PARLAMENTUL ROMÂNIEI

SENATUL

CAMERA DEPUTAŢILOR

LEGE
privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative

Parlamentul României adoptă prezenta lege.

CAPITOLUL I
Dispoziţii generale

Art. 1.

(1) Prezenta lege stabileşte cadrul juridic şi instituţional privind organizarea şi desfăşurarea activităţilor din domeniile securitate şi apărare cibernetică, mecanismele de cooperare şi responsabilităţile instituţiilor cu atribuţii în domeniile menţionate.

(2) Securitatea şi apărarea cibernetică se realizează prin adoptarea şi implementarea de politici şi măsuri în scopul cunoaşterii, prevenirii şi contracarării vulnerabilităţilor, riscurilor şi ameninţărilor în spaţiul cibernetic.

Art. 2.

În sensul prezentei legi, termenii şi expresiile de mai jos au următoarea semnificaţie:

a) apărare cibernetică - totalitatea activităţilor, mijloacelor şi măsurilor utilizate pentru a contracara ameninţările provenite din spaţiul cibernetic şi a atenua efectele acestora asupra sistemelor de comunicaţii şi tehnologia informaţiei, sistemelor de armament, reţelelor şi sistemelor informatice, care susţin capabilităţile militare de apărare;

b) ameninţare cibernetică - astfel cum este definită în art. 2 lit. f) din Ordonanţa de Urgenţă a Guvernului nr. 104/2021;

c) atac cibernetic - acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică;

d) audit de securitate cibernetică - activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor şi măsurilor de protecţie implementate la nivelul unei reţele şi sisteme informatice, în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora;

e) Advanced Persistent Threat (APT) - astfel cum este definită în art. 2 lit. a) din Ordonanța de Urgență a Guvernului nr. 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice;

f) centru operațional de securitate - echipă de experți în securitate cibernetică, ce are rolul de a monitoriza, analiza și răspunde la incidentele de securitate cibernetică;

g) criza cibernetică - astfel cum este definită în art. 2 lit. k) din Ordonanța de Urgență a Guvernului nr. 104/2021;

h) cyber intelligence – activități de culegere, procesare, prelucrare analitică și valorificare a datelor și informațiilor privind acțiuni de natură a afecta interesele și obiectivele naționale de securitate pe linia tehnologiei informației și comunicațiilor, precum și identificarea, cunoașterea, prevenirea și contracararea oricăror acțiuni din spațiul cibernetic care pot constitui riscuri, vulnerabilități și/sau amenințări la adresa securității și apărării naționale a României;

i) cyber counter-intelligence – totalitatea activităților, mijloacelor și măsurilor ofensive și defensive de identificare, descurajare, neutralizare și protecție împotriva activităților de informații privind acțiuni ostile de natură a afecta interesele și obiectivele naționale de securitate, desfășurate în spațiul cibernetic și în domeniul apărării;

j) diplomație cibernetică – activitatea diplomatică prin intermediul căreia se realizează promovarea intereselor de politică externă și de securitate ale României în cadrul formatelor bilaterale și multilaterale de dialog și negociere pe teme cu relevanță pentru domeniul securității cibernetice la nivel național și internațional. Activitatea include promovarea unor obiective care derivă atât din necesitatea asigurării și consolidării securității cibernetice naționale, cât și din prioritățile de politică externă ale României.

k) echipă de răspuns la incidente de securitate cibernetică - astfel cum este definit în art. 2 lit a) din OUG nr. 104/2021;

l) furnizor de servicii tehnice de securitate cibernetică - persoană fizică și/sau juridică care realizează, în vederea protejării rețelelor și sistemelor informatice, cel puțin una dintre următoarele activități: implementarea de măsuri de securitate cibernetică, evaluarea, monitorizarea și testarea măsurilor implementate, precum și managementul riscurilor, amenințărilor, vulnerabilităților și incidentelor de securitate cibernetică;

m) igienă cibernetică sau igienă în spațiul cibernetic - măsuri de rutină aplicate cu regularitate de către persoanele fizice și juridice care au rolul de a reduce expunerea acestora la riscurile pe care le presupun amenințările cibernetice, conform Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) (Text cu relevanță pentru SEE);

n) incident de securitate cibernetică - eveniment survenit în spațiul cibernetic care perturbă funcționarea uneia sau mai multor rețele și sisteme informatice și ale cărui consecințe sunt de natură a afecta securitatea cibernetică;

o) lanțul de aprovizionare - circuitul de la producător până la beneficiarul final, inclusiv proiectarea, dezvoltarea, producția, integrarea, implementarea, configurarea, utilizarea și casarea de produse și servicii software sau hardware, respectiv rețele și sisteme informatice;

p) managementul incidentelor de securitate cibernetică - ansamblul proceselor ce prevăd detectarea, calificarea, raportarea, analiza și răspunsul la incidentele de securitate cibernetică;

q) managementul riscurilor de securitate cibernetică - strategia organizațională și programatică ce presupune activități de evaluare și gestionare a riscurilor de securitate cibernetică;

r) managementul riscurilor de securitate cibernetică specifice lanțului de aprovizionare - strategia organizațională și programatică ce presupune activități de evaluare și gestionare a riscurilor în cadrul proceselor din întreg ciclul de viață al bunului sau serviciului software sau hardware, respectiv al sistemului sau rețelei informatice, de la producător până la beneficiarul final, inclusiv proiectarea, dezvoltarea, producția, integrarea, implementarea, configurarea, utilizarea și casarea de produse și servicii software sau hardware, respectiv rețele și sisteme informatice;

s) politici de securitate cibernetică - principii și reguli generale, necesar a fi aplicate pentru asigurarea securității rețelelor și sistemelor informatice;

t) produs de securitate cibernetică - astfel cum este definit în art. 2 lit l) din OUG nr. 104/2021;

u) rețele și sisteme informatice - astfel cum sunt definite de art. 3 lit. l) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice;

v) rețele și sisteme informatice specifice apărării naționale - rețelele și sistemele informatice aparținând Ministerului Apărării Naționale, rețelele și sistemele informatice naționale care susțin activitățile militare ale NATO și UE, precum și rețelele și sistemele informatice de interes pentru apărarea națională date în responsabilitatea sau puse la dispoziția Ministerului Apărării Naționale în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare, sau a stării de război;

w) reziliența în spațiul cibernetic – capacitatea unei rețele sau sistem informatic de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate de dinaintea incidentului sau atacului cibernetic;

x) risc de securitate cibernetică - probabilitatea ca o amenințare să se materializeze, exploatând o vulnerabilitate specifică rețelelor și sistemelor informatice;

y) securitate cibernetică - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice sau private din spațiul cibernetic;

z) spațiu cibernetic - mediul virtual generat de rețelele și sistemele informatice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta;

aa) vulnerabilitate de securitate cibernetică - slăbiciune în proiectarea, implementarea, dezvoltarea, configurarea și mentenanța rețelelor și sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare.

Art. 3.

(1) În domeniul securității cibernetice prezenta 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).
(2) În domeniul apărării cibernetice, prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru rețelele și sistemele informatice specifice apărării naționale.

Art. 4.
Obiectivele prezentei legi sunt:

a) asigurarea rezilienței și protecției rețelelor și sistemelor informatice ce susțin funcțiile de apărare, securitate națională, ordine publică și guvernare;

b) desemnarea autorităților competente și stabilirea cadrului legal de dezvoltare a capabilităților necesare îndeplinirii responsabilităților acestora în domeniile securității și apărării cibernetice;

c) menținerea sau restabilirea climatului de securitate cibernetică la nivel național, prin cooperarea între autoritățile competente și asigurarea coordonării unitare de către Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC, a persoanelor juridice responsabile de securitatea cibernetică proprie, și asigurarea unei reacții rapide și eficiente la amenințările provenite din spațiul cibernetic;

d) stabilirea și separarea responsabilităților și/sau atribuțiilor funcționale între furnizorii de rețele, sisteme și servicii informatice, autoritățile de aplicare a legii, structurile din cadrul instituțiilor cu atribuții în domeniul securității și apărării cibernetice, astfel încât să se asigure un nivel ridicat de securitate cibernetică la nivel național;

e) dezvoltarea și consolidarea unei culturi de securitate cibernetică la nivel național, prin conștientizarea vulnerabilităților, riscurilor și amenințărilor, respectiv formarea unei conduite proactive și preventive.

Art. 5.
Asigurarea securității și apărării cibernetice se realizează conform următoarelor principii:

a) principiul personalității – responsabilitatea asigurării securității cibernetice și/sau apărării cibernetice a unui sistem, rețea și/sau sistem informatic revine persoanei fizice sau juridice care le deține în proprietate, le organizează, administrează și/sau utilizează, după caz;

b) principiul protecției depline – persoana fizică sau juridică responsabilă de securitatea și/sau apărarea cibernetică a unui sistem, rețea și/sau serviciu informatic răspunde de managementul riscurilor asociate acestora și conexiunilor acestora cu alte sisteme, rețele și/sau servicii informatice terțe, precum și de implementarea măsurilor tehnice și organizaționale necesare protecției cibernetice;

c) principiul minimizării efectelor – în cazul unui incident de securitate cibernetică, persoana fizică sau juridică responsabilă de securitatea și/sau apărarea cibernetică a sistemului, rețelei și/sau serviciului informatic în cauză ia măsuri de evitare a amplificării efectelor și de extindere a acestora la alte sisteme, rețele și/sau servicii informatice din responsabilitatea proprie sau din responsabilitatea altor persoane fizice sau juridice;

d) principiul colaborării, cooperării și coordonării – constă în realizarea, în mod conjugat de către persoanele fizice sau juridice responsabile, a tuturor activităților care să asigure securitatea și/sau apărarea sistemelor, rețelelor și serviciilor informatice care fac obiectul prezentei legi, precum și gestionarea incidentelor de securitate cibernetică, atenuarea efectelor și eliminarea situațiilor care au generat stările de alertă cibernetică instituite la nivel național.

CAPITOLUL II
Sistemul național de securitate cibernetică

Art. 6.

(1) La nivel național, activitățile specifice securității cibernetice se organizează și se desfășoară în mod unitar, potrivit prezentei legi.

(2) În acest scop, se înființează Sistemul Național de Securitate Cibernetică, denumit în continuare SNSC, drept cadru general de cooperare care reunește autoritățile prevăzute la art. 10, precum și alte autorități și instituții publice cu responsabilități și capabilități în domeniu, în vederea coordonării acțiunilor la nivel național pentru asigurarea securității cibernetice.

(3) În exercitarea competențelor, instituțiile și autoritățile publice prevăzute la alin (2) cooperează cu sectorul privat, mediul academic, asociațiile profesionale și cu organizațiile neguvernamentale.

Art. 7.

(1) Activitățile SNSC sunt coordonate, la nivel strategic, de către Consiliul Suprem de Apărare a Țării, denumit în continuare CSAT.

(2) Activitățile SNSC sunt coordonate unitar, la nivel operațional, de către COSC.

(3) Serviciul Român de Informații, denumit în continuare SRI, asigură secretariatul tehnic al COSC, în condițiile prezentei legi.

Art. 8.

(1) COSC este un organ consultativ, fără personalitate juridică, în coordonarea CSAT, format din consilierul prezidențial pentru probleme de securitate națională, consilierul prim-ministrului pe probleme de securitate națională, Secretarul CSAT, precum și reprezentanți ai: Ministerului Apărării Naționale, denumit în continuare MApN, Ministerului Afacerilor Interne, denumit în continuare MAI, Ministerului Afacerilor Externe, denumit în continuare MAE, Ministerului Cercetării, Inovării și Digitalizării, denumit în continuare MCID, SRI, Serviciului de Informații Externe, denumit în continuare SIE, Serviciului de Telecomunicații Speciale, denumit în continuare STS, Serviciului de Protecție și Pază, denumit în continuare SPP, Oficiului Registrului Național al Informațiilor Secrete de Stat, denumit în continuare ORNISS, Autorității Naționale pentru Administrare și Reglementare în Comunicații, denumit în continuare ANCOM, și ai Directoratului Național de Securitate Cibernetică, denumit în continuare DNSC.

(2) COSC emite avize consultative și recomandări, adoptate prin consens, care se adresează autorităților prevăzute la alin. (1), conform competențelor legale.

(3) Conducerea COSC este asigurată de un președinte - consilierul prezidențial pentru probleme de securitate națională și un vicepreședinte - consilierul prim-ministrului pe probleme de securitate națională.

(4) În funcție de natura și evoluția amenințărilor cibernetice sunt invitați să participe în cadrul ședințelor COSC, fără a avea drept de vot, și reprezentanți ai altor entități – autorități, instituții publice, persoane juridice de drept public sau privat – care pot contribui la soluționarea problemelor de securitate cibernetică.

(5) Convocarea COSC se face de către Președintele acestuia, la propunerea oricăruia dintre membrii prevăzuți la alin. (1).

Art. 9.

(1) În exercitarea atribuțiilor sale, COSC analizează și evaluează securitatea cibernetică și înaintează CSAT sau DNSC, după caz, propuneri și informări privind:

a) armonizarea reacției autorităților competente ale statului în situații generate de amenințări cibernetice, care necesită schimbarea nivelului de alertă cibernetică;

b) solicitarea, în caz de necesitate, de asistență din partea altor state sau organizații și organisme internaționale;

c) modalitatea de răspuns la solicitările de asistență adresate României din partea altor state sau organizații și organisme internaționale, altele decât cele din domeniul apărării naționale;

d) planuri sau direcții de acțiune, în funcție de concluziile rezultate și evoluția climatului de securitate în spațiul cibernetic;

e) direcții de dezvoltare și investiții în domeniul securității cibernetice;

f) linii de mandat privind adoptarea oricăror documente la nivel internațional cu privire la securitatea cibernetică care au impact în plan național;

g) modalități de gestionare și răspuns la amenințări și atacuri cibernetice.

(2) În exercitarea atribuțiilor sale, COSC informează CSAT cu privire la recomandările și avizele referitoare la instituirea sau modificarea nivelurilor de alertă cibernetică la nivel național.

(3) Pentru realizarea securității cibernetice, COSC cooperează, după caz, cu organismele de coordonare sau de conducere constituite, la nivel național, pentru managementul situațiilor de urgență, acțiuni în situații de criză în domeniul ordinii publice, prevenirea și combaterea terorismului, securitate și apărare națională.

CAPITOLUL III
Autorități competente și responsabilități

Art. 10.

(1) Sunt autorități competente în sensul prezentei legi:

a) DNSC, pentru spațiul cibernetic național civil, conform prevederilor prezentei legi și ale Ordonanței de urgență nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată, cu modificări și completări, prin Legea nr. 11/2022;

b) MCID, pentru elaborarea și inițierea actelor normative și politicilor publice naționale în domeniul securității cibernetice, a transformării digitale, societății informaționale, comunicațiilor, cercetării, dezvoltării și inovării.

c) ANCOM, pentru coordonarea activităților desfășurate în vederea asigurării securității cibernetice a rețelelor și sistemelor informatice proprii și a celor prevăzute la art. 3 alin (1) lit. b);

d) MApN, MAI, MAE, ORNISS, SRI, SIE, STS și SPP, conform atribuțiilor de la art. 11-18.

(2) Autoritățile prevăzute la alin. (1) au următoarele obligații:

a) să adopte planuri de acțiune corespunzătoare fiecărui nivel de alertă cibernetică;

b) să acorde sprijin, în limita atribuțiilor, la solicitarea proprietarilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate, pentru implementarea măsurilor corespunzătoare nivelurilor de alertă cibernetică;

c) să desfășoare activități de informare și comunicare publică, în limita atribuțiilor;

d) să organizeze sesiuni de formare și instruire în domeniul securității cibernetice, în limita atribuțiilor;

e) să organizeze sau să participe la exerciții naționale de securitate cibernetică;

f) să comunice reciproc date de interes referitoare la securitatea cibernetică, inclusiv către celelalte autorități și instituții publice, care dețin, organizează, administrează, utilizează sau au în competență rețele și sisteme informatice.

(3) Autoritățile prevăzute la art. 10 pot elabora strategii și norme proprii, prin acte administrative ale conducătorilor autorităților, pentru reglementarea activităților de securitate cibernetică, la nivel instituțional.

Art. 11.

MApN este autoritate competentă la nivel național în domeniul apărării cibernetice, iar în sensul prezentei legi are atribuții în domeniul securității cibernetice pentru rețelele și sistemele informatice care susțin capabilitățile militare de apărare.

Art. 12.

MAI, prin structura specializată, este autoritatea competentă la nivel național în domeniul securității cibernetice pentru cunoașterea, prevenirea, identificarea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa sistemelor informatice, rețelelor de comunicații și serviciilor electronice din domeniul de competență.

Art. 13.

(1) MAE este autoritate competentă, la nivel național, în domeniul diplomației cibernetice, pentru asigurarea componentei diplomatice și de relații internaționale aferente securității cibernetice, și îndeplinește următoarele atribuții:

a) asigură și coordonează reprezentarea intereselor României în cadrul formatelor internaționale de negociere și dialog politic la care România este parte și al căror obiect de activitate poate produce implicații în plan național și internațional din perspectiva regulilor, principiilor și normelor de utilizare a tehnologiilor de informații și telecomunicații și a parametrilor conduitei responsabile a statelor în spațiul cibernetic.

b) sprijină și promovează coordonarea, la nivel strategic, a dialogului României în domeniul securității și apărării cibernetice cu principalii parteneri internaționali și în cadrul formatelor internaționale la care România este parte, precum și cu privire la deciziile de politică cu implicații naționale și internaționale privind spațiul cibernetic;

c) promovează și contribuie la înțelegerea, însușirea și aplicarea la nivel național și internațional a principiilor, regulilor și normelor de comportament responsabil în spațiul cibernetic agreate la nivelul ONU, aplicarea dreptului internațional în materie și utilizarea setului de instrumente de diplomație cibernetică de la nivel UE;

d) promovează interesele României în plan internațional într-o manieră conformă cadrului național de valori democratice și apartenenței României la Alianța Nord-Atlantică (NATO) și Uniunea Europeană (UE), prin susținerea și protejarea caracterului global, deschis, liber, stabil și sigur al spațiului cibernetic, a aplicabilității depline a dreptului internațional – inclusiv a dreptului internațional umanitar și a legislației internaționale privind drepturile omului – în acest spațiu, precum și a respectării depline a normelor de conduită responsabilă a statelor în spațiul cibernetic agreate în sistemul ONU, în vederea menținerii stabilității, prevenirii conflictelor și atenuării amenințărilor cibernetice.

(2) MAE colaborează cu autoritățile membre COSC, în principal, în vederea:

a) asigurării componentei diplomatice a securității cibernetice;

b) promovării unitare a intereselor României și a unui mesaj coerent în acțiunea externă a României;

c) participării în ecosistemul securității cibernetice la nivel internațional;

d) asigurării răspunsului unitar și prompt în abordarea de politică externă a evoluțiilor și situațiilor nou apărute din domeniul securității cibernetice care pot produce consecințe pentru securitatea și apărarea cibernetică.

Art. 14.

(1) SRI este autoritate competentă la nivel național în domeniul cyber intelligence, precum și pentru cunoașterea, analizarea, prevenirea și contracararea incidentelor și atacurilor cibernetice care reprezintă amenințări, riscuri și vulnerabilități la adresa securității naționale a României.

(2) Prevenirea și combaterea amenințărilor de tip APT la adresa rețelelor și sistemelor informatice din domeniul de competență, activitate sau responsabilitate, după caz, ale instituțiilor și autorităților prevăzute la art.10, se realizează, astfel:

a) de către MApN potrivit competențelor prevăzute la art.11;
b) de către MAI potrivit competențelor prevăzute la art.12;
c) de către SIE potrivit competențelor prevăzute la art.15;
d) de către STS potrivit competențelor prevăzute la art.16;
e) de către SPP potrivit competențelor prevăzute la art.17;
f) de către SRI, în toate celelalte cazuri.

(3) În situația existenței unor amenințări cibernetice la adresa rețelelor și sistemelor informatice prevăzute la art. 3 alin. (1) lit. b) și lit. c), care ar aduce atingere securității naționale, SRI informează ANCOM și DNSC, în condițiile legii.

Art. 15.

SIE este autoritate competentă pentru cunoașterea, analizarea, prevenirea și contracararea incidentelor și atacurilor cibernetice care reprezintă amenințări, riscuri și vulnerabilități la adresa rețelelor și sistemelor informatice din responsabilitate.

Art. 16.

STS este autoritate competentă în domeniul securității cibernetice pentru infrastructurile, rețelele, sistemele, serviciile proprii și spectrul de frecvențe radio proprii, precum și pentru cele reglementate prin legi speciale.

Art. 17.

SPP este autoritate competentă în domeniul securității cibernetice pentru infrastructurile, rețelele, sistemele și serviciile proprii, coordonează măsurile de securitate cibernetică pentru demnitarii cărora, conform legii, le asigură protecție și acționează, independent sau în cooperare cu celelalte structuri din domeniile apărării, ordinii publice și securității naționale, pentru implementarea acestora.

Art. 18.

ORNISS coordonează activitățile desfășurate în vederea asigurării securității cibernetice a rețelelor și sistemelor informatice care stochează, procesează sau transmit informații clasificate, conform atribuțiilor prevăzute în Ordonanța de Urgență nr. 153/2002 privind organizarea și

funcționarea Oficiului Registrului Național al Informațiilor Secrete de Stat, cu modificările și completările ulterioare.

Art. 19.

(1) Autoritățile prevăzute la art. 10 constituie și operaționalizează structuri specializate în realizarea de audit de securitate cibernetică și structuri specializate de securitate cibernetică pentru gestionarea amenințărilor cibernetice la adresa rețelelor și sistemelor informatice din responsabilitate.

(2) Structurile prevăzute la alin. (1) se înființează, se organizează și funcționează prin act administrativ al conducătorului autorităților prevăzute la art. 10.

CAPITOLUL IV
Managementul incidentelor și reziliența în spațiul cibernetic

SECȚIUNEA 1
Managementul incidentelor de securitate cibernetică

Art. 20.

(1) DNSC dezvoltă și asigură managementul Platformei naționale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC.

(2) Autoritățile prevăzute la art. 10 au acces la PNRISC, pentru îndeplinirea responsabilităților care le revin, conform legii.

(3) Procesarea informațiilor din PNRISC se realizează cu respectarea politicilor de confidențialitate și transparență stabilite și implementate de DNSC.

Art. 21.

(1) Persoanele prevăzute la art. 3 alin. (1) lit. b) și lit. c), au obligația de a notifica incidentele de securitate cibernetică prin intermediul PNRISC, de îndată dar nu mai târziu de 48 de ore de la constatarea incidentului.

(2) Dacă incidentele de securitate cibernetică nu pot fi comunicate complet în termenul prevăzut la alin. (1), acestea se transmit în cel mult 5 zile calendaristice de la notificarea inițială, informațiile putând fi completate și ulterior cu cele care reies din investigațiile realizate pe baza evenimentului.

(3) Autoritățile care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3 alin. (1) lit. a), fără a aduce atingere normelor aplicabile în materie de raportare, confidențialitate, secret profesional și protecția informațiilor clasificate, notifică incidentele de securitate cibernetică prin intermediul PNRISC.

Art. 22.

Incidentele de securitate cibernetică sunt notificate în PNRISC în condițiile secțiunii a 2-a din Capitolul IV al Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

Art. 23.

În domeniul managementului incidentelor de securitate cibernetică, autoritățile prevăzute la art. 10 lit. c) și d) au următoarele responsabilități:

a) să colecteze notificările cu privire la incidente de securitate cibernetică din cadrul rețelelor și sistemelor informatice aflate în domeniul lor de competență, activitate sau responsabilitate;

b) să evalueze datele și informațiile cu privire la incidentele și atacurile cibernetice la adresa rețelelor și sistemelor informatice aflate în domeniul lor de competență, activitate sau responsabilitate;

c) să coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul rețelelor și sistemelor informatice aflate în domeniul lor de competență, activitate sau responsabilitate;

d) să acorde sprijin, la cerere, proprietarilor, administratorilor, posesorilor și/sau utilizatorilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgență pentru remedierea efectelor incidentelor de securitate cibernetică;

e) să păstreze pe un termen de 5 ani datele referitoare la incidentele de securitate cibernetică și rezultatele măsurilor de contracarare a acestora, fără a colecta date conținut.

SECȚIUNEA 2

Reziliența în spațiul cibernetic

Art. 24.

(1) Asigurarea rezilienței în spațiul cibernetic se realizează prin implementarea de măsuri proactive și reactive de către persoanele prevăzute la art. 3.

(2) Măsurile proactive sunt destinate prevenirii incidentelor de securitate cibernetică și descurajării atacatorilor din spațiul cibernetic și includ:

a) constituirea și antrenarea echipelor de răspuns la incidente de securitate cibernetică;

b) asigurarea de resurse umane specializate pentru dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri și măsuri de control tehnic privind apărarea și securitatea cibernetică;

c) constituirea și operarea Centrelor Operaționale de Securitate;

d) constituirea unei rezerve de resurse și de capabilități întrunite de securitate cibernetică care să poată fi utilizate în caz de necesitate;

e) dezvoltarea unor capabilități proactive, care să permită cunoașterea anticipativă a amenințărilor din spațiul cibernetic;

f) finanțarea pentru dezvoltarea capabilităților de securitate și apărare cibernetică, inclusiv din perspectiva cercetării, dezvoltării, inovării și digitalizării în domeniu și asimilării tehnologiilor emergente;

g) cooperarea și schimbul de informații între autoritățile competente și sectorul privat pentru identificarea amenințărilor cibernetice;

h) identificarea serviciilor, rețelelor și sistemelor informatice, conform competențelor fiecărei instituții responsabile de administrare și asigurarea managementului acestora;

i) implementarea de soluții de securitate cibernetică, care să crească capacitatea de detecție și capabilitățile de prevenție la atacuri cibernetice;

j) dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri și măsuri de control tehnic privind apărarea și securitatea cibernetică;

k) demonstrarea nivelului de maturitate atins de capabilitățile de securitate cibernetică în cadrul exercițiilor organizate la nivel național sau internațional;

l) instruirea personalului din cadrul persoanelor prevăzute la art. 3 în domeniul securității cibernetice, prin realizarea periodică de campanii de informare, conștientizare și igienă cibernetică la nivel organizațional.

(3) Măsurile reactive sunt destinate reducerii efectelor atacurilor cibernetice și includ:

a) punerea în aplicare a planurilor de răspuns la incidente și de contingență în domeniul securității cibernetice;

b) utilizarea rezervei de resurse și de capabilități de securitate cibernetică;

c) restabilirea funcționalității rețelelor și sistemelor informatice din cadrul instituțiilor afectate;

d) diseminarea informațiilor despre evenimentele cibernetice prin alerte în mediul interinstituțional pentru evaluarea riscului și diminuarea posibilităților de exploatare a vulnerabilităților;

e) descurajarea prin atribuirea publică a autorilor atacurilor cibernetice, conform atribuțiilor legale.

Art. 25.

(1) Furnizorii de servicii tehnice de securitate cibernetică au obligația de a pune la dispoziția autorităților prevăzute la art. 10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art. 3 alin. 1, precum și interconectarea acestora cu terții și cu utilizatorii finali.

(2) Datele și informațiile prevăzute la alin. (1) nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut.

(3) Datele și informațiile prevăzute la alin. (1) se transmit în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord, în formatul și structura conforme raportării de incidente cibernetice în PNRISC, menționate la art. 22.

Art. 26.

Pentru creșterea nivelului de reziliență cibernetică și realizarea descurajării în spațiul cibernetic la nivel național, DNSC și instituțiile din domeniile apărării, ordinii publice și securității naționale iau măsuri pentru:

a) realizarea unui cadru interinstituțional de securitate cibernetică care să permită instruirea comună, transferul de cunoștințe, schimbul de informații, sprijinul de specialitate și federalizarea de resurse și capabilități de securitate cibernetică;

b) îmbunătățirea și extinderea capabilităților de protecție și detecție automată a atacurilor, prin implementarea de instrumente de analiză inteligentă a amenințărilor și distribuirea oportună a indicatorilor și avertizărilor privind iminența unor atacuri cibernetice asupra rețelelor și sistemelor informatice naționale;

c) elaborarea de manuale cu tehnici, tactici și proceduri, precum și a planurilor de contingență și exersarea lor în cadrul exercițiilor de securitate cibernetică în scopul întăririi rezilienței în spațiul cibernetic;

d) constituirea de echipe de intervenție la incidente de securitate cibernetică de tip CSIRT, echipe de protecție cibernetică și/sau alte forțe specializate în desfășurarea de acțiuni în spațiul cibernetic.

CAPITOLUL V
Sistemul național de alertă cibernetică

Art. 27.

(1) Sistemul Național de Alertă Cibernetică, denumit în continuare SNAC, constă într-un ansamblu de măsuri tehnice și procedurale destinate prevenirii, descurajării și combaterii acțiunilor sau inacțiunilor ce se pot constitui în vulnerabilități, riscuri sau amenințări la adresa securității cibernetice a României.

(2) SNAC asigură un serviciu de notificare publică privind nivelul de alertă cibernetică existent la nivel național, pentru o zonă geografică delimitată sau pentru un anumit domeniu de activitate, stabilit în funcție de gradul de risc asociat amenințărilor, incidentelor sau atacurilor cibernetice identificate la un anumit moment.

Art. 28.

(1) Nivelurile de alertă cibernetică și modalitățile de acțiune în situații de alertă cibernetică se stabilesc printr-o metodologie elaborată de DNSC, avizată conform de COSC și aprobată prin ordin al directorului DNSC.

(2) Instituirea nivelurilor de alertă, precum și trecerea de la un nivel la altul se decid de către directorul DNSC, cu avizul consultativ și prealabil sau la propunerea COSC, după caz.

(3) Trecerea de la un nivel de alertă cibernetică superior la unul inferior se face după încetarea cauzelor care au generat ridicarea nivelului de alertă.

Art. 29.

(1) Persoanele prevăzute la art. 3 au obligația să elaboreze planuri proprii de acțiune pentru fiecare tip de alertă cibernetică, conform metodologiei emise de DNSC.

(2) La declararea stărilor de alertă cibernetică, persoanele prevăzute la art. 3 pun în aplicare măsurile din planurile prevăzute la alin. (1).

CAPITOLUL VI
Apărarea cibernetică

Art. 30.

(1) În domeniul apărării cibernetice, MApN are următoarele atribuții:

a) apără și protejează sistemele și rețelele informatice aparținând MApN ;

b) planifică și conduce operații în spațiul cibernetic prin Centrul Național Militar de Comandă, potrivit legii;

c) planifică și execută operații defensive în spațiul cibernetic, pe timp de pace, prin Comandamentul Apărării Cibernetice;

d) dezvoltă și implementează capabilități militare de execuție a operațiilor în spațiul cibernetic prin Comandamentul Apărării Cibernetice;

e) desfășoară operații de cyber intelligence și cyber counter-intelligence în spațiul cibernetic în scopul cunoașterii, monitorizării și contracarării amenințărilor la adresa apărării naționale, la adresa structurilor MApN și a forțelor aliate;

f) dezvoltă capabilități de răspuns ofensiv, în mod individual sau ca parte dintr-o coaliție ori alianță, utilizabile în caz de atacuri cibernetice care contravin dreptului internațional;

g) participă la activități de descurajare în spațiul cibernetic;

h) asigură punctul unic de contact în relația cu NATO pentru operațiuni militare în spațiul cibernetic;

i) elaborează și implementează politici și standarde în domeniul apărării cibernetice, în acord cu interesul național, precum și cu standardele și cerințele ce decurg din aderarea României la Organizația Tratatului Atlanticului de Nord, Uniunea Europeană și Organizația pentru Cooperare și Dezvoltare Economică.

(2) MApN cooperează cu celelalte structuri din cadrul sistemului național de apărare, ordine publică și securitate națională pentru asigurarea apărării cibernetice a rețelelor și sistemelor informatice din domeniul lor de competență, activitate sau responsabilitate.

(3) Activitățile de apărare cibernetică și operațiunile în spațiul cibernetic, dezvoltarea de capabilități de răspuns ofensiv și activitățile de descurajare în spațiul cibernetic menționate la alin. (1) se organizează, planifică și desfășoară cu respectarea dreptului internațional, inclusiv a dreptului internațional umanitar, a normelor de conduită responsabilă a statelor în spațiul cibernetic agreate în sistemul ONU, precum și a celorlalte tratate la care România este parte.

Art. 31.

MApN stabilește, prin hotărâre de Guvern, condițiile concrete de recrutare/selecție, modalitățile de formare și instruire periodică, măsurile de stimulare ale persoanelor juridice de drept privat, precum și condițiile necesare constituirii și utilizării rezervei de specialiști în domeniul apărării cibernetice.

CAPITOLUL VII
Cercetare, dezvoltare și inovare în domeniul securității cibernetice

Art. 32.

(1) Cercetarea, dezvoltarea și inovarea în domeniul securității cibernetice sunt parte integrantă a sistemului național de cercetare, dezvoltare și inovare și se aliniază măsurilor promovate de MCID pentru încadrarea spațiului românesc al cercetării în Spațiul European al Cercetării.

(2) MCID elaborează un program multianual de finanțare a proiectelor de cercetare, dezvoltare și inovare în domeniul securității cibernetice, la care pot participa organizații de cercetare publice și private, precum și autorități și instituții publice cu atribuții în domeniul securității cibernetice.

(3) Prin derogare de la prevederile art. 30 alin. (2) din Legea responsabilității fiscal-bugetare nr. 69/2010, republicată în Monitorul Oficial, Partea I nr. 472 din 04 iunie 2020, cu modificările și completările ulterioare, bugetul anual alocat programului prevăzut la alin. (2) este de minimum 10% din bugetul alocat programelor de cercetare finanțate de MCID pentru anul respectiv.

(4) Finanțarea pentru programul prevăzut la alin. (2) se realizează pe criterii transparente și competitive, potrivit unei metodologii de concurs adoptată prin ordin al ministrului cercetării, inovării și digitalizării, publicat în Monitorul Oficial, Partea I.

Art. 33.

(1) Autoritățile prevăzute la art. 10 dezvoltă strategii și politici proprii privind cercetarea, dezvoltarea și inovarea în domeniile securității și apărării cibernetice, în funcție de potențialul științific avut la dispoziție, de competențele sau de misiunile specifice.

(2) La nivelul fiecărei autorități prevăzute la art. 10 se desemnează de către conducătorul instituției entitatea responsabilă pentru managementul activităților de cercetare, dezvoltare și inovare în domeniile securității și apărării cibernetice.

(3) Autoritățile prevăzute la art. 10 cooperează cu mediul academic, industria de profil și Centrul european de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică, precum și cu Rețeaua de centre naționale de coordonare, pentru implementarea următoarelor linii de efort în domeniul cercetării, dezvoltării, inovării și digitalizării:

a) menținerea unei poziții avansate în rândul instituțiilor ce investesc și valorifică rezultatele activităților de cercetare, dezvoltare și inovare desfășurate în domeniul securității cibernetice;

b) dezvoltarea și menținerea de parteneriate eficiente în domeniul cercetării, dezvoltării, inovării și digitalizării;

c) promovarea de noi tehnologii, de prototipuri și demonstratoare tehnologice în domeniile securității și apărării cibernetice;

d) dezvoltarea rețelelor de experți în domeniu la nivel național și interinstituțional.

CAPITOLUL VIII
Cooperare în domeniul securității și apărării cibernetice

SECȚIUNEA 1
La nivel național

Art. 34.

(1) Cooperarea în domeniul securității și apărării cibernetice, la nivel național, are următoarele obiective:

a) realizarea unui răspuns dinamic și eficient la incidentele de securitate cibernetică;

b) valorificarea experienței și bunelor practici în domeniile securității și apărării cibernetice;

c) implementarea unui mediu deschis, transparent, colaborativ și de încredere între instituțiile cu responsabilități în domeniile securității și apărării cibernetice la nivel național;

d) acceptarea și promovarea standardelor de securitate cibernetică în parteneriat cu industria națională de profil;

e) dezvoltarea și implementarea de soluții de securitate cibernetică de către toate autoritățile și instituțiile publice;

f) dezvoltarea unei culturi de securitate cibernetică și implementarea bunelor practici de igienă cibernetică la nivel național;

g) asigurarea comunicării publice coordonate și unitare, atunci când situația o impune, în cadrul situațiilor de alertă cibernetică, atacuri cibernetice cu impact semnificativ sau a amenințărilor nou apărute din spațiul cibernetic;

h) conștientizarea situațională și comunicarea către public a măsurilor recomandate spre implementare, în vederea facilitării managementului situațiilor de criză cibernetică.

(2) Activitățile de cooperare la nivel național includ, după caz, cel puțin următoarele:

a) dezvoltare de capabilități de securitate și apărare cibernetică;
b) raportarea de incidente cibernetice și cooperarea în situații de alertă cibernetică;
c) programe de cercetare, dezvoltare, inovare și digitalizare;
d) cursuri de formare profesională sau de specializare;
e) exerciții de securitate cibernetică;
f) conferințe și alte manifestări științifice.

SECȚIUNEA 2
La nivel internațional

Art. 35.
Cooperarea internațională în domeniile securității și apărării cibernetice are următoarele obiective:

a) informarea reciprocă privind amenințările din spațiul cibernetic;
b) creșterea capacității de reacție la amenințările cibernetice și formarea coeziunii de acțiune a echipelor specializate, în cadrul exercițiilor multinaționale de securitate și apărare cibernetică;
c) verificarea și validarea nivelului de maturitate atins de capabilitățile de securitate și apărare cibernetică implementate la nivel național;
d) realizarea interoperabilității tehnice și procedurale a forțelor de apărare cibernetică;
e) dezvoltarea și exersarea mecanismelor de avertizare și schimb de informații privind amenințările de natură cibernetică, precum și a celor de descurajare;
f) dezvoltarea de proiecte comune de cercetare, dezvoltare și inovare în domeniile securității și apărării cibernetice;
g) evaluarea și implementarea de soluții revoluționare de securitate cibernetică, precum și adoptarea de concepte noi de proiectare și utilizare a tehnologiilor emergente în spațiul cibernetic;
h) creșterea contribuției naționale la activități de transfer de cunoștințe, de creștere a încrederii și de dezvoltare a capacității în domeniul securității și apărării cibernetice;
i) reprezentarea intereselor României în cadrul formatelor internaționale de negociere și dialog al căror obiect de activitate poate produce implicații în plan național și internațional din perspectiva regulilor, principiilor și normelor de utilizare a tehnologiilor de informații și telecomunicații și a parametrilor conduitei responsabile a statelor în spațiul cibernetic precum și în acțiunile comune cu partenerii strategici și de la nivelul NATO și UE în aplicarea instrumentelor diplomației cibernetice pentru descurajarea activităților cibernetice maligne la nivel internațional.

Art. 36.
(1) Autoritățile prevăzute la art. 10 cooperează cu autoritățile și instituțiile din statele membre, cu organismele, agențiile și instituțiile Uniunii Europene și ale NATO cu atribuții în domeniul securității și apărării cibernetice, inclusiv cu autorități și instituții din alte state partenere, conform domeniilor de competență.
(2) Cooperarea în domeniul apărării cibernetice cu instituțiile NATO, cu armatele țărilor membre UE și ale statelor aliate se realizează prin MApN.
(3) Pentru asigurarea coordonării și a dialogului interinstituțional în vederea asigurării unei reprezentări adecvate și a unui mesaj coerent în acțiunea externă a României, precum și pentru realizarea obiectivelor de prevăzute la art. 13 alin (1), activitățile prevăzute la alin (1) se realizează în cooperare cu MAE.

CAPITOLUL IX
Formarea profesională, educația, instruirea

Art. 37.
Persoanele prevăzute la art. 3 au obligația de a asigura, pentru personalul propriu, formarea profesională, educația și instruirea în domeniul securității și apărării cibernetice prin cursuri, exerciții, conferințe, seminarii, precum și alte tipuri de activități.

Art. 38.
(1) Autoritățile și instituțiile din domeniile apărării, ordinii publice și securității naționale pot organiza, la nivel instituțional sau interinstituțional, exerciții de securitate și apărare cibernetică.
(2) Autoritățile și instituțiile prevăzute la alin. (1) elaborează și adoptă un plan anual și multianual de exerciții de securitate și apărare cibernetică.

Art. 39.
(1) Autoritățile și instituțiile din domeniile apărării, ordinii publice și securității naționale participă la exerciții de securitate și apărare cibernetică organizate la nivel internațional, respectiv la la nivelul UE și NATO.
(2) Participarea la exercițiile de apărare cibernetică organizate în cadrul NATO se realizează sub coordonarea MApN.

Art. 40.
DNSC și autoritățile și instituțiile din domeniile apărării, ordinii publice și securității naționale au următoarele atribuții:

a) asigură informarea și pregătirea, la nivel național, a populației precum și a tuturor persoanelor fizice și juridice care acționează în spațiul cibernetic național, inclusiv a operatorilor economici din sectoarele stabilite în baza Legii nr. 362/2018 și din sectorul public cu privire la riscurile, amenințările și vulnerabilitățile de securitate cibernetică identificate;

b) promovează dezvoltarea unui comportament responsabil în spațiul cibernetic pentru persoanele fizice și juridice prin conștientizarea efectelor atacurilor cibernetice și a modalității de semnalare a acestora;

c) emit informări privind obligațiile care derivă din calitatea de proprietar, administrator, organizator, furnizor sau utilizator al rețelelor și sistemelor informatice, privind atitudinea în fața unor posibile atacuri cibernetice, privind conștientizarea cetățenilor și instituțiilor publice și private, despre necesitatea semnalării/notificării atacurilor cibernetice;

d) dezvoltă cadrul național de conștientizare a populației în cooperare cu mediul public, privat și academic, în scopul pregătirii populației privind modalitățile de comportament, reacție și apărare în mediul online;

e) desfășoară și participă la campanii/acțiuni de prevenire și conștientizare a cauzelor și consecințelor atacurilor cibernetice asupra rețelelor și sistemelor informatice civile, la nivel internațional, național și regional.

CAPITOLUL X
Securitatea lanțului de aprovizionare

Art. 41.

(1) Persoanele prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare, conform metodologiei menționate la art. 52 alin. (1).

(2) Riscurile lanțului de aprovizionare includ cel puțin următoarele:

a) livrarea de soluții informatice false sau contrafăcute;

b) producție neautorizată;

c) manipulare frauduloasă a produselor și serviciilor software și hardware, respectiv a sistemelor și rețelelor informatice;

d) inserarea de componente software și hardware false sau contrafăcute;

e) servicii software și hardware periculoase pentru funcționare;

f) spionaj cibernetic;

g) compromiteri neintenționate ale sistemelor și rețelelor informatice;

h) practici deficitare de fabricație și dezvoltare de produse software și hardware.

Art. 42.

Persoanele prevăzute la art. 3 desemnează responsabili de securitate cibernetică, conform metodologiei menționate la art. 52 alin. (1), pentru:

a) stabilirea politicilor, strategiilor și proceselor de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare;

b) includerea în conținutul politicilor, strategiilor și proceselor existente a cerințelor noi și emergente privind managementul riscurilor cibernetice specifice lanțului de aprovizionare;

c) stabilirea standardelor de management al riscurilor de securitate cibernetică obligatorii pentru autoritățile contractante în cadrul procedurilor de achiziții;

d) stabilirea măsurilor de stimulare a potențialilor furnizori în cadrul proceselor de achiziții, raportat la nivelul de implementare a practicilor de securitate cibernetică ale acestora;

e) stabilirea metodologiilor și aplicațiilor folosite în evaluarea riscurilor de securitate cibernetică, specifice lanțului de aprovizionare;

f) schimbul de informații cu celelalte instituții referitoare la amenințările, riscurile și vulnerabilitățile de natură cibernetică specifice lanțului de aprovizionare;

g) elaborarea metodologiei de evaluare a nivelului de maturitate și a capacității operatorilor de pe lanțurile de aprovizionare de a realiza managementul riscurilor de securitate cibernetică;

h) colectarea și actualizarea datelor referitoare la eficiența furnizorilor în eliminarea sau diminuarea riscurilor de securitate cibernetică.

Art. 43.

Persoanele prevăzute la art. 3 dispun măsurile necesare pentru organizarea de cursuri de instruire în domeniul managementului riscurilor de securitate cibernetică specifice lanțului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor și programelor de instruire existente.

Art. 44.

Persoanele prevăzute la art. 3 pot dezvolta capabilități avansate de testare și evaluare a riscurilor de securitate cibernetică în scopul identificării vulnerabilităților cibernetice ale echipamentelor, produselor software sau pieselor componente achiziționate sau dezvoltate la nivel instituțional.

CAPITOLUL XI
Confidențialitatea și protecția securității datelor și informațiilor persoanelor fizice și juridice

Art. 45.

(1) Autoritățile prevăzute la art. 10 care solicită și primesc date și informații de la orice persoană fizică și juridică în temeiul prezentei legi iau măsuri adecvate pentru a proteja interesele de securitate și comerciale ale acestora, ale persoanelor care furnizează datele și informațiile respective, precum și ale persoanelor la care se referă datele și informațiile respective.
(2) Transmiterea de date și informații obținute potrivit prezentei legi de la orice persoană fizică și juridică de drept privat poate fi efectuată numai pentru îndeplinirea atribuțiilor legale ale autorităților și instituțiilor care obțin aceste date și informații, cu garantarea păstrării confidențialității datelor cu caracter personal și a protecției intereselor și secretelor comerciale ale persoanelor fizice și juridice de drept privat.

Art. 46.

(1) Prelucrările de date cu caracter personal ce intră sub incidența prezentei legi se efectuează cu respectarea reglementărilor legale privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal.
(2) Notificările realizate în temeiul prezentei legi nu afectează obligațiile operatorilor de date cu caracter personal stabilite potrivit art. 33 și 34 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.
(3) În scopul îndeplinirii atribuțiilor ori furnizării serviciilor prevăzute de prezenta lege, precum și în scopul prevenirii și răspunsului la incidentele de securitate cibernetică ori al cooperării la nivel național, comunitar și internațional în prevenirea și răspunsul la incidentele de securitate cibernetică, autoritățile prevăzute la art. 10 colectează, primesc, prelucrează și transmit date și informații ce pot constitui sau pot conține date cu caracter personal, în limitele legislației aplicabile, cu asigurarea respectării prevederilor alin. (2).

Art. 47.

(1) Prezenta lege nu afectează legislația națională privind protecția datelor cu caracter personal, în special Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), cu modificările și completările ulterioare, și Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare.
(2) Prezenta lege respectă drepturile fundamentale și principiile recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la respectarea vieții 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.

CAPITOLUL XII
Contravenţii şi sancţiuni

Art. 48.

(1) Următoarele fapte constituie contravenţii dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate infracţiuni potrivit legii:

a) nerespectarea de către persoanele prevăzute la art. 3 alin. (1) lit. b) şi lit. c) a obligaţiei de notificare a incidentelor de securitate cibernetică, prin intermediul PNRISC, în termenul prevăzut la art. 21 alin. (1);

b) nerespectarea de către persoanele prevăzute la art. 3 alin. (1) lit. b) şi lit. c) a obligaţiei de comunicare completă a incidentelor de securitate cibernetică, prin intermediul PNRISC, în termenul şi condiţiile prevăzute la art. 21 alin. (2) şi art. 22;

c) nerespectarea de către furnizorii de servicii de securitate cibernetică obligaţiei de a pune la dispoziţia autorităţilor prevăzute la art. 10 date şi informaţii privind incidente, ameninţări, riscuri sau vulnerabilităţi a căror manifestare poate afecta o reţea sau sistem informatic al deţinătorului sau al unor terţi, în condiţiile şi la termenul prevăzut la art. 25 alin. (1).

(2) Prin derogare de la dispoziţiile art. 8 alin. (2) lit. a) din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, contravenţiile prevăzute la alin. (1) se sancţionează astfel:

a) cu amendă de la 5.000 lei la 50.000 lei, iar în cazul săvârşirii unei noi contravenţii în termen de 6 luni, de la data săvârşirii primei contravenţii, limita maximă a amenzii este de 200.000 lei;

b) pentru operatorii economici cu o cifră de afaceri netă de peste 1.000.000 lei, cu amendă în cuantum de până la 5% din cifra de afaceri netă, iar, în cazul săvârşirii unei noi contravenţii, în termen de 6 luni, de la data săvârşirii primei contravenţii, limita maximă a amenzii este de 10% din cifra de afaceri netă.

(3) Cifra de afaceri netă prevăzută la alin. 2) lit. b) este cea înregistrată de operatorul economic în ultimul exerciţiu financiar.

(4) În vederea individualizării sancţiunii prevăzute la alin. (2), agentul de constatare şi aplicare a contravenţiei ia în considerare gradul de pericol social concret al faptei şi perioada de timp în care obligaţia legală a fost încălcată.

(5) Pentru persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, cifrei de afaceri prevăzute la alin. (2) lit. b) îi corespunde totalitatea veniturilor realizate de respectivii operatori economici în exerciţiul financiar anterior sancţionării.

(6) Pentru persoanele juridice nou-înfiinţate şi pentru persoanele juridice care nu au înregistrat cifra de afaceri în exerciţiul financiar anterior sancţionării, amenda prevăzută la alin. (2) se stabileşte în cuantum de minimum 1 şi maximum 25 de salarii minime brute pe economie.

(7) În măsura în care prezenta lege nu prevede altfel, contravenţiilor prevăzute la alin. (2) li se aplică dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor,

aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

Art. 49.

(1) Constatarea contravenţiilor prevăzute la art. 48 alin. (1), lit a) şi b) se realizează de către personalul de control din cadrul DNSC, iar aplicarea sancţiunii corespunzătoare se face prin decizia directorului DNSC.

(2) Constatarea contravenţiilor prevăzute la art. 48 alin. (1), lit. c) se realizează de către personalul de control anume desemnat din cadrul autorităţilor prevăzute de la art. 10, corespunzător autorităţii care a formulat cererea de punere la dispoziţie a informaţiilor şi datelor, iar aplicarea sancţiunii corespunzătoare se face prin act administrativ al personalului de control anume desemnat şi delegat de conducătorul autorităţii.

(3) Actul administrativ prevăzut la alin. (1) şi (2) trebuie să cuprindă următoarele elemente:

a) datele de identificare ale contravenientului;

b) data săvârşirii faptei;

c) descrierea faptei contravenţionale şi a împrejurărilor care au fost avute în vedere la individualizarea sancţiunii;

d) indicarea temeiului legal potrivit căruia se stabileşte şi se sancţionează contravenţia;

e) sancţiunea aplicată;

f) termenul şi modalitatea de plată a amenzii;

g) termenul de exercitare a căii de atac şi instanţa de judecată competentă.

(4) Prin derogare de la prevederile art. 13 din Ordonanţa Guvernului nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, aplicarea sancţiunii potrivit art. 48 alin. (2) se prescrie în termen de un an de la data săvârşirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârşirea, în baza aceleiaşi rezoluţii, la intervale diferite de timp, a mai multor acţiuni sau inacţiuni, care prezintă, fiecare în parte, conţinutul aceleiaşi contravenţii, prescripţia începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârşit, dacă acest moment intervine anterior constatării.

(5) Prin derogare de la dispoziţiile art. 14 alin. (1) din Ordonanţa Guvernului nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002 cu modificările şi completările ulterioare, actul administrativ prevăzut la alin. (3) se comunică contravenientului în termen de 15 zile de la data emiterii acestuia.

(6) Odată cu actul prevăzut la alin. (3), contravenientului i se comunică şi înştiinţarea de plată, care conţine menţiunea privind obligativitatea achitării amenzii în termen de 30 de zile de la data comunicării actului.

(7) Actul administrativ prevăzut la alin. (3) constituie titlu executoriu, fără vreo altă formalitate. Acţiunea în contencios administrativ în condiţiile alin. (9) suspendă executarea numai în ceea ce priveşte achitarea amenzii, până la pronunţarea de către instanţa de judecată a unei hotărâri definitive.

(8) Sumele provenite din amenzile aplicate în conformitate cu dispoziţiile prezentului articol se fac venit integral la bugetul de stat. Executarea se realizează în conformitate cu dispoziţiile legale privind executarea silită a creanţelor fiscale. În vederea punerii în executare a sancţiunii, DNSC şi autorităţile prevăzute la art. 10 comunică din oficiu organelor de specialitate ale Agenţiei Naţionale de Administrare Fiscală actul administrativ prevăzut la alin. (3), după expirarea termenului prevăzut în înştiinţarea de plată sau după rămânerea definitivă a hotărârii judecătoreşti prin care s-a soluţionat acţiunea în contencios administrativ.

(9) Prin derogare de la dispoziţiile art. 7 din Legea contenciosului administrativ nr. 554/2004, cu modificările şi completările ulterioare, şi de la dispoziţiile art. 32 alin. (1) din Ordonanţa Guvernului nr. 2/2001, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare, deciziile adoptate potrivit prezentului proiect de lege pot fi atacate în contencios administrativ la Curtea de Apel Bucureşti, fără parcurgerea procedurii prealabile, în termen de 30 de zile de la comunicarea acestora.

CAPITOLUL XIII

Dispoziţii privind modificarea şi completarea Legii nr. 51/1991 privind securitatea naţională a României, republicată , precum şi a Ordonanţei de urgenţă a Guvernului nr. 1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, cu modificările şi completările ulterioare

Art. 50.

La articolul 3 din Legea nr. 51/1991 privind securitatea naţională a României, republicată în Monitorul Oficial, Partea I, nr. 190 din 18 martie 2014, cu modificările şi completările ulterioare, după litera m), se introduc trei noi litere, literele n), o) şi p), care vor avea următorul cuprins:

"n) ameninţări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice şi de comunicaţii de interes naţional;

o) acţiuni, inacţiuni sau stări de fapt cu consecinţe la nivel naţional, regional sau global care afectează reziliența statului în raport cu riscurile și amenințările de tip hibrid;

p) acţiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spaţiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituţională.".

Art. 51.

Ordonanţa de urgenţă nr. 1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, publicată în Monitorul Oficial al României, Partea I, nr. 22 din 21 ianuarie 1999, cu modificările şi completările ulterioare, se modifică şi se completează astfel:

1. Articolul 2 se modifică şi va avea următorul cuprins:

"Art. 2. - Starea de asediu reprezintă ansamblul de măsuri excepţionale de natură politică, militară, economică, socială şi de altă natură aplicabile pe întreg teritoriul ţării ori în unele unităţi administrativ-teritoriale, instituite pentru adaptarea capacităţii de apărare a ţării, inclusiv apărarea cibernetică, la pericole grave, actuale sau iminente, care ameninţă suveranitatea, independenţa, unitatea ori integritatea teritorială a statului. În cazul instituirii stării de asediu se pot lua măsuri excepţionale aplicabile pe întreg teritoriul ţării ori în unele unităţi administrativ-teritoriale."

2. ***La articolul 3, litera a) se modifică și va avea următorul cuprins:***

"a) existența unor pericole grave actuale sau iminente privind securitatea națională a ***României, inclusiv securitatea cibernetică pentru rațiuni de securitate națională,*** *ori funcționarea democrației constituționale;"*

3. ***Articolul 23 se modifică și se completează și va avea următorul cuprins:***

"(1) Ordonanțele militare se emit în limitele stabilite prin decretul de instituire a măsurii excepționale, astfel:

1. pe durata stării de asediu:

a) de ministrul apărării naționale sau de șeful Statului Major General, când starea de asediu a fost instituită pe întregul teritoriu al țării;

b) de comandanții de mari unități în raza teritorială pentru care au fost împuterniciți de șeful Statului Major General, când starea de asediu a fost instituită în anumite unități administrativ-teritoriale;

2. pe durata stării de urgență:

a) de ministrul administrației și internelor sau de înlocuitorul de drept al acestuia, când starea de urgență a fost instituită pe întregul teritoriu al țării;

b) de ofițerii împuterniciți de ministrul administrației și internelor sau de înlocuitorii legali ai acestora, când starea de urgență a fost instituită în anumite unități administrativ-teritoriale;

(2) În situația instituirii stării excepționale pentru cauze ce privesc securitatea sau apărarea cibernetică în condițiile art. 2 și art. 3 lit. a), emitenții ordonanțelor militare solicită avizul prealabil și consultativ al Consiliului Operativ de Securitate Cibernetică.

CAPITOLUL XIV
Dispoziții tranzitorii și finale

Art. 52.

(1) Categoriile de persoane prevăzute la art. 3, alin. (1), lit. c) 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) se emit în maximum 90 de zile de la intrarea în vigoare a prezentei legi.

(3) În vederea aplicării prevederilor art. 20 alin. (3), 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, 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. 28 alin. (1), 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. 31, Guvernul adoptă o hotărâre în maximul 90 de zile de la intrarea în vigoare a prezentei legi.

(7) În vederea aplicării prevederilor art. 32 alin. (2)-(4), ministrul cercetării, inovării și digitalizării emite un ordin în maximum 120 de zile de la intrarea în vigoare a prezentei legi.

Art. 53.
Prevederile art. 48 şi 49 intră în vigoare în termen de 30 de zile de la data publicării prezentei legi în Monitorul Oficial al României, Partea I.

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

PREŞEDINTELE CAMEREI DEPUTAŢILOR PREŞEDINTELE SENATULUI

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 și 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 și 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 și 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 vulnerabilităților de securitate cibernetică și 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 Curții Constituționale asupra obiecției de neconstituționalitate a dispozițiilor 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 național, un cadru normativ care va permite crearea instrumentelor instituționale și a mecanismelor de acțiune integrată și cooperare interinstituțională în domeniile securitate și 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 și 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 creșterea nivelului de securitate cibernetică a rețelelor publice pe plan național și internațional și va preveni apariția unor situații în care

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

Adoptarea prezentei legi oferă posibilitatea instituțiilor publice să colaboreze cu entitățile din sectorul privat și din mediul academic, cu asociațiile profesionale și organizațiile neguvernamentale.

Totodată, această lege stabilește un cadru armonizat de acțiune a autorităților și instituțiilor publice cu responsabilități și capabilități specifice contracarării amenințărilor cibernetice.

Având în vedere contextul în care, la nivelul Alianței Nord-Atlantice, s-a luat decizia de declarare a spațiului cibernetic ca mediu operațional de ducere a operațiilor militare, prin prezentul proiect de act normativ sunt create mecanismele pentru ca Ministerului Apărării Naționale și celelalte autorități publice din domeniul apărării, ordinii publice și securității naționale să poată realiza acțiuni și să poată implementa politici și 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 Ordonanța de urgență 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 şi completările ulterioare. Proiectul de lege nu modifică conţinutul şi regimul juridic al stării de urgenţă şi de asediu reglementat de OUG nr. 1/1999, ci instituie doar cauzele de securitate cibernetică şi apărare cibernetică drept raţiuni/ motive de instituire a acestor stări excepţionale. Prin prezenta măsură se asigură o actualizare a cauzelor de instituire a stărilor excepţionale raportate la noile tipuri de ameninţări şi riscuri care afectează statele moderne.

Cu privire la introducerea definirii conceptului de cyber intelligence, în cadrul acestuia sunt înglobate *per se* activităţi, mijloace şi măsuri de securitate cibernetică care au ca scop asigurarea stării de normalitate a reţelelor şi sistemelor informatice. Componenta de securitate cibernetică aferentă activităţilor de cyber intelligence vizează asigurarea securităţii naţionale, prin aplicarea unui set de măsuri proactive şi reactive la nivelul reţelelor şi sistemelor informatice din plan naţional, menite să asigurea confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informaţiilor în format electronic a resurselor şi serviciilor publice.
Situaţia actuală, la nivel internaţional, demonstrează imposibilitatea separării ameninţării cibernetice de celelalte tipuri de ameninţări la adresa securităţii naţionale. Instrumentele specifice operaţiunilor cibernetice au fost adoptate de toate categoriile de vectori de ameninţare, de la extremism şi terorism la criminalitate organizată transfrontalieră şi spionaj. În prezent, actorii statali ostili derulează operaţiuni cibernetice complexe prin care vizează atingerea unor obiective strategice proprii la nivel internaţional, generând un impact semnificativ în planul intereselor de securitate naţională ale ţărilor afectate, prin exfiltrarea unor cantităţi foarte mari de date sensibile şi creându-şi inclusiv capacitatea de a afecta funcţionalitatea sistemelor respective.

La nivel conceptual, securitatea cibernetică nu poate fi separată de securitatea naţională, fiind o dimensiune cu relevanţă din ce în ce mai crescută a acesteia. Exemple în acest sens se regăsesc la nivel internaţional:
- în ianuarie 2022, administraţia Biden a declarat că Securitatea cibernetică este un imperativ de securitate naţională şi securitate economică, cu un nivel crescut, fără precedent de prioritate la nivelul SUA;
- în Strategia Naţională pentru Securitate Digitală a Franţei, se precizează că riscurile cibernetice reprezintă a treia prioritate pe lista ameninţărilor, conform White Paper privind Apărarea şi Securitatea Naţională;
- Strategia de securitate cibernetică a Marii Britanii pentru anul 2022 face referire extensivă la ameninţările cibernetice diverse şi complexe la adresa securităţii naţionale, precum şi la necesitatea implicării instituţiilor de securitate naţională cu măsuri pentru atingerea obiectivelor de securitate cibernetică

Practica a demonstrat faptul că activităţile de culegerea de informaţii reprezintă o condiţie sine qua non în combaterea ameninţărilor cibernetice complexe. Activitatea de culegere de informaţii s-a dovedit esenţială pentru obţinerea, prin mijloace specifice (HUMINT, OSINT, TECHINT, SIGINT, cooperare etc.) de date tehnice cu privire la tacticile, tehnicile şi procedurile atacatorilor, infrastructurile utilizate, ţintele predilecte ale operaţiunilor cibernetice şi chiar atacurile aflate în derulare. Aceste date s-au dovedit esenţiale pentru creşterea capabilităţilor infrastructurii tehnice de securitate cibernetică, făcând posibilă detectarea unor incidente şi atacuri cibernetice de tip APT în reţelele şi sistemele informatice care asigură funcţii esenţiale pentru statul român.

Astfel, în cursul anilor, utilizarea sinergică a activităţilor de informaţii şi a sistemelor tehnice de securitate cibernetică s-a dovedit a fi cel mai eficient instrument pe linia asigurării securităţii cibernetice care permite derularea unor măsuri specifice de cyberintelligence pe dimensiunea cunoaşterii, prevenirii şi contracarării ameninţărilor 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 Naționale de Apărare a Țării 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, Ordonanței de Urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență, precum și a Ordonanței de Urgență a Guvernului nr. 124/2021 privind stabilirea cadrului instituțional și financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare și reziliență, precum și pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 155/2020 privind unele măsuri pentru elaborarea Planului național de redresare și reziliență necesar României pentru accesarea de fonduri externe rambursabile și nerambursabile în cadrul Mecanismului de redresare și reziliență.

Riscurile şi ameninţările de tip hibrid la adresa securităţii cibernetice sunt acele ameninţări şi riscuri cibernetice, astfel cum sunt definite în art. 2, lit. b) şi w) din proiectul de lege, care se manifestă sub formă hibridă. Forma hibridă a ameninţărilor şi 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 ameninţare prezintă toate garanţiile de calitate, claritate şi previzibilitate a legii impuse de prevederile art. 1, alin. (5) din Constituţia României, republicată.

3. acţiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spaţiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituţională.

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 proveniență, 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 aceeaşi strategie de apărare a ţării 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"*.
Direcţiile de acţiune pe linia de informaţii, contrainformaţii şi de securitate, conform SNAp 2020-2024, vizează şi *"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"*.
Ţinând cont de cele anterioare, apreciem necesară instituirea, la nivelul legii, a unor noi tipuri de ameninţări care să răspundă nevoilor de securitate cibernetică şi securitate naţională a României, astfel încât să se asigure cu succes protejarea cetăţenilor şi a statului român.
Acţiunile de propagandă şi dezinformare vizate sunt doar cele care afectează ordinea constituţională, adică setul de principii fundamentale pe care este constituit statul român, regimul constituţional de drepturi şi libertăţi fundamentale, regimul constituţional al funcţionării autorităţilor publice de rang constituţional protejarea garanţiilor prevăzute de Constituţie.

Menţionăm că aceste ameninţări instituite au relevanţă doar pentru activitatea de informaţii şi contrainformaţii, activitate desfăşurată doar de autorităţile competente potrivit art. 6 din Legea nr. 51/1991. Prin prezentul proiect de lege nu se pot desfăşura activităţi de natură a restrânge exerciţiul unor drepturi şi libertăţi fundamentale şi nici activităţi specifice culegerii de informaţii, precum nici activităţi de contrainformaţii. Prezenta lege reglementează activitatea de cyberintelligence şi counter cyber intelligence doar la nivel conceptual, urmând ca definiţiile să se completeze corespunzător cu dreptul material prevăzut în Legea nr. 51/1991 şi alte legi speciale din domeniul securităţii naţionale.

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, şi 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 contravenției. 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 evoluție a tehnologiilor, precum și modificarea cadrului legislativ la nivel NATO și UE, legea va fi analizată și revizuită periodic, în vederea adaptării continue la provocările și oportunitățile 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 reziliență 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 și 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 creşterii cheltuielilor bugetare						
4.5 Propuneri pentru a compensa reducerea veniturilor bugetare						
4.6 Calcule detaliate privind fundamentarea modificărilor veniturilor şi/sau cheltuielilor bugetare						

4.7 Prezentarea, în cazul proiectelor de acte normative a căror adoptare atrage majorarea cheltuielilor bugetare, a următoarelor documente:

a) fişa financiară prevăzută la art.15 din Legea nr. 500/2002 privind finanţele publice, cu modificările şi completările ulterioare, însoţită de ipotezele şi metodologia de calcul utilizată;

b) declaraţie conform căreia majorarea de cheltuială respectivă este compatibilă cu obiectivele şi priorităţile strategice specificate în strategia fiscal-bugetară, cu legea bugetară anuală şi cu plafoanele de cheltuieli prezentate în strategia fiscal-bugetară.

4.8 Alte informaţii

Prezentul proiect de lege nu are impact financiar.

Proiectul de lege se încadrează în limitele de cheltuieli aprobate de Guvern pentru anul 2023 şi estimările pentru 2024-2026.

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:

-Prin Decizia CCR nr. 455/2018, parag. 63. Curtea a statuat că securitatea reţelelor şi sistemelor informatice se află în strânsă legătură cu domeniul securităţii naţionale. Acest aspect este reliefat şi în Hotărârea Parlamentului nr. 22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024 şi HG nr. 1.321 din 30 decembrie 2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum şi a Planului de acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027. În acest sens, s-a apreciat că o protecţie adecvată a securităţii cibernetică a României nu se poate realiza fără a se institui şi noi ameninţări cibernetice la adresa securităţii naţionale a României, ameninţări apărute în contextul dezvoltării exponenţiale a activităţilor în spaţiul cibernetic.

Astfel, prin proiectul de lege se completează art. 3 din Legea nr. 51/1991 privind securitatea naţională a României cu următoarele tipuri de ameninţări:

- acţiuni şi inacţiuni de natură a afecta interesele şi obiectivele naţionale de securitate pe linia infrastructurilor de comunicaţii şi tehnologia informaţiei de interes naţional, respectiv ameninţări sau atacuri cibernetice asupra infrastructurilor informatice şi de comunicaţii de interes naţional;
- acţiuni, inacţiuni sau stări de fapt cu consecinţe la nivel naţional, regional sau global care afectează reziliența statului român în raport cu riscurile şi ameninţările de tip hibrid;
- acţiuni derulate de către o entitate statală sau grupare ostilă, prin realizarea, în spaţiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituţională.

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 și/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 și 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 transparența 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 și 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 proicctului de act normativ
8.2 Alte informații

Față 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 ȘI 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 şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE

MARCEL-IOAN BOLOŞ

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

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 și 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

Față de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea și apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

SEBASTIAN-IOAN BURDUJA

AVIZĂM FAVORABIL:

MINISTRUL APĂRĂRII NAȚIONALE

ANGEL TÎLVĂR

MINISTRUL AFACERILOR INTERNE

LUCIAN NICOLAE BODE

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE

IONEL-SORIN BĂLAN

DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII

EDUARD RAUL HELLVIG

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 și 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

Față de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea și apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

SEBASTIAN-IOAN BURDUJA

AVIZĂM FAVORABIL:

MINISTRUL APĂRĂRII NAȚIONALE

ANGEL TÎLVĂR

MINISTRUL AFACERILOR INTERNE

LUCIAN NICOLAE BODE

DIRECTORUL
SERVICIULUI DE TELECOMUNICAȚII SPECIALE

IONEL-SORIN BĂLAN

DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAȚII

EDUARD RAUL HELLVIG

şi angajamentelor rezultate prin PNRR, Legea privind apărarea şi securitatea cibernetică a României trebuie să stabilească cadrul juridic şi instituţional pentru organizarea şi desfăşurarea activităţilor din domeniul securităţii cibernetice şi al apărării cibernetice, mecanismele de cooperare şi răspunsurile instituţiilor în domeniile în cauză. Termenul de intrare în vigoare a legii este 31 decembrie 2022. De asemenea, complexitatea atacurilor cibernetice la adresa autorităţilor şi instituţiilor statului român, în contextul războiului din Ucraina, impune adoptarea unei legislaţii curajoase, care să garanteze funcţionarea infrastructurilor critice, siguranţa cetăţenilor în spaţiul cibernetic şi buna funcţionare a administraţiei publice.
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.
7.3 Alte informaţii
Secţiunea a 8-a: **Măsuri privind implementarea, monitorizarea şi evaluarea proiectului de act normativ**
8.1 Măsurile de punere în aplicare a proiectului de act normativ
8.2 Alte informaţii

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

SEBASTIAN-IOAN BURDUJA

AVIZĂM FAVORABIL:

MINISTRUL APĂRĂRII NAŢIONALE

ANGEL TÎLVĂR

MINISTRUL AFACERILOR INTERNE

LUCIAN NICOLAE BODE

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE

IONEL-SORIN BĂLAN

DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII

EDUARD RAUL HELLVIG

şi angajamentelor rezultate prin PNRR, Legea privind apărarea şi securitatea cibernetică a României trebuie să stabilească cadrul juridic şi instituţional pentru organizarea şi desfăşurarea activităţilor din domeniul securităţii cibernetice şi al apărării cibernetice, mecanismele de cooperare şi răspunsurile instituţiilor în domeniile în cauză. Termenul de intrare în vigoare a legii este 31 decembrie 2022. De asemenea, complexitatea atacurilor cibernetice la adresa autorităţilor şi instituţiilor statului român, în contextul războiului din Ucraina, impune adoptarea unei legislaţii curajoase, care să garanteze funcţionarea infrastructurilor critice, siguranţa cetăţenilor în spaţiul cibernetic şi buna funcţionare a administraţiei publice.
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.
7.3 Alte informaţii
Secţiunea a 8-a: **Măsuri privind implementarea, monitorizarea şi evaluarea proiectului de act normativ**
8.1 Măsurile de punere în aplicare a proiectului de act normativ
8.2 Alte informaţii

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

MINISTRUL CERCETĂRII, INOVĂRII ŞI DIGITALIZĂRII

SEBASTIAN-IOAN BURDUJA

AVIZĂM FAVORABIL:

MINISTRUL APĂRĂRII NAŢIONALE

ANGEL TÎLVĂR

MINISTRUL AFACERILOR INTERNE

LUCIAN NICOLAE BODE

DIRECTORUL SERVICIULUI DE TELECOMUNICAŢII SPECIALE

IONEL-SORIN BĂLAN

DIRECTORUL SERVICIULUI ROMÂN DE INFORMAŢII

EDUARD RAUL HELLVIG

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, precum şi pentru completarea Legii nr. 51/1991 privind securitatea naţională a României, republicată, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE

MARCEL-IOAN BOLOŞ

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN-SILVAN PAHONŢU

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 FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN-SILVAN PAHONŢU

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 CIMPEAN

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL INVESTIŢIILOR ŞI PROIECTELOR EUROPENE

MARCEL-IOAN BOLOŞ

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL FINANTELOR

ADRIAN CACIU

MINISTRUL AFACERILOR EXTERNE

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU

Faţă de cele prezentate mai sus, a fost elaborat proiectul de Lege privind securitatea şi apărarea cibernetică a României, pe care îl supunem Guvernului pentru aprobare.

AVIZĂM FAVORABIL:

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ

LUCIAN-SILVAN PAHONŢU

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE

GABRIEL VLASE

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT

MARIUS PETRESCU

DIRECTORUL DIRECTORATULUI NAŢIONAL DE SECURITATE CIBERNETICĂ

DAN CÎMPEAN

MINISTRUL FINANŢELOR

ADRIAN CÂCIU

MINISTRUL AFACERILOR EXTERNE,

BOGDAN LUCIAN AURESCU

MINISTRUL JUSTIŢIEI

MARIAN-CĂTĂLIN PREDOIU