# 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**

## Secțiunea a 2-a
## Motivul emiterii actului normativ

**2.1 Sursa Proiectului de act normativ**

Proiectul a fost inițiat de Ministerul Cercetării, Inovării și Digitalizării.

**2.2 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 rusești[1].

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 Kaspersky[2]. Între timp, reglementările au fost adoptate astfel cum sunt descrise la secțiunea 5, pct. VI din prezenta expunere.

Potrivit unor informații publice apărute în presă[3], Primăria municipiului București a organizat o licitație pentru achiziționarea unui antivirus Kaspersky Endpoint Security For Business-

---

[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.

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. 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 cibernetice 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 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."*

**1^1. Proiectul de act normativ transpune legislație comunitară sau creează cadrul pentru aplicarea directă a acesteia**

Proiectul de act normativ nu se referă la acest subiect.

**2. <u>Schimbări preconizate</u>**

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 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 60 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 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 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 niciunuia 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 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.

---

[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.

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

---

[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.*

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 și instituțiilor publice de la nivel central și local este o subcomponentă a securității naționale[13], apreciem că și regimul juridic care guvernează securitatea cibernetică - inclusiv măsuri de interzicere a unor programe informatice care reprezintă amenințări - trebuie să se supună regulilor instituite de art. 53 din Constituție. De altfel, noțiunea de securitate națională, prin raportare la art. 53, a fost descrisă de CCR ca fiind plurivalentă și poate include și o componentă economică (stabilitatea macro-economică și financiară a țării) de vreme ce ea poate justifica inclusiv restrângerea exercițiului 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 națională"* și protecția informațiilor clasificate din perspectiva art. 53, astfel, în contextul obiectului de reglementare a prezentului domeniu, se impune ca acesta să fie prevăzut numai prin lege.

**2.3 Alte informații**

Nu este cazul.

**Secțiunea a 3–a**

**Impactul socioeconomic**

**3.1. Descrierea generală a beneficiilor și costurilor estimate ca urmare a intrării în vigoare a actului normativ**

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

[12] *Idem.*

[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 realităților obiective este în continuă schimbare, iar relațiile sociale referitoare la securitatea rețelelor și sistemelor informatice vizează un interes general a cărui amploare impune calificarea acestui domeniu ca fiind în strânsă interdependență cu securitatea națională."

Autoritățile și instituțiile publice care intră sub incidența prezentului proiect de lege sunt nevoite să-și redimensioneze capitolul bugetar, cu ocazia rectificării bugetare, astfel încât să poată să-și asigure achiziționarea de noi produse și servicii software care nu intră sub interdicțiile prevăzute de lege.

**3.2. Impactul social**

Proiectul de act normativ nu se referă la acest subiect.

**3.3. Impactul asupra drepturilor și libertăților fundamentale ale omului**

Proiectul de act normativ nu se referă la acest subiect.

**3.4 Impactul macroeconomic**

Proiectul de act normativ nu se referă la acest subiect.

**3.4.1. Impactul asupra economiei și asupra principalilor indicatori macroeconomici**

În limitele art. 53 din Constituție, prin lege se va interzice accesul pe piața românească, strict pentru autoritățile și instituțiile publice centrale și locale, a unor produse și servicii dintre cele prevăzute la art. 1 din proiect și care provin din Federația Rusă ori sunt sub controlul direct sau indirect al Federației Ruse.

**3.4.2. Impactul asupra mediului concurențial și domeniul ajutoarelor | de stat Impactul asupra mediului concurențial și domeniului ajutoarelor de stat**

Proiectul de act normativ nu se referă la acest subiect.

**3.6 Impactul asupra mediului înconjurător**

Proiectul de act normativ nu se referă la acest subiect.

**3.7. Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării**

Prezentul proiect are drept scop creșterea securității cibernetice a sistemelor și rețelelor informatice ale instituțiilor și autorităților publice.

**3.8. Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile**

Proiectul de act normativ nu se referă la acest subiect.

**3.9. Alte informații**

**Nu este cazul**

**Secțiunea a 4–a**

**Impactul financiar asupra bugetului general consolidat,**

**atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani), includiv informatii cu privire la cheltuieli si venituri**

- mii lei (ron) -

| Indicatori | Anul curent | Următorii 4 ani | | | | Media pe 5 ani |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 4. 1. Modificări ale veniturilor bugetare, plus/minus, din care:<br>a) buget de stat, din acesta:<br>i. impozit pe profit<br>ii. impozit pe venit | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul |

| | | | | | | |
|---|---|---|---|---|---|---|
| b) bugete locale<br>i. impozit pe profit<br>c) bugetul asigurărilor sociale de stat:<br>i. contribuții de asigurări<br>d) alte tipuri de venituri | | | | | | |
| 4. 2. Modificări ale cheltuielilor bugetare, plus/minus, din care:<br>a) buget de stat, din acesta:<br>i. cheltuieli de personal<br>ii. bunuri şi servicii<br>b) bugete locale:<br>i. cheltuieli de personal<br>ii. bunuri şi servicii<br>c) bugetul asigurărilor sociale de stat:<br>i. cheltuieli de personal<br>bunuri şi servicii<br>d) alte tipuri de venituri | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul |
| 4. 3. Impact financiar, plus/minus, din care:<br>a) buget de stat<br>b) bugete locale | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul |
| 4. 4. Propuneri pentru acoperirea creşterii cheltuielilor bugetare | Nu este cazul | | | | | |
| 4. 5. Propuneri pentru a compensa reducerea veniturilor bugetare | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul | Nu este cazul |
| 4. 6. Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare | Nu este cazul | | | | | |
| 4.7. | Nu este cazul | | | | | |
| 4. 8. Alte informatii | | | | | | |

**Secţiunea a 5–a**

**Efectele proiectului de act normativ asupra legislaţiei în vigoare**

**5.1. 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;**

a) **acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziţii.**

- Ordin al ministrului cercetării, inovării şi digitalizării privind tabelul nominal al entităților, produselor şi serviciilor interzise în temeiul art. 2, alin. (2) din Lege;
- Ordin al ministrului cercetării, inovării şi digitalizării privind tabelul nominal al entităților, produselor şi serviciilor interzise în temeiul art. 4, alin. (3) din Lege;
- Ordin al ministrului cercetării, inovării şi digitalizării privind tabelul nominal al entităților, produselor şi serviciilor interzise în temeiul art. 5, alin. (1) din Lege;

**5.2. Impactul asupra legislaţiei în domeniul achiziţiilor publice**

Proiectul de act normativ nu se referă la acest subiect.

**5. 3. Conformitatea proiectului de act normativ cu legislaţia UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE)**

Proiectul de act normativ nu se referă la acest subiect

**5.3.1. Măsuri normative necesare transpunerii directivelor UE**

Proiectul de act normativ nu se referă la acest subiect

**5.3.2. Măsuri normative necesare aplicării actelor legislative UE**

Proiectul de act normativ nu se referă la acest subiect

**5.4 Hotărâri ale Curţii de Justiţie a Uniunii Europene**

Proiectul de act normativ nu se referă la acest subiect

**5.5. Alte acte normative şi/sau documente internaţionale din care decurg angajamente asumate**

Proiectul de act normativ nu se referă la acest subiect

**5.6. Alte informaţii**

Nu este cazul

**Secţiunea a 6–a**

**Consultările efectuate în vederea elaborării proiectului de act normativ**

**6.1. Informaţii privind neaplicarea procedurii de participare la elaborarea actelor normative**

Proiectul de act normativ nu se referă la acest subiect

**6.2. Informaţii privind procesul de consultare cu organizaţiile neguvernamentale, institute de cercetare şi alte organisme implicate**

**6.3. Informaţii despre consultările organizate cu autorităţile administraţiei publice locale,**

Nu este necesară consultarea autorităților administrației publice locale, deoarece proiectul de lege privește aspecte de securitate cibernetică, iar securitatea cibernetică este parte componentă a securității naționale (Decizia CCR nr. 455/2018, parag. 63). Securitatea națională este un domeniul în care doar autoritățile publice centrale exercită atribuții de reglementare, în funcție de specificul fiecărei autorități. MCID este, potrivit art. 1, alin. (3) din HG nr. 371/2021, autoritate de stat în domeniul securității cibernetice. În calitate de autoritate de stat cu atribuții de reglementare în domeniul securității cibernetice, MCID a inițiat proiectul de act normativ în urma consultării cu alte autorități publice centrale cu atribuții în domeniul securității naționale și al securității cibernetice, condiție pe care o apreciem ca fiind necesară și suficientă.

**6.4.Informaţii privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative**
**Nu este cazul**

**6.5. Informaţii privind avizarea de către:**

**a) Consiliul Legislativ**

b) Consiliul Suprem de Apărare a Ţării – se solicită aviz

c) Consiliul Economic şi Social – se solicită aviz

| |
|---|
| d) Consiliul Concurenţei<br>e) Curtea de Conturi<br>**Proiectul de act normativ va fi supus avizării Consiliului Legislativ.** |
| **6.6 Alte informaţii**<br>Nu este cazul. |
| **Secţiunea a 7–a**<br>**Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ** |
| **7.1 Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ** |
| **7.2 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.**<br>Proiectul de act normativ nu se referă la acest subiect. |
| **Secţiunea a 8–a**<br>**Măsuri de implementare, monitorizarea şi evaluarea proiectului de act normativ** |
| 8.1 **Măsurile de punere în aplicare a proiectului de act normativ**<br>Proiectul de act normativ nu se referă la acest subiect |
| 8.2 **Alte informaţii**<br>8.3 Nu este cazul. |

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

**MINISTERUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII**
**Ministru,**
**Sebastian – Ioan BURDUJA**

| |
|---|
| Proiectul de act normativ va fi supus avizării Consiliului Legislativ si Consiliul Suprem de Apărare a Ţării |
| 6. Alte informaţii: |
| **Secţiunea a 7-a**<br>**Activităţi de informare publică privind elaborarea**<br>**şi implementarea proiectului de act normativ** |
| 1.Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ.<br>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:<br>Proiectul de act normativ nu se referă la acest subiect. |
| 1.Alte informaţii |
| **Secţiunea a 8-a**<br>**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:<br>Nu este cazul. |
| 2. Alte informaţii. |

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

**MINISTERUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII**
**Ministru,**
**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

**Avizăm favorabil:**

**Directoratul Național de Securitate Cibernetică**
**Director – Dan CÎMPEAN**

**Autoritatea pentru Digitalizarea României**
**Președinte- Dragoș-Cristian Vlad**

**Serviciul de Telecomunicații Speciale**
**Director - Ionel-Sorin BĂLAN**

**Serviciul Român de Informații**
**Director- Eduard Raul HELLVIG**

**Serviciul de Informații Externe**
**Director - Gabriel VLASE**

**Serviciul de Protecție și Pază**
**Director - Lucian-Silvan PAHONȚU**

Oficiul Registrului Național al Informațiilor Secrete de Stat
Director General - Marius PETRESCU

**Ministerul Apărării Naționale**
**Vasile DÎNCU**

**Ministerul Afacerilor Interne**
**Ministru – Lucian Nicolae BODE**

**Ministerul Afacerilor Externe**
**Ministru – Bogdan AURESCU**

**Ministrul Finanțelor**
**Ministru – Adrian CÂCIU**

**Ministerul Justiției**
**Ministru - Marian – Cătălin PREDOIU**

**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 general și necesar în vederea interzicerii achiziționării și utilizării de către autoritățile și instituțiile publice, de la nivel central și local, a produselor și serviciilor software de tip antivirus provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărei capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă.

(2) Este considerat operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă acela care se află în cel puțin una dintre următoarele situații:

a) una sau mai multe persoane fizice sau juridice din Federația Rusă dețin, individual sau împreună, în mod direct sau indirect, o participație calificată de cel puțin 25% din drepturile de vot ale respectivului operator;

b) una sau mai multe persoane fizice sau juridice din Federația Rusă dețin, în mod direct sau indirect, majoritatea drepturilor de vot în adunarea generală a operatorului respectiv;

c) în calitate de asociat sau acționar al respectivului operator, o persoană fizică sau juridică din Federația Rusă dispune de puterea de a numi sau de a revoca majoritatea membrilor organelor de administrație, conducere sau supraveghere;

d) una sau mai multe persoane fizice sau juridice din Federația Rusă finanțează, prin orice mod, direct sau indirect, pe operator;

e) una sau mai multe persoane fizice sau juridice din Federația Rusă promite, oferă sau dă bani sau alte foloase operatorului.

(3) Scopul prezentei legi este prevenirea și contracararea amenințărilor cibernetice, derulate de entități ostile, statale și non-statale, asupra infrastructurilor de comunicații și tehnologia informației cu valențe critice pentru securitatea națională.

**Art. 2.**

(1) Se interzice achiziționarea, instalarea și utilizarea de către instituțiile publice centrale și locale a următoarelor produse și servicii software , care îndeplinesc criteriile din art. 1:

a. produse privind securitatea dispozitivului, securitatea punctului final;

b. aplicații și programe software de detecție antivirus;
c. aplicații și programe software anti malware, firewall pentru aplicații web, firewall as a service;
d. rețele virtuale private;
e. sisteme de detecție și răspuns pentru Endpoint-uri;

(2) În aplicarea prevederilor art. 1 și art. 2 alin.(1), prin ordin al ministrului cercetării, inovării și digitalizării se adoptă, în termen de 15 zile de la intrarea în vigoare a prezentei legi, criteriile de stabilire și lista nominală privind produsele, serviciile și entitățile producătoare și furnizoare interzise, care va fi actualizată semestrial sau ori de câte ori este nevoie, după caz.

(3) În aplicarea prevederilor art. 1, alin. (2) și ale art. 2, alin. (2), Ministerul Cercetării, Inovării și Digitalizării, denumit în continuare MCID, solicită puncte de vedere Ministerului Finanțelor, Ministerului Economiei, Serviciului Român de Informații și Serviciului de Informații Externe.

**Art. 3.**

Interdicția prevăzută la art. 2 produce efecte până la data de 31 decembrie 2026.

**Art. 4.**

(1) Constituie contravenție următoarele fapte:
a) Cumpărarea, instalarea și utilizarea produselor și serviciilor prevăzute la art. 2 alin.(1);
b) Nedezinstalarea/nedeconectarea produselor și serviciilor în termenul prevăzut la art.5 alin.(2).

(2) Prin derogare de la prevederile art. 8 alin. (2) lit. a) din OG nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, nerespectarea de către autoritățile și instituțiile publice a prevederilor alin. (1) constituie contravenție și se sancționează cu amendă de 50.000 lei la 200.000 lei.

(3) Constatarea și aplicarea contravențiilor se fac de către personal anume desemnat prin ordin al ministrului cercetării, inovării și digitalizării.

(4) 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. 5.**

(1) În aplicarea prevederilor art. 2 alin. (1) , în termen de 15 zile de la intrarea în vigoare a prezentei legi, prin ordin al ministrului cercetării, inovării și digitalizării se stabilesc mecanismele necesare încetării utilizării produselor și serviciilor interzise.

(2) În termen de 60 de zile de la intrarea în vigoare a ordinului prevăzut la alin. (1), 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 centrale și locale.

(3) În aplicarea prevederilor art. 2 alin. (2 ), MCID identifică produsele și serviciile prevăzute la art. 2 alin. (1), la propunerea Autorității pentru Digitalizarea României, al

Directoratului Național de Securitate Cibernetică, al Serviciului Român de Informații, al Ministerului Apărării Naționale, al Ministerului Afacerilor Interne, al Serviciului de Telecomunicații Speciale, al Serviciului de Protecție și Pază și al Oficiului Registrului Național al Informațiilor Secrete de Stat.

(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. 2 alin. (1), cu respectarea legislației privind achizițiile publice și a termenului prevăzut la alin. (2) pentru asigurarea continuității activității, cu încadrarea în bugetul autorităților și instituțiilor publice .

(5) Prevederile prezentei legi nu se aplică autorităților și instituțiilor publice cu atribuții proprii în domeniul securității naționale, în domeniul securității cibernetice, apărării naționale și ordinii publice.

*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**