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 aflate 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 50.000 lei la 200.000 lei.

(2) Constatarea și aplicarea contravențiilor se fac 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, al Directoratului Național de Securitate Cibernetică, al Serviciului Român de Informații și al 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

Secţiunea 1
Titlul proiectului de act normativ:
LEGE
privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei

1. Descrierea situaţiei 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 autorităţi şi instituţii publice să schimbe soluţiile 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 esenţiale. BSI susţine că ar fi bine ca toate companiile germane care folosesc soluţii AV sau alte tipuri de soft-uri de la Kaspersky să renunţe la ele şi să folosească programe de la alte companii. BSI explică faptul că soluţiile antivirus menţin o legătură permanentă, criptată şi imposibil de verificat cu serverele vendor-ului, pentru o actualizare permanentă a definiţiilor virusilor. Teama este că fişiere sensibile ar putea fi extrase de pe computerele care folosesc soluţiile companiei, pentru a fi trimise pe serverele Kaspersky şi ale altor companii ruseşti[1].

În Italia, Franco Gabrielli, secretar de stat la preşedinţia Consiliului de miniştri, a declarat în Senat că Guvernul de la Roma lucrează la un set de reguli care ar permite entităţilor de stat să înlăture programele software dezvoltate de firma rusă Kaspersky[2]. Între timp, reglementările au fost adoptate astfel cum sunt descrise la secţiunea 5, pct. VI din prezenta expunere.

Potrivit unor informaţii publice apărute în presă[3], Primăria municipiului Bucureşti a organizat o licitaţie pentru achiziţionarea unui antivirus Kaspersky Endpoint Security For Business-Select pentru 1.200 de echipamente, cu mentenanţă inclusă 12 luni. Biroul de Presă al instituţiei primarului general a transmis că Primăria Capitalei foloseşte antivirusul Kaspersky din anul 2012 şi nu a întâmpinat probleme din cauza acestui produs.

Există informaţii conform cărora foarte multe instituţii publice şi autorităţi ale administraţiei publice locale achiziţionează programe software de antivirus ruseşti din cauza preţurilor mici şi care au prevalenţă prin Sistemul informatic colaborativ pentru mediu performant de desfăşurare al achiziţiilor publice (SICAP).

Prezenţa software-urilor ruseşti de tip antivirus reprezintă o vulnerabilitate la adresa securităţii cibernetice a autorităţilor şi instituţiilor româneşti, din cauză că aceste programe acaparează funcţii importante ale reţelelor şi sistemelor informatice, creând relaţii de interdependenţă. În contextul în care Federaţia Rusă utilizează inclusiv atacuri de tip cibernetic la adresa statelor occidentale şi îşi foloseşte companiile naţionale şi cetăţenii ruşi, prin diverse metode, în războiul asupra Ucrainei, încălcând toate normele de drept internaţional în materie, România nu poate să-şi asume prezenţa unor produse şi servicii IT ruseşti în infrastructura cibernetică naţională.

Potrivit **Hotărârii Parlamentului României nr. nr. 22 din 30 iunie 2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024, obiectivele naţionale de securitate vizează şi** ***"asigurarea securităţii şi protecţiei***

---

[1]Disponibil 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.

[2]Disponibil 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.

[3]Disponibil la: https://stiripesurse.directorylib.com/primaria-capitalei-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, prevenirea 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;*

*- **Creșterea 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 rețelelor 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 operaționalizeze 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 cibernetice 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 cibernetice 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 capabilităților naționale de detectare, investigare și contracarare a atacurilor cibernetice

Pentru a avea rețele și sisteme informatice sigure și reziliente este necesară dezvoltarea și adaptarea permanentă a capabilităților 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 cibernetice.

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 cibernetice, 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 cibernetice 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 capabilitățile 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 ruseşti 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 instalate 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 dezinstaleze. Deconectarea, respectiv dezinstalarea 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 declanşată de Federaţia Rusă împotriva Ucrainei, până la data semnării unui tratat de pace sau a unui acord permanent de armistiţiu care să consfinţească integritatea teritorială a Ucrainei, reparaţii pentru prejudiciile suferite de ţara invadată, precum şi cooperarea Federaţiei Ruse cu organismele naţionale şi internaţionale competente pentru pedepsirea persoanelor care se fac vinovate de crime de război sau crime împotriva umanităţii.

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 50.000 lei la 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 permisiei 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. 53[4]. 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. Problematica 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-problematica-limitarii-exercitiului-unor-drepturi-si-libertati-fundamentale.html; accesat la data de 07.05.2022.

unor drepturi pot fi adoptate fie pentru a preveni anumite stări de lucruri, fie pentru a contracara, fie pentru a limita sau împiedica extinderea consecințelor lor negative.

Condițiile de validitate pentru restrângerea exercițiului drepturilor și libertăților fundamentale sunt următoarele:

1. **Restrângerea exercițiului se poate înfăptui numai prin lege**. Termenul de lege a fost interpretat de doctrină în sens restrâns, anume doar prin act normativ al Parlamentului. **Doctrina**[5] nu recunoaște dreptul Guvernului de a restrânge exercițiul drepturilor și libertăților fundamentale prin ordonanță sau ordonanță de urgență, această competență rămânând unicei autorități legiuitoare a țării pentru a conferi un grad de protecție sporită drepturilor subiective oferite de Constituție. Astfel cel puțin teoretic, Legea nr. 182/2002 sau Legea nr. 51/1991 nu ar putea fi modificate pe calea ordonanțelor de urgență. Cu toate acestea, practica administrativă și jurisprudența constituțională au admis ideea că și ordonanțele guvernului intră sub sfera noțiunii de lege **(Decizia CCR nr. 567/2006**[6] **și Decizia CCR nr. 1221/2008**[7]).
2. **Restrângerea trebuie să fie necesară într-o societate democratică**. Prin această condiție sunt valorificate documentele internaționale în materie, care includ o circumstanțiere de natură similară pentru marja de apreciere pe care o lasă statelor în a recurge la măsuri cu vădit caracter antidemocratic de vreme ce tind la diminuarea posibilităților de manifestare în sfera publică a cetățenilor[8].
3. **Restrângerea trebuie să aibă natură excepțională și nu poate reprezenta regula într-o societate democratică**. O frecvență a restrângerii exercițiului drepturilor duce la o delegitimare a autorității legiuitoare și, deci, la o delegitimare a restrângerii însăși[9].
4. **Caracterul măsurii instituită prin legea care restrânge exercițiul dreptului trebuie să aibă caracter temporar**. Ea trebuie să înceteze la momentul la care dispare cauza care a declanșat aplicarea ei[10].
5. **Restrângerea trebuie să aibă loc numai pentru rațiuni ce țin de: apărarea securității naționale**, a ordinii publice, a sănătății, a moralei publice, a drepturilor și a libertăților cetățenilor, desfășurarea instrucției penale, prevenirea consecințelor unei calamități, ale unui dezastru ori ale unui sinistru deosebit de grav[11].
6. **Restrângerea trebuie să fie proporțională cu situațiile de fapt care au generat restrângerea.** În cazul legislației din domeniul securității naționale, raportul de proporționalitate se evaluează în funcție de amenințările, riscurile și vulnerabilitățile la adresa securității naționale[12].
7. **Măsura trebuie să fie nediscriminatorie,** adică să se aplice tuturor subiecților de drept pentru care există aceeași rațiune și să existe criterii obiective de aplicare a acestor restrângeri.

Printre ipotezele limitativ și expres enumerate se numără și **securitatea națională**, deoarece starea de echilibru și pace socială poate fi asigurată numai printr-o adaptare proporțională a regulilor de conviețuire socială cu amenințările, vulnerabilitățile și riscurile la adresa existenței și dezvoltării statului. Cum securitatea cibernetică a rețelelor și sistemelor informatice ale autorităților

---

[5] Elena Simina Tănăsescu, "Art. 53. Restrângerea exercițiului unor drepturi sau al unor libertăți" în Ioan Moraru, Elena Simina Tănăsescu, *Constituția României, comentariu pe articole,* Editura C. H. Beck, București, 2009, p. 462.

[6] Publicat în Monitorul Oficial, Partea I nr. 613 din 14 iulie 2006.

[7] Publicat în Monitorul Oficial, Partea I nr. 804 din 02 decembrie 2008.

[8] Elena Simina Tănăsescu, "Art. 53. Restrângerea exercițiului unor drepturi sau al unor libertăți" în Ioan Moraru, Elena Simina Tănăsescu, *Op. Cit.*, p. 463.

[9] *Ibid*, p. 464.

[10] *Idem.*

[11] Decizia nr. 872/2010, publicată în Monitorul Oficial, Partea I nr. 433 din 28 iunie 2010.

[12] *Idem.*

şi instituţiilor publice de la nivel central şi local este o subcomponentă a securităţii naţionale[13], apreciem că şi regimul juridic care guvernează securitatea cibernetică - inclusiv măsuri de interzicere a unor programe informatice care reprezintă ameninţări - trebuie să se supună regulilor instituite de art. 53 din Constituţie. De altfel, noţiunea de securitate naţională, prin raportare la art. 53, a fost descrisă de CCR ca fiind plurivalentă şi poate include şi o componentă economică (stabilitatea macro-economică şi financiară a ţării) de vreme ce ea poate justifica inclusiv restrângerea exerciţiului la salariu prin reducerea procentuală a cuantumului salariilor aflate în plată în cadrul sectorului bugetar (Decizia CCR nr.872/2010). CCR a analizat aproape mereu sintagma *"securitate naţională"* şi protecţia informaţiilor clasificate din perspectiva art. 53, astfel, în contextul obiectului de reglementare a prezentului domeniu, se impune ca acesta să fie prevăzut numai prin lege.
3.Alte informaţii Nu au fost identificate.
Secţiunea a 3-a **Impactul socio-economic al proiectului de act normativ**
1. Impactul macroeconomic Prezentul act normativ nu se referă la acest subiect.
1[1]. Impactul asupra mediului concurenţial şi domeniului ajutoarelor de stat Prezentul act normativ nu se referă la acest subiect.
2. Impactul asupra mediului de afaceri Prezentul act normativ nu se referă la acest subiect.
2[1] Impactul asupra sarcinilor administrative - Ministerul Cercetării, Inovării şi Digitalizării, Autoritatea pentru Digitalizarea României, Directoratul Naţional de Securitate Cibernetică, cu sprijinul Serviciului Român de Informaţii şi Serviciul de Telecomunicaţii Speciale, vor identifica produsele şi serviciile care fac obiectul interdicţiei impuse de proiectul de lege, în vederea elaborării listei. - Autoritatea pentru Digitalizarea României, Directoratul Naţional de Securitate Cibernetică, Serviciul Român de Informaţii şi Serviciul de Telecomunicaţii Speciale au obligaţia de a monitoriza autorităţile şi instituţiile publice centrale şi locale pentru a identifica dacă şi unde există produse şi servicii dintre cele interzise prin prezentul proiect de lege. - Ministerul Cercetării, Inovării şi Digitalizării va constata şi aplica amenzi contravenţionale pentru încălcarea art. 1 din lege.
2[2] Impactul asupra întreprinderilor mici şi mijlocii În limitele art. 53 din Constituţie, prin lege se va interzice accesul pe piaţa românească, strict pentru autorităţile şi instituţiile publice centrale şi locale, a unor produse şi servicii dintre cele prevăzute la art. 1 din proiect şi care provin din Federaţia Rusă ori sunt sub controlul direct sau indirect al Federaţiei Ruse.
3. Impactul social Prezentul act normativ nu se referă la acest subiect.
4. Impactul asupra mediului Proiectul de act normativ nu are impact asupra mediului
5. Alte informaţii Nu au fost identificate.
Secţiunea a 4-a **Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât şi pe termen lung (pe 5 ani)**
- mii lei -

[13] Decizia CCR nr. 455/2018, publicat în Monitorul Oficial, Partea I nr. 622 din 18 iulie 2018. "63. Curtea constată că ritmul actual al realităţilor obiective este în continuă schimbare, iar relaţiile sociale referitoare la securitatea reţelelor şi sistemelor informatice vizează un interes general a cărui amploare impune calificarea acestui domeniu ca fiind în strânsă interdependenţă cu securitatea naţională."

Indicatori	Anul curent	Următorii 4 ani				Media pe 5 ani
1	2	3	4	5	6	7
1. Modificări ale veniturilor bugetare, plus/minus, din care: a) buget de stat, din acesta: (i) impozit pe profit (ii) impozit pe venit b) bugete locale: (i) impozit pe profit a) bugetul asigurărilor sociale de stat: (i) contribuţii de asigurări						
2. Modificări ale cheltuielilor bugetare, plus/minus, din care: a) buget de stat, din acesta: (i) cheltuieli de personal (ii) bunuri şi servicii (iii) transferuri intre unitati ale administratiei publice b) bugete locale: (i) cheltuieli de personal (ii) bunuri şi servicii c) bugetul asigurărilor sociale de stat: (i) cheltuieli de personal (ii) bunuri şi servicii						
3. Impact financiar, plus/minus, din care: a) buget de stat b) bugete locale						
4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare						
7. Alte informaţii Nu există.						

Secţiunea a 5-a
Efectele proiectului de act normativ asupra legislaţiei în vigoare

1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ:
a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ - Nu este cazul;
b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziţii - Ordin al ministrului cercetării, inovării şi digitalizării privind tabelul nominal al entităţilor, produselor şi serviciilor interzise în temeiul art. 1, alin. (1) din Lege;

1^1. Compatibilitatea proiectului de act normativ cu legislaţia în domeniul achiziţiilor publice:
– Proiectul de act normativ este în concordanţă cu prevederile Legii nr.98/2016 privind achiziţiile publice, cu modificările şi completările ulterioare, Legii nr. 99/2016 privind achiziţiile sectoriale, cu modificările şi completările ulterioare, Legii nr. 100/2016 privind concesiunile de lucrări şi concesiunile de servicii, cu modificările şi completările ulterioare, Ordonanţei de urgenţă a Guvernului nr. 114/2011 privind atribuirea anumitor contracte de achiziţii publice în domeniile apărării şi securităţii, cu modificările şi completările ulterioare.

2. Conformitatea proiectului de act normativ cu legislația comunitară în cazul proiectelor ce transpun prevederi comunitare:
- Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (Text cu relevanță pentru SEE);
- Regulamentul (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare;
- Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;
- Strategia de securitate cibernetică a Uniunii Europene pentru deceniul digital, având la bază Comunicarea comună către Parlamentul European și Consiliu JOIN(2020) 18 final din 16 decembrie 2020.

3. Măsuri normative necesare aplicării directe a actelor normative comunitare:
Proiectul de act normativ nu se referă la acest subiect.

4. Hotărâri ale Curții de Justiție a Uniunii Europene:
Proiectul de act normativ nu se referă la acest subiect.

5. Alte acte normative și/sau documente internaționale din care decurg angajamente, făcându-se referire la un anume acord, o anume rezoluție sau recomandare internațională ori la alt document al unei organizații internaționale:
Proiectul de act normativ nu se referă la acest subiect.

6. Alte informații:

1. **Italia**

La data de 21 aprilie 2022, Agenția Națională de Securitate Cibernetică a adoptat Circulara nr. 4336 pentru punerea în aplicare a articolului 29, alineatul 3, din Decretul-lege nr. 21 din 21 martie 2022[14].

Prin Decretul-lege nr. 21 din 21 martie 2022[15], care conține „Măsuri urgente de contracarare a efectelor economice și umanitare ale crizei ucrainene", Guvernul a considerat, printre altele, necesitatea și urgența extraordinară de a asigura întărirea garanțiilor de securitate, apărare națională, rețele de comunicații. electronice și achiziții de materii prime. În acest sens, art. 29, alin.1 din același Decret-lege prevede că, pentru a preveni deteriorarea securității rețelelor, sistemelor informatice și serviciilor informatice ale administrațiilor publice, în temeiul art. 1, alin.2, din decretul legislativ 30 martie 2001, nr. 165, decurgând din riscul ca firmele producătoare de produse și servicii de tehnologie de securitate informatică legate de Federația Rusă să nu poată furniza servicii și actualizări ale produselor lor, ca urmare a crizei din Ucraina, aceleași administrații vor proceda cu promptitudine la diversificarea produselor în uz.

Mai precis, același art. 29, conform prevederilor combinate ale alin. 1 si 3, prevede ca identificarea produselor și serviciilor de diversificat are loc în raport cu categoriile indicate în circulara Agenției Naționale de Securitate Cibernetică și vizează asigurarea următoarelor funcții de securitate:

a) securitatea dispozitivului (securitatea punctului final), inclusiv aplicațiile antivirus, anti-malware și „detecție și răspuns la punctele terminale" (EDR);
b) „paravan de protecție pentru aplicații web" (WAF).

Prin urmare, această circulară are scopul de a indica categoriile de produse și servicii tehnologice de securitate IT pentru pe care administrațiile publice vor trebui să le diversifice în temeiul art. 29, din decretul-lege nr. 21 din 2022.

În scopul identificării produselor și serviciilor tehnologice de securitate informatică ale companiilor producătoare legate de Federația Rusă, în temeiul art. 29, alin. 1 si 3, din decretul-lege nr. 21 din 2022, fiecare administrație publică căreia i se adresează prezenta circulară va diversifica următoarele categorii de produse și servicii tehnologice de securitate informatică:

[14] Publicată în Gazeta Oficială, Seria Generală GU nr.96 din 26-04-2022, disponibilă la: https://www.gazzettaufficiale.it/eli/id/2022/04/26/22A02611/sg; accesat la data de 07.05.2022.
[15] Publicată în Gazeta Oficială, Seria Generală GU nr.67 din 21-03-2022, disponibilă la: https://www.gazzettaufficiale.it/eli/id/2022/03/21/22G00032/sg; accesat la data de 08.05.2022.

1) produse și servicii în temeiul art. 29, alin. 3, lit. a), din decretul-lege nr. 21 din 2022, a companiei „Kaspersky Lab" și a companiei „Group-IB", comercializate tot prin canal indirect de revânzare și/sau vehiculate și prin acorduri-cadru sau contracte-cadru în „on-premise" sau „la distanță";

2) produsele și serviciile prevăzute la art. 29, alin.3, lit.b), din decretul-lege nr. 21 din 2022, a companiei „ Tehnologii pozitive", comercializate tot prin canal indirect de revânzare și/sau vehiculate și prin acorduri-cadru sau contracte -cadru în modul „on-premise" sau „la distanță".

Circulara recomandă administrațiilor cărora li se adresează următoarele:

- să fie responsabili cu efectuarea operațiunilor de configurare a noilor servicii și produse achiziționate în temeiul art. 29 din decretul-lege nr. 21 din 2022, de asemenea, în legătură cu cunoașterea precisă a activelor acestora (rețele, sisteme informatice și servicii IT) și impactul acestora asupra continuității serviciilor și protecției datelor;

- să adopte toate măsurile și bunele practici de management ale serviciilor IT și de risc cibernetic și, în special, să țină cont de ceea ce este definit de Cadrul național de securitate cibernetică și protecție a datelor, ediția 2019, creat de Centrul de Cercetare în Inteligență Cibernetică și securitatea informațiilor (CIS) al Universității Sapienza din Roma și al laboratorului național de securitate cibernetică al Consorțiului Național Interuniversitar pentru Tehnologia Informației (CINI), cu sprijinul Autorității Garante pentru protecția datelor cu caracter personal și al Departamentului de Informații pentru Securitate.

În special, se recomandă:

1) cercetarea în detaliu a serviciilor și produselor menționate la paragraful B) din circulară, analizând impactul actualizărilor acestora asupra operațiunilor, cum ar fi timpii necesari de întreținere;

2) să identifice și să evalueze noi servicii și produse, validarea compatibilității acestora cu activele lor, precum și a complexității managementului operațional al structurilor suport existente ;

3) definirea, partajarea și comunicarea planurilor de migrație cu toate părțile interesate direct sau indirect, cum ar fi organizațiile din cadrul administrațiilor și terții;

4) validarea metodelor de executare a planului de migrare asupra activelor de testare semnificative, asigurându-se că se procedează cu migrarea serviciilor și produselor pe cele mai critice active numai după validarea unor migrări și, cu ajutorul planurilor de recuperare pe termen scurt, la asigura necesarul de continuitate operațională. Planul de migrare trebuie să asigure că funcția de protecție garantată de instrumentele supuse diversificării nu este în niciun moment întreruptă;

5) să analizeze și să valideze funcționalitățile și integrările noilor servicii și produse, asigurând aplicarea regulilor și a configurațiilor de securitate proporționale cu scenariile cu risc ridicat (cum ar fi, de exemplu, autentificarea cu mai mulți factori pentru toate accesul privilegiat, activarea numai a serviciilor și funcțiilor). strict necesar, adoptarea principiilor „zero-trust");

6) asigurarea monitorizării și auditării adecvate a noilor produse de servicii, oferind suport adecvat pentru actualizarea și revizuirea configurațiilor online.

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

1. Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate:
În vederea elaborării proiectului de act normativ, proiectul s-a aflat în procesul de transparență decizională, fiind formulate propuneri și observații din partea tuturor organismelor implicate.

2. Fundamentarea alegerii organizațiilor cu care a avut loc consultarea, precum și a modului în care activitatea acestor organizații este legată de obiectul proiectului de act normativ:
Proiectul de act normativ nu se referă la acest subiect.

3. Consultările organizate cu autorităţile administraţiei publice locale, în situaţia în care proiectul de act normativ are ca obiect activităţi ale acestor autorităţi, în condiţiile Hotărârii Guvernului nr. 521/2005 privind procedura de consultare a structurilor asociative ale autorităţilor administraţiei publice locale la elaborarea proiectelor de acte normative. Proiectul de act normativ nu face obiectul unor asemenea consultări.
4. Consultările desfăşurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr. 750/2005 privind constituirea consiliilor interministeriale permanente Proiectul de act normativ nu face obiectul unor asemenea dezbateri.
5. Informaţii privind avizarea de către: a) Consiliul Legislativ b) Consiliul Suprem de Apărare a Ţării c) Consiliul Economic şi Social d) Consiliul Concurenţei e) Curtea de Conturi Proiectul de act normativ va fi supus avizării Consiliului Legislativ si Consiliul Suprem de Apărare a Ţării
6. Alte informaţii:
Secţiunea a 7-a **Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ**
1.Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ. Proiectul de act normativ nu se referă la acest subiect
2. Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice: Proiectul de act normativ nu se referă la acest subiect.
1.Alte informaţii
Secţiunea a 8-a **Măsuri de implementare**
1. Măsurile de punere în aplicare a proiectului de act normativ de către autorităţile administraţiei publice centrale şi/sau locale - înfiinţarea unor noi organisme sau extinderea competenţelor instituţiilor existente: Nu este cazul.
2. Alte informaţii.

Faţă de cele prezentate, a fost a fost promovată prezenta Lege privind protejarea sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei.

MINISTRUL CERCETĂRII, INOVĂRII SI DIGITALIZĂRII

Sebastian – Ioan BURDUJA

Față de cele prezentate, a fost a fost promovată prezenta Lege privind protejarea sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei

AVIZAT

AUTORITATEA PENTRU DIGITALIZAREA ROMÂNIEI

Presedinte – Dragoș - Cristian VLAD

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Director – Dan CÎMPEAN

MINISTERUL FINANȚELOR

Ministru – Adrian CÂCIU

MINISTERUL AFACERILOR EXTERNE

Ministru – Bogdan AURESCU

MINISTERUL JUSTIȚIEI
Ministru - Marian- Cătălin PREDOIU