2022.

