EXPUNERE DE MOTIVE

Secțiunea 1:
Titlul proiectului de act normativ
LEGE
privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative

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 în temeiul art. 1, alin. (3) și art. 4, alin. (1) din HG nr. 371/2021.
MCID inițiază proiectul de lege, în calitate de coordonator de reformă, pe Componenta C7 - Transformare digitală, reforma 3 din Programul Național de Redresare și Reziliență, conform Anexei la OUG nr. 124/2021 coroborat cu Acordul de finanțare dintre MIPE și MCID.

2.2 Descrierea situației actuale

În contextul tot mai intensei digitalizări a întregului spectru de relaționare și comunicare, securitatea și apărarea cibernetică reprezintă o prioritate pentru fiecare stat.

În condițiile transpunerii în legislația națională a prevederilor Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune, cunoscută ca Directiva NIS, prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, coroborate cu prevederile art. 72 din Tratatul privind funcționarea Uniunii Europene au devenit evidente responsabilitatea națională și necesitatea reglementării domeniului securității și apărării cibernetice.

Totodată, preocupările Uniunii Europene în domeniul securității cibernetice și interesul pentru dezvoltarea acestuia transpar din deciziile anunțate în decembrie 2020 de elaborare a unei noi strategii de securitate cibernetică, de stabilire la București a Centrului European de Competență Industrială, Tehnologică și Cercetare în domeniul securității cibernetice, precum și din intenția de extindere a prevederilor Directivei (UE) 2016/1148, respectiv Directiva NIS 2.

Agresiunile cibernetice sunt caracterizate de un nivel ridicat de risc, cu tendințe de evoluție în creștere a impactului şi probabilității de materializare, vizând cu predilecție rețelele și sistemele informatice ale instituțiilor publice, sau care susțin furnizarea de servicii publice ori de interes public.

Problematica securității și apărării cibernetice, ca dimensiune a securității naționale, a devenit prioritară, astfel că sunt necesare demersuri de reglementare pentru dezvoltarea de mecanisme coerente şi eficiente pentru asigurarea securității și apărării rețelelor și sistemelor informatice de interes național.
În prezent nu există cadrul legislativ care să creeze cadrul de cooperare operațională directă, concretă și coerentă, care să stabilească responsabilitățile şi atribuțiile specifice pentru asigurarea apărării cibernetice la nivel național.

Pentru a implementa prevederile *Hotărârii de Guvern nr. 1321/2021 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*, precum și pentru a asigura complementaritatea cu prevederile *Ordonanței de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată prin Legea 11/2022 pentru aprobarea Ordonanței de urgență a Guvernului numărul 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică* și cu măsurile privind apărarea cibernetică este nevoie de elaborarea unei legi care să integreze aspectele specifice, manifestate în spațiul cibernetic.

Prin Programul Național de Redresare și Reziliență (PNRR), România și-a asumat implementarea măsurii „Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice" (Componenta 7 - Transformare digitală – Reforma 3). În jalonul 151, indicatorul de implementare prevede „Dispoziție legală care indică intrarea în vigoare a Legii privind apărarea și securitatea cibernetică a României". Conform negocierilor și angajamentelor rezultate prin PNRR, Legea privind apărarea și securitatea cibernetică a României trebuie să stabilească cadrul juridic și instituțional pentru organizarea și desfășurarea activităților din domeniul securității cibernetice și al apărării cibernetice, mecanismele de cooperare și răspunsurile instituțiilor în domeniile în cauză.

Date fiind incertitudinile conceptuale și diferențele de interpretare a prevederilor Dreptului Internațional Public aplicate domeniului cibernetic, în special în privința atribuirii activității cibernetice răuvoitoare, precum și inexistența unor inițiative internaționale similare, demersurile pentru crearea unui proiect de Lege a securității și apărării cibernetice viabil au trebuit să exploreze concepte, incidente și soluții din mediul internațional, care să fie raportate la realitățile și specificul legislației și instituțiilor naționale.

Totodată, dezvoltarea la nivel național a unor capabilități specializate, cu arii de acțiune delimitate, așa cum este de exemplu Comandamentul Apărării Cibernetice din cadrul Ministerului Apărării Naționale, crește necesitatea relaționării operaționale interinstituționale flexibile.

De asemenea, dezvoltarea entităților specializate la nivelul instituțiilor din domeniile apărării, ordinii publice și securității naționale permite abordarea unui spectru larg de incidente și atacuri cibernetice în deplină capacitate de reacție.

Crearea unui cadru de relaționare și cooperare între autoritățile cu competențe în domeniul securității și apărării cibernetice oferă posibilitatea utilizării eficiente a resurselor, inclusiv prin dezvoltarea și exploatarea în comun a unor capabilități specializate.

Diplomația cibernetică constituie, deopotrivă, un domeniu în care pot fi promovate prioritățile generale de politică externă ale României, cât și o parte integrantă a procesului de asigurare și consolidare a securității cibernetice naționale prin promovarea intereselor naționale în acțiunile diplomatice bilaterale și multilaterale în acest domeniu și prin participarea coordonată în acțiunile, negocierile și formatele de cooperare privitoare la asigurarea comună a securității, păcii și stabilității în spațiul cibernetic, promovarea valorilor democratice, protejarea drepturilor și libertăților fundamentale ale omului și acțiunea comună la nivel internațional ca răspuns la amenințările cibernetice. De aceea, se impune o reglementare expresă cu prilejul prezentului proiect, care să confere mecanismele legale necesare MAE în exercitarea atribuțiilor.

Accentuarea necesității de stabilire a responsabilităților și competențelor, la nivel național, a fost determinată de utilizarea extensivă a mediului online pentru desfășurarea activităților lucrative și educaționale, din cauza restricțiilor impuse de pandemia de SARS-CoV-2.

În lipsa acestei legi, statul român nu va dispune de pârghiile necesare diminuării vulnerabilităţilor de securitate cibernetică şi asigurării apărării cibernetice, în scopul reducerii riscurilor la adresa securității rețelelor și sistemelor informatice ale statului.
Prezentul proiect a fost întocmit cu luarea în considerare a criticilor aduse prin Decizia nr. 17/2015 a Curţii Constituţionale asupra obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind securitatea cibernetică a României.

România este prezentă pe harta țintelor atacurilor cibernetice, confruntându-se permanent, atât cu atacuri complexe, care au ca scop obținerea unor avantaje strategice sau a unor beneficii financiare, cu potențial impact major la adresa securității naționale, societății și economiei, cât și cu atacuri "clasice", care folosesc malware comun și exploatează vulnerabilități larg răspândite și cunoscute, și care, deși au un potențial redus de a aduce atingere securității naționale, afectează economia și societatea. Aceste atacuri cibernetice afectează, de multe ori, infrastructuri critice naționale care slăbesc capacitatea statului de a funcționa, blocând servicii publice elementare, funcționare aparatului guvernamental și pun în pericol ordinea constituțională. De aceea, este nevoie de măsuri concrete pentru a preveni și combate aceste realități, prin mecanismele constituționale și legale adaptate la noile tipuri de amenințări din spațiul virtual.

2.3 Schimbări preconizate

Proiectul Legii privind securitatea și apărarea cibernetică este un proiect legislativ nou, care reglementează cadrul juridic și instituțional referitor la organizarea și desfășurarea activităților din domeniile securitate cibernetică și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate.

Obiectivele prezentului proiect de lege sunt:
1. Crearea de rețele și sisteme informatice sigure și reziliente;
2. Elaborarea și adoptarea unui cadru normativ și instituțional consolidat;
3. Consolidarea unui parteneriat public-privat, pragmatic, pe linia securității cibernetice;
4. Asigurarea rezilienței prin abordare proactivă și descurajare;
5. Transformarea României într-un actor relevant în arhitectura internațională de cooperare în domeniul securității cibernetice.

Conceptul de securitate cibernetică reglementat prin prezentul proiect de lege se bazează pe următorii piloni:

1. Securitatea națională a României;
2. Apărarea națională a României;
3. Asigurarea rezilienței naționale a statului român: prevenție, răspuns, restabilire, capacitate funcționare stat, protecție societate.
4. Respectarea Directivei NIS;
5. Prevenirea și combaterea pericolelor la adresa securității cibernetice în sectorul public și privat: actori statali și nonstatali ostili, criminalitate, conflicte și crize.

În domeniul securității cibernetice prezentul proiect de lege are ca obiect stabilirea cadrului general de reglementare pentru:

a) rețelele și sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat.
b) rețelele și sistemele informatice deținute de persoanele fizice și juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale.
c) rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de autorități și instituții ale administrației publice centrale și locale, altele decât cele

prevăzute la lit. a), precum și de persoane fizice și juridice care desfășoară activități cu scop lucrativ și nelucrativ, de cercetare, dezvoltare, inovare și producție în domeniul tehnologia informației și a comunicațiilor, sau furnizează servicii publice ori de interes public, altele decât cele de la lit. b).

Adoptarea prezentului proiect de lege va institui, la nivel naţional, un cadru normativ care va permite crearea instrumentelor instituționale și a mecanismelor de acțiune integrată și cooperare interinstituțională în domeniile securitate şi apărare cibernetică, prin:

- definirea domeniilor de activitate, atribuțiilor și responsabilităților fiecărei instituții/autorități în domeniul securității cibernetice la nivel național;
- definirea rolului, compunerii și atribuțiilor Consiliului Operativ de Securitate Cibernetică, ca mecanism de coordonare a instituțiilor din domeniile apărare, ordine publică și securitate națională și a DNSC; COSC este organ consultativ aflat în coordonarea CSAT, care emite avize consultative și recomandări (operațiuni administrative).
- stabilirea atribuțiilor și domeniilor de competență ale DNSC și ale celorlalte autorități, delimitate strict și în concordanță cu natura juridică a fiecărei autorități;
- organizarea sistemului de management a incidentelor de securitate cibernetică, la nivel național. În acest sens, au fost stabilite responsabilitățile privind managementul incidentelor de securitate cibernetică adecvate fiecărei instituții din domeniul apărării, ordinii publice și securității naționale, precum și posibilitățile de cooperarea interinstituțională, inclusiv cu DNSC, pentru situațiile în care capacitățile proprii de asigurare a securității sunt depășite sau există riscul propagării efectelor incidentului de securitate cibernetică în alte rețele;
- definirea sistemului național de alertă cibernetică și a atribuțiilor instituțiilor/autorităților în situații de alertă;
- reglementarea aspectelor privind asigurarea rezilienței rețelelor și sistemelor informatice, la nivel național, în spațiul cibernetic;
- stabilirea cadrului general de reglementare pentru acțiunile militare în spațiul cibernetic. Astfel, a fost introdus conceptul de rezervă de specialiști în securitate și apărare cibernetică, au fost stabilite responsabilități privind procesul de reglementare și constituire a acestei rezerve de specialiști și au fost incluse prevederi referitoare la responsabilitățile instituțiilor din domeniile securității, ordinii publice și securității naționale privind formarea profesională şi instruirea în domeniul securității și apărării cibernetice;
- reglementarea anumitor aspecte privind cercetarea, dezvoltarea, inovarea în domeniul securității cibernetice;
- stabilirea cadrului de cooperare, la nivel național și în relațiile internaționale, în domeniul securității, precum și în privința apărării cibernetice, unde MApN este autoritate competentă.

Astfel, prin intermediul arhitecturii de cooperare interinstituțională instituită prin această lege, se asigură o coerență crescută în ceea ce privește răspunsul la incidente sau atacuri cibernetice, precum și responsabilități clare și predictibilitate în ceea ce privește tipul de acțiuni desfășurate de fiecare instituție din domeniile apărării, ordinii publice și securității naționale.

De asemenea, abordarea acestui proiect de lege privind securitatea și apărarea cibernetică permite un răspuns coerent, ajustat, proporțional și efectiv, indiferent de situație, pornind de la un incident de securitate izolat, până la un atac cibernetic complex efectuat la nivelul unei instituții, sau asupra mai multor rețele și sisteme informatice aflate în responsabilitatea mai multor instituții.

Implementarea măsurilor menționate va contribui la creşterea nivelului de securitate cibernetică a reţelelor publice pe plan naţional şi internaţional şi va preveni apariţia unor situaţii în care

rețele și sisteme informatice naţionale sunt utilizate pentru propagarea campaniilor de atacuri cibernetice împotriva rețelelor și sistemelor informatice aparținând altor state.

Adoptarea prezentei legi oferă posibilitatea instituţiilor publice să colaboreze cu entitățile din sectorul privat și din mediul academic, cu asociaţiile profesionale şi organizaţiile neguvernamentale.

Totodată, această lege stabilește un cadru armonizat de acţiune a autorităţilor şi instituţiilor publice cu responsabilităţi şi capabilităţi specifice contracarării ameninţărilor cibernetice.

Având în vedere contextul în care, la nivelul Alianței Nord-Atlantice, s-a luat decizia de declarare a spațiului cibernetic ca mediu operaţional de ducere a operaţiilor militare, prin prezentul proiect de act normativ sunt create mecanismele pentru ca Ministerului Apărării Naţionale şi celelalte autorități publice din domeniul apărării, ordinii publice şi securităţii naţionale să poată realiza acțiuni și să poată implementa politici şi standarde în domeniul apărării cibernetice.

Interconectarea rețelelor și sistemelor informatice și de comunicații și a infrastructurilor susținute de acestea la nivel regional și internațional și dependențele în lanțul de aprovizionare TIC au condus la situații în care atacurile cibernetice asupra unui stat, pot avea consecințe și impact semnificativ asupra altor state sau chiar regiuni, făcând necesară dezvoltarea relațiilor între state la nivel bilateral și regional specifică asigurării securității cibernetice, stabilirea încrederii, asistența reciprocă în dezvoltarea capacităților de a face față amenințărilor, schimbul de informații și coordonarea și răspunsul comun la amenințările din spațiul cibernetic.
În același timp, relațiile dintre state au în prezent o componentă semnificativă care se desfășoară prin intermediul spațiului cibernetic ori utilizând tehnologiile comunicațiilor și informației.
Motivat de evoluția rapidă a problematicii securității cibernetice la nivel internațional, a impactului asupra păcii și stabilității pe care o are utilizarea tehnologiilor informației și comunicațiilor, a nevoii de asigurare a unui comportament responsabil în spațiul cibernetic dar și a unui răspuns comun al statelor în fața amenințărilor cibernetice, activitatea diplomatică în legătură cu aceste elemente a devenit omniprezentă atât în relațiile bilaterale cât și în formatele de cooperare și negocierile de la nivelul organizațiilor internaționale și regionale, fiind parte integrantă a politicilor și strategiilor de securitate cibernetică naționale și a mecanismelor naționale de asigurare a securității cibernetice.
Având în vedere complexitatea problematicilor securității cibernetice, este necesară o abordare de tipul whole-of-government care să adreseze multitudinea de dimensiuni și domenii de expertiză aferente, prin asigurarea unor mecanisme de cooperare adecvată care să permită adaptarea la evoluțiile rapide din domeniul securității cibernetice sub toate aspectele. De aceea, proiectul de lege prevede o componentă solidă, proactivă și ambițioasă de diplomație cibernetică.
Strategia de Securitate Cibernetică a României prevede ca obiective de politică externă în domeniul securității cibernetice, consolidarea rolului României la nivel global, consolidarea rolului României la nivel regional și pe plan bilateral, precum și consolidarea rolului diplomației cibernetice, elemente care necesită pe plan intern cooperare, dialog interinstituțional, informare reciprocă și coordonare între MAE și instituțiile naționale cu competențe în domeniul securității cibernetice pentru asigurarea unei reprezentări adecvate și a unui mesaj coerent în acțiunea externă a României, printr-o diplomație cibernetică eficientă.

Având în vedere că atacurile și amenințările cibernetice pot paraliza complet instituții publice, infrastructuri critice și servicii publice, este nevoie ca statul să poată institui situațiile excepționale, la nevoie, în acord cu limitele și condițiile impuse de Constituție. Pentru a da această prerogativă autorităților competente, proiectul de lege prevede posibilitatea instituirii stării de asediu sau de urgență pentru rațiuni de securitate cibernetică și apărare cibernetică, prevederile prezentului proiect completându-se corespunzător cu Ordonanţa de urgenţă a

Guvernului nr. 1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, publicată în Monitorul Oficial, Partea I nr. 22 din 21 ianuarie 1999, cu modificările și completările ulterioare. Proiectul de lege nu modifică conținutul și regimul juridic al stării de urgență și de asediu reglementat de OUG nr. 1/1999, ci instituie doar cauzele de securitate cibernetică și apărare cibernetică drept rațiuni/ motive de instituire a acestor stări excepționale. Prin prezenta măsură se asigură o actualizare a cauzelor de instituire a stărilor excepționale raportate la noile tipuri de amenințări și riscuri care afectează statele moderne.

Cu privire la introducerea definirii conceptului de cyber intelligence, în cadrul acestuia sunt înglobate *per se* activități, mijloace și măsuri de securitate cibernetică care au ca scop asigurarea stării de normalitate a rețelelor și sistemelor informatice. Componenta de securitate cibernetică aferentă activităților de cyber intelligence vizează asigurarea securității naționale, prin aplicarea unui set de măsuri proactive și reactive la nivelul rețelelor și sistemelor informatice din plan național, menite să asigurea confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice.
Situația actuală, la nivel internațional, demonstrează imposibilitatea separării amenințării cibernetice de celelalte tipuri de amenințări la adresa securității naționale. Instrumentele specifice operațiunilor cibernetice au fost adoptate de toate categoriile de vectori de amenințare, de la extremism și terorism la criminalitate organizată transfrontalieră și spionaj. În prezent, actorii statali ostili derulează operațiuni cibernetice complexe prin care vizează atingerea unor obiective strategice proprii la nivel internațional, generând un impact semnificativ în planul intereselor de securitate națională ale țărilor afectate, prin exfiltrarea unor cantități foarte mari de date sensibile și creându-și inclusiv capacitatea de a afecta funcționalitatea sistemelor respective.

La nivel conceptual, securitatea cibernetică nu poate fi separată de securitatea națională, fiind o dimensiune cu relevanță din ce în ce mai crescută a acesteia. Exemple în acest sens se regăsesc la nivel internațional:
- în ianuarie 2022, administrația Biden a declarat că Securitatea cibernetică este un imperativ de securitate națională și securitate economică, cu un nivel crescut, fără precedent de prioritate la nivelul SUA;
- în Strategia Națională pentru Securitate Digitală a Franței, se precizează că riscurile cibernetice reprezintă a treia prioritate pe lista amenințărilor, conform White Paper privind Apărarea și Securitatea Națională;
- Strategia de securitate cibernetică a Marii Britanii pentru anul 2022 face referire extensivă la amenințările cibernetice diverse și complexe la adresa securității naționale, precum și la necesitatea implicării instituțiilor de securitate națională cu măsuri pentru atingerea obiectivelor de securitate cibernetică

Practica a demonstrat faptul că activitățile de culegerea de informații reprezintă o condiție sine qua non în combaterea amenințărilor cibernetice complexe. Activitatea de culegere de informații s-a dovedit esențială pentru obținerea, prin mijloace specifice (HUMINT, OSINT, TECHINT, SIGINT, cooperare etc.) de date tehnice cu privire la tacticile, tehnicile și procedurile atacatorilor, infrastructurile utilizate, țintele predilecte ale operațiunilor cibernetice și chiar atacurile aflate în derulare. Aceste date s-au dovedit esențiale pentru creșterea capabilităților infrastructurii tehnice de securitate cibernetică, făcând posibilă detectarea unor incidente și atacuri cibernetice de tip APT în rețelele și sistemele informatice care asigură funcții esențiale pentru statul român.

Astfel, în cursul anilor, utilizarea sinergică a activităților de informații și a sistemelor tehnice de securitate cibernetică s-a dovedit a fi cel mai eficient instrument pe linia asigurării securității cibernetice care permite derularea unor măsuri specifice de cyberintelligence pe dimensiunea cunoașterii, prevenirii și contracarării amenințărilor cibernetice prin:

- detectarea, în timp real, a unui număr semnificativ de atacuri cibernetice complexe (de tip advanced persistent threat - APT) care au vizat rețelele și sistemele informatice din țara noastră;
- monitorizarea alertelor de securitate cibernetică și a aplicării de măsuri de protecție și de prevenire a răspândirii aplicațiilor malware în rețelele și sistemele informatice de la nivel național;
- protejarea instituțiilor de atacuri cibernetice derulate de atacatori prin rețelelor și sistemelor informatice cu întindere transfrontalieră care permit realizarea de spionaj cibernetic, blocarea sistemelor în vederea obținerii de beneficii financiare(ransomware) sau activități de activism sau cu motivație ideologică.
- eliminarea sau limitarea efectelor produse în urma unor atacuri cibernetice asupra rețelelor și sistemelor informatice naționale, restaurarea funcționalității, precum și asigurarea rezilienței cibernetice a acestora.

Combaterea amenințărilor cibernetice complexe la adresa securității naționale îndreptate de actori statali ostili împotriva României, caracterizate de creșterea exponențială a complexității tehnice a APT-urilor care face extrem de dificilă identificarea lor, reclamă utilizarea întregii game de măsuri de culegere de informații pentru prevenirea și combaterea lor.

Pentru a da relevanță practică conceptelor de cyber intelligence și counter-cyberintellicence, prin proiectul de lege se completează art. 3 din Legea nr. 51/1991 privind securitatea națională a României cu următoarele tipuri de amenințări:

1. amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național;

Conceptul de amenințare cibernetică este definit la art. 2, lit. b) din proiectul de lege, cu trimitere la art. 2 lit. f) din Ordonanța de Urgență a Guvernului nr. 104/2021;
Conceptul de atac cibernetic este definit la art.2, lit. c) din proiectul de lege ca fiind ”*acțiune ostilă (de rea-credință) desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică*”.
Conceptul de infrastructură informatică și de comunicații de interes național este definită de art. 2, lit.d) din Legea nr. 163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice și de comunicații de interes național și condițiile implementării rețelelor 5G.
Astfel, apreciem că acest tip de amenințare prezintă toate garanțiile de calitate, claritate și previzibilitate a legii impuse de prevederile art. 1, alin. (5) din Constituția României, republicată.

2. acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului român în raport cu riscurile și amenințările de tip hibrid;

Conceptul de reziliență este amplu definit în mai multe acte normative la nivelul statului român, plecându-se de la definiția rezilienței în spațiul cibernetic, prevăzută la art. 2 lit.v) din proiectul lege, până la dezvoltarea conceptului în Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024, Hotărârea Guvernului nr. 1321/2021 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, Ordonanţei de Urgenţă a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă, precum și a Ordonanţei de Urgenţă a Guvernului nr. 124/2021 privind stabilirea cadrului instituţional şi financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare şi rezilienţă, precum şi pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă.

Riscurile și amenințările de tip hibrid la adresa securității cibernetice sunt acele amenințări și riscuri cibernetice, astfel cum sunt definite în art. 2, lit. b) și w) din proiectul de lege, care se manifestă sub formă hibridă. Forma hibridă a amenințărilor și riscurilor de securitate cibernetică este conceptualizată prin Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024.
Astfel, apreciem că acest tip de amenințare prezintă toate garanțiile de calitate, claritate și previzibilitate a legii impuse de prevederile art. 1, alin. (5) din Constituția României, republicată.

3. acțiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spațiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituțională.

Prin Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024 s-a stabilit ca obiectiv strategic ”*prevenirea şi contracararea riscurilor de natură teroristă asociate activităţilor unor organizaţii de profil, prezenţei pe teritoriul naţional a membrilor sau adepţilor unor astfel de entităţi, intensificării propagandei extremist-jihadiste, în special în mediul online, şi a proceselor de radicalizare în România.”*
Acţiunile informative ostile continuă să vizeze dezvoltarea unor puncte de sprijin, utilizate în scop de influenţă, obţinerea de informaţii cu privire la evoluţiile interne, necesare susţinerii proceselor decizionale din statele de provenienţă, dar şi pentru rafinarea şi dezvoltarea bazelor de sprijin şi a canalelor de propagandă, cu potenţial de obstrucţionare a proiectelor strategice ale României şi a deciziilor în stat. Parteneriatele strategice ale României şi politicile promovate în acord cu statutul de membru al UE şi NATO menţin ţara noastră în atenţia spionajului străin, nivelul de intruziune şi ofensivitate oscilând în funcţie de interesele statelor agresoare în raport cu Bucureştiul şi alianţele sau parteneriatele noastre.
Prin aceeași strategie de apărare a țării s-a constatat, ca vulnerabilitate, ”*persistenţa unor lacune legislative în domeniul securităţii naţionale sau în ceea ce priveşte contracararea agresiunilor informaţionale, respectiv pe palierul reglementării instrumentelor necesare prevenirii şi contracarării propagandei cu scop destabilizator, inclusiv în eventualitatea unor campanii de tip hibrid”.*
Direcțiile de acțiune pe linia de informații, contrainformații și de securitate, conform SNAp 2020-2024, vizează și ”*Prevenirea şi contracararea riscurilor asociate activităţilor unor entităţi teroriste, prezenţei pe teritoriul naţional a membrilor sau simpatizanţilor unor asemenea entităţi, intensificării propagandei extremist-teroriste, în special a celei jihadiste în ascensiune în mediul online, şi a proceselor de radicalizare în România”.*
Ținând cont de cele anterioare, apreciem necesară instituirea, la nivelul legii, a unor noi tipuri de amenințări care să răspundă nevoilor de securitate cibernetică și securitate națională a României, astfel încât să se asigure cu succes protejarea cetățenilor și a statului român.
Acțiunile de propagandă și dezinformare vizate sunt doar cele care afectează ordinea constituțională, adică setul de principii fundamentale pe care este constituit statul român, regimul constituțional de drepturi și libertăți fundamentale, regimul constituțional al funcționării autorităților publice de rang constituțional protejarea garanțiilor prevăzute de Constituție.

Menționăm că aceste amenințări instituite au relevanță doar pentru activitatea de informații și contrainformații, activitate desfășurată doar de autoritățile competente potrivit art. 6 din Legea nr. 51/1991. Prin prezentul proiect de lege nu se pot desfășura activități de natură a restrânge exercițiul unor drepturi și libertăți fundamentale și nici activități specifice culegerii de informații, precum nici activități de contrainformații. Prezenta lege reglementează activitatea de cyberintelligence și counter cyber intelligence doar la nivel conceptual, urmând ca definițiile să se completeze corespunzător cu dreptul material prevăzut în Legea nr. 51/1991 și alte legi speciale din domeniul securității naționale.

Prezentul proiect de lege nu afectează legislaţia naţională privind protecţia datelor cu caracter personal, în special Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi

protecţia vieţii private în sectorul comunicaţiilor electronice, cu modificările şi completările ulterioare, Directiva 2002/58/CE a Parlamentului European şi a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale şi protejarea confidenţialităţii în sectorul comunicaţiilor publice (Directiva asupra confidenţialităţii şi comunicaţiilor electronice), cu modificările şi completările ulterioare, și Regulamentul (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), cu modificările ulterioare.

Prezentul proiect de lege respectă drepturile fundamentale şi principiile recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la respectarea vieţii private şi de familie, dreptul la protecţia datelor cu caracter personal, dreptul la proprietate şi integrarea persoanelor cu dizabilităţi, astfel încât nicio prevedere din prezenta lege nu trebuie să facă obiectul unei interpretări sau puneri în aplicare care nu este conformă cu Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale a Consiliului Europei.

Cu privire la prevederile art. 51 alin. 2 din proiectul de lege, prin care se derogă de la prevederile art. 8, alin. (2), lit. a) din OG nr. 2/2001, apreciem că soluția majorării limitelor maxime ale amenzilor pentru necomunicarea informațiilor privind incidentele cibernetice este justificată de amplitudinea fenomenului atacurilor și amenințărilor cibernetice care gravitează asupra României, atât în contextul transformării digitale a țării cât și a conflictelor de tip hibrid și convențional de la granițele statului. De aceea, este nevoie de o strânsă cooperare între toți furnizorii de servicii de securitate cibernetică, pe de-o parte, și autoritățile publice cu atribuții în domeniul securității cibernetice, pe de altă parte, pentru a asigura un nivel ridicat și constant de securitate cibernetică la nivel național.
Cu privire la prevederile art. 52 alin. (4) din proiectul de lege, privind majorarea termenului de prescripție a răspunderii contravenționale, pentru contravențiile reglementate prin prezentul proiect, se impune ca urmare a multitudinii de potențiali subiecți activi ai contravenției și numărului limitat de autorități competente, potrivit proiectului, în constatarea și aplicarea contraventiei. Mai mult, de multe ori se impune o analiză atentă pentru constatarea și individualizarea faptei contravenționale, astfel încât să se stabilească caracterul sancțiunii sub aspectul proporționalității.
Cu privire la prevederile art. 52 alin. (9) din proiectul de lege, apreciem că, pe de-o parte, se impune celeritatea procedurii contestării amenzii, facilitată de eludarea oricărei proceduri prealabile, iar, pe de altă parte, se impune specializarea instanței care judecă actul administrativ prin care se constată și se aplică contravenția, în acest sens apreciind că instanța de contencios administrativ și fiscal fiind cea mai în măsură să judece astfel de cauze.
Prevederile art. 51 și 52 din proiectul de lege se circumscriu elementelor care trebuie să compună o normă juridică (ipoteză, dispoziție și sancțiune). Astfel, prin instituirea contravențiilor și sancțiunilor anterior menționate să oferă garanții de aplicabilitate a normelor prevăzute la art. 22 și 26 din proiect.
Apreciem că dispozițiile sancționatorii respectă criteriile de prevăzute de art. 53 din Constituție, încadrându-se în limitele și condițiile tipurilor de contravenții din domeniul ITC (ex: Legea nr. 362/2018, Legea nr. 242/2022 și OUG nr. 104/2021).

Proiectul de lege este realizat în condiții de corelare cu legile care privesc activitatea DNSC și este avizat favorabil de DNSC, confirmând astfel prevenirea riscurilor referitoare la o eventuală atingere sau diluare a prerogativelor DNSC ca autoritate națională în domeniul securității cibernetice pentru spațiul cibernetic civil.

DNSC își păstrează în continuare statutul de autoritate națională în domeniu și primește prerogative de coordonare a activităților tehnice referitoare la gestionarea incidentelor cibernetice pe timp de pace.

Celelalte autorități se supun în continuare limitelor stabilite de legile proprii de funcționare, prezentul proiect de lege aducând o detaliere privind modalitatea de abordare a acestora în spațiul cibernetic. Mai mult, se are în vedere crearea unor repere pentru delimitarea jurisdicțiilor și a competențelor dintre acestea, pentru eficientizarea operațională și eliminarea situațiilor de suprapunere, acolo unde este cazul, în practică, întrucât există multe ariile de competență instituțională comune.

În plus, controlul și departajarea operațională sunt asigurate în permanență prin cooperare și sincronizare la nivel înalt (prin COSC și sub coordonarea CSAT). Când situația o impune, CSAT asigură operativitatea răspunsului rapid la incidente cibernetice care pot aduce atingere securității și apărării naționale. Astfel, este creat un mecanism flexibil, care permite funcționarea corectă a instituțiilor atât pe timp de pace, cât și în situații de criză cibernetică.

PNRISC se află în spațiul civil, sub control democratic, fiind gestionat de DNSC în calitate de autoritate națională civilă în domeniul securității cibernetice.

Controlul instituțiilor din SNAOPSN se realizează conform legilor în vigoare iar prezentul proiect de lege nu modifică atribuțiile autorităților publice în domeniul securității naționale și nici nu naște noi atribuții în sarcina unor autorități care nu au astfel de atribuții în domeniul securității naționale.

Prezenta lege nu intră în contradicție și nu dublează Legea nr. 362/2018 și Legea nr. 104/2021, ci le completează în vederea creării unei arhitecturi legislative cuprinzătoare și satisfăcătoare pentru domeniul securității și apărării cibernetice. Prezentul proiect de lege și cele două legi menționate formează un pachet legislativ coerent, corelat, care asigură facilitare în dezvoltare și eficiență în implementarea de măsuri și capabilități reale de securitate și apărare cibernetică. În lipsa sincronizării și cooperării în timp real, autoritățile statului pierd din start lupta împotriva amenințărilor existente în spațiul cibernetic, care - prin natura lor - au un grad spectaculos de agilitate și complexitate.

2.4 Alte informații

Dat fiind ritmul rapid de evoluţie a tehnologiilor, precum şi modificarea cadrului legislativ la nivel NATO şi UE, legea va fi analizată şi revizuită periodic, în vederea adaptării continue la provocările şi oportunităţile generate de un mediu de securitate în permanentă schimbare.

Secțiunea a 3-a:
Impactul socioeconomic **)

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

Prezentul act normativ va contribui la susținerea procesului de digitalizare a economiei și a serviciilor, inclusiv a celor oferite de către stat, prin asigurarea unui grad ridicat de securitate cibernetică, a unei capacități de reacție instituțională rapidă la incidente din spațiul cibernetic și a unor capabilități robuste de apărare cibernetică în cazul atacurilor cibernetice, asupra rețelelor și sistemelor informatice de interes național.

De asemenea, prin crearea unui sistem integrat de conducere și cooperare în domeniul securității cibernetice care asigură o capacitate sporită de acțiune preventivă și de reacție vor putea fi evitate prejudicii extinse la nivelul operatorilor care desfășoară activități economice în România.

3.2 Impactul social

Atacurile cibernetice, în special asupra serviciilor esențiale ori a infrastructurilor critice pot avea, datorită interconectivității, impact asupra serviciilor furnizate la nivel regional sau internațional, cu efecte destabilizatoare regionale sau internaționale, în plan economic și social, și cu potențiale repercusiuni la adresa păcii și stabilității.

În același timp, noile tehnologii și implementarea rapidă a unei interconectivități sporite în domenii esențiale oferă oportunități reale de creștere economică și dezvoltare socială în România, generând evoluția securității cibernetice ca domeniu de afaceri. Tehnologiile emergente, precum internetul obiectelor (Internet of Things), inteligența artificială (Artificial Intelligence), tehnicile de învățare automată (Machine Learning) și tehnologii de comunicații de bandă (5G și generații viitoare), se pot constitui în oportunități de lansare a unor investiții în contextul dezvoltării procesului industriei 4.0, tehnologiei medicale și mobilității 4.0, precum și al creșterii competitivității economice, atât pe plan național, cât și internațional. Condiția premisă pentru concretizarea tuturor acestor oportunități este asigurarea unui nivel ridicat de securitate cibernetică la nivel național.

Pentru români 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.

Toate aceste măsuri instituite de proiectul de lege generează beneficii economico-sociale majore: existența resursei umane calificate și chiar înalt specializate, capabile să răspundă provocărilor mediului de securitate cibernetică, creșterea contribuției industriei tehnologiei informațiilor și comunicațiilor și de securitate cibernetică la PIB-ul național.

3.3 Impactul asupra drepturilor și libertăților fundamentale ale omului

Prezentul proiect de act normativ nu prezintă prevederi care restrâng exercițiul drepturilor și libertăților fundamentale, cu excepția instituirii unor contravenții prevăzute la art. 51 și art. 52 din proiectul de lege. Menționăm că acestea îndeplinesc elementele prevăzute de art. 53 din Constituția României, republicată.

3.4 Impactul macroeconomic

Proiectul de lege nu se referă la acest subiect.

3.4.1 Impactul asupra economiei și asupra principalilor indicatori macroeconomici

Proiectul de lege nu se referă la acest subiect.

3.4.2 Impactul asupra mediului concurențial si domeniul ajutoarelor de stat

Proiectul de lege nu se referă la acest subiect.

3.5. Impactul asupra mediului de afaceri

Prezentul act normativ va contribui la: creșterea nivelului de cooperare între instituțiile din domeniile apărării, ordinii publice și securității naționale și mediul academic, industria națională de profil sau alți parteneri din mediul public sau privat, inclusiv prin mecanismul rezervei de specialiști în securitate și apărare cibernetică, stimularea cercetării, dezvoltării și inovării în domeniul securității cibernetice, consolidarea securității cibernetice a rețelelor și sistemelor informatice și a serviciilor digitale de interes strategic la nivel național.

3.6 Impactul asupra mediului înconjurător

Proiectul de lege nu se referă la acest subiect.

3.7 Evaluarea costurilor și beneficiilor din perspectiva inovării și digitalizării

Proiectul de lege nu se referă la acest subiect.

3.8 Evaluarea costurilor și beneficiilor din perspectiva dezvoltării durabile

Proiectul de lege nu se referă la acest subiect.

3.9 Alte informații

Proiectul de lege definește noțiunea de diplomație cibernetică drept set de acțiuni diplomatice desfășurate în scopul promovării, susținerii, apărării și protejării, prin dialog internațional și cooperare cu țările partenere și organizațiile internaționale a unui spațiu cibernetic global, deschis, liber, stabil și sigur, în care drepturile omului, libertățile fundamentale și statul de drept se aplică pe deplin pentru bunăstarea socială, creșterea economică, prosperitatea și integritatea societății libere și democratice și care contribuie la prevenirea conflictelor, atenuarea amenințărilor la adresa securității cibernetice și la o mai mare stabilitate în relațiile internaționale. În acest sens, Ministerul Afacerilor Europene este desemnat autoritate națională în domeniul diplomației cibernetice, având rol de coordonare și sprijin pentru activitatea diplomatică, la nivel național.

România, în acest context, devine pionier printre statele membre ONU, reglementându-și, la nivelul legii primare, activitatea de diplomație cibernetică, în scopul garantării angajamentelor internaționale la care este parte.

Secțiunea a 4-a

Impactul financiar asupra bugetului general consolidat atât pe termen scurt, pentru anul curent, cât şi pe termen lung (pe 5 ani), inclusiv informații cu privire la cheltuieli și venituri.*)**

- în mii lei (RON) -

Indicatori	**Anul curent**	**Următorii patru ani**				**Media pe cinci ani**
1	2	3	4	5	6	7
4.1 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						
c) bugetul asigurărilor sociale de stat: i. contribuții de asigurări						
d) alte tipuri de venituri (se va menționa natura acestora)						
4.2 Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta: i. cheltuieli de personal ii. bunuri și servicii						
b) bugete locale: i. cheltuieli de personal ii. bunuri și servicii						
c) bugetul asigurărilor sociale de stat: i. cheltuieli de personal ii. bunuri și servicii						
d) alte tipuri de cheltuieli (se va menționa natura acestora)						

4.3 Impact financiar, plus/minus, din care: a) buget de stat b) bugete locale						
4.4 Propuneri pentru acoperirea creșterii cheltuielilor bugetare						
4.5 Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6 Calcule detaliate privind fundamentarea modificărilor veniturilor și/sau cheltuielilor bugetare						

4.7 Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente:
a) fișa financiară prevăzută la art.15 din Legea nr. 500/2002 privind finanțele publice, cu modificările şi completările ulterioare, însoțită de ipotezele și metodologia de calcul utilizată;
b) declarație conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi prioritățile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.

4.8 Alte informații
Prezentul proiect de lege nu are impact financiar.
Proiectul de lege se încadrează în limitele de cheltuieli aprobate de Guvern pentru anul 2023 și estimările pentru 2024-2026.

Secțiunea a 5-a:
Efectele proiectului de act normativ asupra legislației 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:
-Prin Decizia CCR nr. 455/2018, parag. 63. Curtea a statuat că securitatea rețelelor și sistemelor informatice se află în strânsă legătură cu domeniul securității naționale. Acest aspect este reliefat și în Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024 și HG 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. În acest sens, s-a apreciat că o protecție adecvată a securității cibernetică a României nu se poate realiza fără a se institui și noi amenințări cibernetice la adresa securității naționale a României, amenințări apărute în contextul dezvoltării exponențiale a activităților în spațiul cibernetic.
Astfel, prin proiectul de lege se completează art. 3 din Legea nr. 51/1991 privind securitatea națională a României cu următoarele tipuri de amenințări:

- acțiuni și inacțiuni de natură a afecta interesele și obiectivele naționale de securitate pe linia infrastructurilor de comunicații și tehnologia informației de interes național, respectiv amenințări sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național;
- acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului român în raport cu riscurile și amenințările de tip hibrid;
- acțiuni derulate de către o entitate statală sau grupare ostilă, prin realizarea, în spațiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituțională.

Menționăm că acestea au relevanță doar pentru activitatea de informații și contrainformații, activitate desfășurată doar de autoritățile competente potrivit art. 6 din Legea nr. 51/1991.

b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziții:

1. Categoriile de persoane prevăzute la art. 3, alin. (1), lit. c) din proiectul de lege se stabilesc prin hotărâre de Guvern, inițiată de MCID, adoptată în maximum 60 de zile de la intrarea în vigoare a prezentei legi.
2. Actele administrative prevăzute la art. 19 alin. (2) din proiectul de lege se emit în maximum 90 de zile de la intrarea în vigoare a prezentei legi.
3. În vederea aplicării prevederilor art. 20 alin. (3) din proiectul de lege , politicile de confidențialitate și transparență se emit prin ordin al directorului DNSC în maximum 90 de zile de la data intrării în vigoare a prezentei legi.
4. În vederea aplicării prevederilor art. 24 din proiectul de lege, autoritățile prevăzute la art. 10 adoptă măsuri proprii de reziliență în spațiul cibernetic în maximum 120 de zile de la data intrării în vigoare a prezentei legi.
5. În vederea aplicării prevederilor art. 31 alin. (1) din proiectul de lege , metodologia se emite prin ordin al directorului DNSC în maximum 6 luni de la data intrării în vigoare a prezentei legi.
6. În vederea aplicării prevederilor art. 34 din proiectul de lege , Guvernul adoptă o hotărâre în maximul 90 de zile de la intrarea în vigoare a prezentei legi.
7. În vederea aplicării prevederilor art. 35 alin. (2)-(4) din proiectul de lege , ministrul cercetării, inovării și digitalizării emite un ordin în maximum 120 de zile de la intrarea în vigoare a prezentei legi.

5.2 Impactul asupra legislației în domeniul achizițiilor publice

Proiectul de lege nu se referă la acest subiect.

5.3 Conformitatea proiectului de act normativ cu legislația UE (în cazul proiectelor ce transpun sau asigură aplicarea unor prevederi de drept UE).

Proiectul de lege nu se referă la acest subiect.

5.3.1 Măsuri normative necesare transpunerii directivelor UE

Prezentul proiect de act normativ nu are drept obiect transpunerea Directivei NIS. Prezenta propunere de act normativ urmărește sincronizarea cu Directiva NIS 2 în vederea armonizării măsurilor de securitate cibernetică necesar a fi aplicate la nivel național și reglementate printr-un act ulterior, dedicat acestui scop.

Prin prezentul demers de reglementare, s-a avut în vedere crearea unui cadru juridic general în domeniul securității și apărării cibernetice la nivel național, care să permită și să asigure armonizarea și complementarizarea diferitelor reglementări în domeniu, care au un grad mai ridicat de specificitate și se adresează în mod nișat anumitor sectoare sociale de activitate.

Elaborarea textului de lege a fost realizat ținând cont de necesitățile de corelare atât cu legislația în vigoare (precum Legea nr. 104/2021, Legea nr. 362/2018 sau OUG nr. 111/2011), pregătind în același timp condițiile de sincronizare și cu o viitoare lege care va transpune Directiva NIS 2 și va abroga actuala Lege nr.362/2018.

5.3.2 Măsuri normative necesare aplicării actelor legislative UE

Proiectul de lege nu se referă la acest subiect.

5.4 Hotărâri ale Curții de Justiție a Uniunii Europene

Proiectul de lege nu se referă la acest subiect.

5.5 Alte acte normative şi/sau documente internaționale din care decurg angajamente asumate

Proiectul de lege nu se referă la acest subiect.

5.6. Alte informații

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

6.1 Informații privind neaplicarea procedurii de participare la elaborarea actelor normative
Proiectul de lege nu se referă la acest subiect.

6.2 Informații privind procesul de consultare cu organizații neguvernamentale, institute de cercetare și alte organisme implicate.
În data de 18.11.2022, ora 13, la Universitatea Politehnica din București (UPB), Splaiul Independenței nr. 313, Clădirea Rectorat, etajul 2, Sala Senatului, MCID a organizat o dezbatere publică cu reprezentanți ai mediului academic, organizații neguvernamentale și organizații profesionale din domeniul IT&C.

- https://www.research.gov.ro/uploads/sistemul-de-cercetare/legislatie-organizare-si-functionare/proiecte-de-acte-normative/2022/minute/minuta.pdf;
- https://www.research.gov.ro/ro/articol/6059/comunicare-br-mass-media-anun-privind-modificarea-locului-de-desfa-urare-a-dezbaterii-publice-pentru-proiectul-de-lege-privind-securitatea-i-apararea-cibernetica-a-romaniei.

6.3 Informații despre consultările organizate cu autoritățile administrației publice locale
Proiectul de lege nu se referă la acest subiect.

6.4 Informații privind puncte de vedere/opinii emise de organisme consultative constituite prin acte normative
Proiectul de lege nu se referă la acest subiect.

6.5 Informații privind avizarea de către:
a)Consiliul Legislativ
Se solicită avizul Consiliului Legislativ.
b)Consiliul Suprem de Apărare a Țării
Se solicită avizul Consiliului Suprem de Apărare a Țării.
c)Consiliul Economic și Social
Se solicită avizul Consiliului Economic și Social.
d)Consiliul Concurenței
e)Curtea de Conturi

6.6 Alte informații
S-a solicitat punctul de vedere al Consiliului Superior al Magistraturii prin adresa nr SG/102601/25.11.2022.
S-a solicitat punctul de vedere al Autoritatea Națională pentru Administrare și Reglementare în Comunicații prin adresa SG/102580/24.11.2022.

Secțiunea a 7-a:
Activități de informare publică privind elaborarea şi implementarea proiectului de act normativ

7.1 Informarea societății civile cu privire la elaborarea proiectului de act normativ

Pentru proiectul de act normativ a fost îndeplinită procedura stabilită prin dispozițiile Legii nr. 52/2003 privind transparenţa decizională în administrația publică, republicată.
Prezentul proiect de lege este supus consultării publice potrivit prevederilor art. 7 alin. (13) din Legea nr. 52/2003, termenul de punere în procedura de consultare publică fiind de 10 zile lucrătoare.

Urgența promovării prezentului proiect de act normativ este generată din calendarul de implementare a Programului Național de Redresare și Reziliență (PNRR), în care România și-a asumat implementarea măsurii „Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice” (Componenta 7 - Transformare digitală – Reforma 3). În jalonul 151, indicatorul de implementare prevede „Dispoziție legală care indică intrarea în vigoare a Legii privind apărarea și securitatea cibernetică a României”. Conform negocierilor și angajamentelor rezultate prin PNRR, Legea privind apărarea și securitatea cibernetică a României trebuie să stabilească cadrul juridic și instituțional pentru organizarea și desfășurarea activităților din domeniul securității cibernetice și al apărării cibernetice, mecanismele de cooperare și răspunsurile instituțiilor în domeniile în cauză. Termenul de intrare în vigoare a legii este 31 decembrie 2022. De asemenea, complexitatea atacurilor cibernetice la adresa autorităților și instituțiilor statului român, în contextul războiului din Ucraina, impune adoptarea unei legislații curajoase, care să garanteze funcționarea infrastructurilor critice, siguranța cetățenilor în spațiul cibernetic și buna funcționare a administrației publice.
7.2 Informarea societății civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătății și securității cetățenilor sau diversității biologice.
7.3 Alte informații
Secțiunea a 8-a: **Măsuri privind implementarea, monitorizarea și evaluarea proiectului de act normativ**
8.1 Măsurile de punere în aplicare a proiectului de act normativ
8.2 Alte informații

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

SEBASTIAN-IOAN BURDUJA

AVIZĂM FAVORABIL:

MINISTRUL APĂRĂRII NAȚIONALE

ANGEL TÎLVAR

MINISTRUL AFACERILOR INTERNE

LUCIAN NICOLAE BODE

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE

IONEL SORIN BĂLAN

DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII

EDUARD RAUL HELLVIG

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN SILVAN PAHONȚU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAȚIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL INVESTIȚIILOR ȘI PROIECTELOR EUROPENE

MARCEL-IOAN BOLOȘ

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIȚIEI

MARIAN-CĂTĂLIN PREDOIU