PARLAMENTUL ROMÂNIEI

SENATUL **CAMERA DEPUTAȚILOR**

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

Parlamentul României adoptă prezenta lege.

CAPITOLUL I
Dispoziții generale

Art. 1.

(1) Prezenta lege stabilește cadrul juridic și instituțional privind organizarea și desfășurarea activităților din domeniile securitate și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate.

(2) Securitatea și apărarea cibernetică se realizează prin adoptarea și implementarea de politici și măsuri în scopul cunoașterii, prevenirii și contracarării vulnerabilităților, riscurilor și amenințărilor în spațiul cibernetic.

Art. 2.

În sensul prezentei legi, termenii și expresiile de mai jos au următoarea semnificație:

a) apărare cibernetică - totalitatea activităților, mijloacelor și măsurilor utilizate pentru a contracara amenințările provenite din spațiul cibernetic și a atenua efectele acestora asupra sistemelor de comunicații și tehnologia informației, sistemelor de armament, rețelelor și sistemelor informatice, care susțin capabilitățile militare de apărare;

b) amenințare cibernetică - astfel cum este definită în art. 2 lit. f) din Ordonanța de Urgență a Guvernului nr. 104/2021;

c) atac cibernetic - acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;

d) audit de securitate cibernetică - activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul unei rețele și sisteme informatice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții 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 situaţiilor de urgență, acțiuni în situaţii de criză în domeniul ordinii publice, prevenirea şi combaterea terorismului, securitate şi 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

funcţionarea Oficiului Registrului Naţional al Informaţiilor 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 şi 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 Organizaţia pentru Cooperare şi 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 responsabilităţii 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 incidenţa prezentei legi se efectuează cu respectarea reglementărilor legale privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal.

(2) Notificările realizate în temeiul prezentei legi nu afectează obligaţiile operatorilor de date cu caracter personal stabilite potrivit art. 33 şi 34 din 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.

(3) În scopul îndeplinirii atribuţiilor ori furnizării serviciilor prevăzute de prezenta lege, precum şi în scopul prevenirii şi răspunsului la incidentele de securitate cibernetică ori al cooperării la nivel naţional, comunitar şi internaţional în prevenirea şi răspunsul la incidentele de securitate cibernetică, autoritățile prevăzute la art. 10 colectează, primesc, prelucrează şi transmit date şi informaţii ce pot constitui sau pot conţine date cu caracter personal, în limitele legislaţiei aplicabile, cu asigurarea respectării prevederilor alin. (2).

Art. 47.

(1) Prezenta 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.

(2) Prezenta 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.

CAPITOLUL XII
Contravenții și sancțiuni

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) și lit. c) a obligației 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) și lit. c) a obligației de comunicare completă a incidentelor de securitate cibernetică, prin intermediul PNRISC, în termenul și condițiile prevăzute la art. 21 alin. (2) și art. 22;

c) nerespectarea de către furnizorii de servicii de securitate cibernetică obligației de a pune la dispoziția autorităților prevăzute la art. 10 date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau sistem informatic al deținătorului sau al unor terți, în condițiile și 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 și aplicare a contravenției 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) și 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 autorităților prevăzute de la art. 10, corespunzător autorității care a formulat cererea de punere la dispoziție a informațiilor și datelor, iar aplicarea sancţiunii corespunzătoare se face prin act administrativ al personalului de control anume desemnat și delegat de conducătorul autorității.

(3) Actul administrativ prevăzut la alin. (1) și (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 și 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 aceleiași 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 și autoritățile 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

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

Art. 50.

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

”n) amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național;

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

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

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 și completările ulterioare, se modifică și se completează astfel:

1. Articolul 2 se modifică și 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) existenţa unor pericole grave actuale sau iminente privind securitatea naţională ***a României****,* ***inclusiv securitatea cibernetică pentru rațiuni de securitate națională****, ori funcţionarea democraţiei constituţionale;”*

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

”(1) Ordonanţele militare se emit în limitele stabilite prin decretul de instituire a măsurii excepţionale, astfel:

1. pe durata stării de asediu:

a) de ministrul apărării naţionale sau de şeful Statului Major General, când starea de asediu a fost instituită pe întregul teritoriu al ţării;

b) de comandanţii de mari unităţi în raza teritorială pentru care au fost împuterniciţi de şeful Statului Major General, când starea de asediu a fost instituită în anumite unităţi administrativ-teritoriale;

2. pe durata stării de urgenţă:

a) de ministrul administraţiei şi internelor sau de înlocuitorul de drept al acestuia, când starea de urgenţă a fost instituită pe întregul teritoriu al ţării;

b) de ofiţerii împuterniciţi de ministrul administraţiei şi internelor sau de înlocuitorii legali ai acestora, când starea de urgenţă a fost instituită în anumite unităţi 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 și 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.

PREȘEDINTELE CAMEREI DEPUTAȚILOR PREȘEDINTELE SENATULUI