LEGE Nr. 58/2023 din 14 martie 2023

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

EMITENT: PARLAMENTUL ROMÂNIEI

PUBLICATĂ ÎN: MONITORUL OFICIAL NR. 214 din 15 martie 2023

**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 cibernetice 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 la art. 2 lit. f) din Ordonanţa de urgenţă a Guvernului nr. 104/2021 privind înfiinţarea Directoratului Naţional de Securitate Cibernetică, aprobată cu modificări şi completări prin Legea nr. 11/2022, cu modificările ulterioare;

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 unor reţele şi sisteme informatice, în vederea identificării disfuncţionalităţilor şi vulnerabilităţilor şi furnizării unor soluţii de remediere a acestora;

e) Advanced Persistent Threat, denumită în continuare APT - astfel cum este definită în art. 2 lit. a) din Ordonanţa de urgenţă a Guvernului nr. 89/2022 privind înfiinţarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud utilizate de autorităţile şi instituţiile publice;

f) centru operaţional de securitate - echipă de experţi în securitate cibernetică, ce are rolul de a monitoriza, analiza şi răspunde la incidentele de securitate cibernetică;

g) criză cibernetică - astfel cum este definită în art. 2 lit. k) din Ordonanţa de urgenţă a Guvernului nr. 104/2021, aprobată cu modificări şi completări prin Legea nr. 11/2022, cu modificările ulterioare;

h) cyber intelligence - activităţi de culegere, procesare, prelucrare analitică şi valorificare a datelor şi informaţiilor privind acţiuni de natură a afecta interesele şi obiectivele naţionale de securitate pe linia tehnologiei informaţiei şi comunicaţiilor, precum şi identificarea, cunoaşterea, prevenirea şi contracararea oricăror acţiuni din spaţiul cibernetic care pot constitui riscuri, vulnerabilităţi şi/sau ameninţări la adresa securităţii şi apărării naţionale a României;

i) cyber counter-intelligence - totalitatea activităţilor, mijloacelor şi măsurilor ofensive şi defensive de identificare, descurajare, neutralizare şi protecţie împotriva activităţilor de informaţii privind acţiuni ostile de natură a afecta interesele şi obiectivele naţionale de securitate, desfăşurate în spaţiul cibernetic şi în domeniul apărării;

j) diplomaţie cibernetică - activitatea diplomatică prin intermediul căreia se realizează promovarea intereselor de politică externă şi de securitate ale României în cadrul formatelor bilaterale şi multilaterale de dialog şi negociere pe teme cu relevanţă pentru domeniul securităţii cibernetice la nivel naţional şi internaţional. Activitatea include promovarea unor obiective care derivă atât din necesitatea asigurării şi consolidării securităţii cibernetice naţionale, cât şi din priorităţile de politică externă ale României;

k) echipă de răspuns la incidente de securitate cibernetică - astfel cum este definită la art. 2 lit. a) din Ordonanţa de urgenţă a Guvernului nr. 104/2021, aprobată cu modificări şi completări prin Legea nr. 11/2022, cu modificările ulterioare;

l) furnizor de servicii tehnice de securitate cibernetică - persoană fizică şi/sau juridică care realizează, în vederea protejării reţelelor şi sistemelor informatice, cel puţin una dintre următoarele activităţi: implementarea de măsuri de securitate cibernetică, evaluarea, monitorizarea şi testarea măsurilor implementate, precum şi managementul riscurilor, ameninţărilor, vulnerabilităţilor şi incidentelor de securitate cibernetică;

m) igienă cibernetică - măsuri de rutină aplicate cu regularitate de către persoanele fizice şi juridice, care au rolul de a reduce expunerea acestora la riscurile pe care le presupun ameninţările cibernetice, conform Regulamentului (UE) 2019/881 al Parlamentului European şi al Consiliului din 17 aprilie 2019 privind ENISA (Agenţia Uniunii Europene pentru Securitate Cibernetică) şi privind certificarea securităţii cibernetice pentru tehnologia informaţiei şi comunicaţiilor şi de abrogare a Regulamentului (UE) nr. 526/2013, denumit în continuare Regulamentul privind securitatea cibernetică;

n) incident de securitate cibernetică - eveniment survenit în spaţiul cibernetic care perturbă funcţionarea uneia sau mai multor reţele şi sisteme informatice şi ale cărui consecinţe sunt de natură a afecta securitatea cibernetică;

o) lanţ de aprovizionare - circuitul de la producător până la beneficiarul final, inclusiv proiectarea, dezvoltarea, producţia, integrarea, implementarea, configurarea, utilizarea şi casarea de produse şi servicii software sau hardware, respectiv reţele şi sisteme informatice;

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

q) managementul riscurilor de securitate cibernetică - strategia organizaţională şi programatică ce presupune activităţi de evaluare şi gestionare a riscurilor de securitate cibernetică;

r) managementul riscurilor de securitate cibernetică specifice lanţului de aprovizionare - strategia organizaţională şi programatică ce presupune activităţi de evaluare şi gestionare a riscurilor în cadrul proceselor din întreg ciclul de viaţă al bunului sau serviciului software sau hardware, respectiv al sistemului sau reţelei informatice, de la producător până la beneficiarul final, inclusiv proiectarea, dezvoltarea, producţia, integrarea, implementarea, configurarea, utilizarea şi casarea de produse şi servicii software sau hardware, respectiv reţele şi sisteme informatice;

s) politici de securitate cibernetică - principii şi reguli generale necesar a fi aplicate pentru asigurarea securităţii reţelelor şi sistemelor informatice;

t) produs de securitate cibernetică - astfel cum este definit la art. 2 lit. l) din Ordonanţa de urgenţă a Guvernului nr. 104/2021, aprobată cu modificări şi completări prin Legea nr. 11/2022, cu modificările ulterioare;

u) reţele şi sisteme informatice - astfel cum sunt definite la art. 3 lit. l) din Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cu modificările şi completările ulterioare;

v) reţele şi sisteme informatice specifice apărării naţionale - reţelele şi sistemele informatice aparţinând Ministerului Apărării Naţionale, reţelele şi sistemele informatice naţionale care susţin activităţile militare ale Organizaţiei Tratatului Atlanticului de Nord, denumită în continuare NATO, şi Uniunii Europene, denumită în continuare UE, precum şi reţelele şi sistemele informatice de interes pentru apărarea naţională date în responsabilitatea sau puse la dispoziţia Ministerului Apărării Naţionale în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război;

w) rezilienţa în spaţiul cibernetic - capacitatea unei reţele sau a unui sistem informatic de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate de dinaintea incidentului sau atacului cibernetic;

x) risc de securitate cibernetică - astfel cum este definit la art. 2 lit. r) din Ordonanţa de urgenţă a Guvernului nr. 89/2022;

y) securitate cibernetică - stare de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic ale resurselor şi serviciilor publice sau private din spaţiul cibernetic;

z) spaţiu cibernetic - mediul virtual generat de reţelele şi sistemele informatice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta;

aa) vulnerabilitate de securitate cibernetică - slăbiciune în proiectarea, implementarea, dezvoltarea, configurarea şi mentenanţa reţelelor şi sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o ameninţare.

ART. 3

(1) În domeniul securităţii cibernetice, prezenta lege se aplică următoarelor:

a) reţelele şi sistemele informatice deţinute, organizate, administrate, utilizate sau aflate în competenţa autorităţilor şi instituţiilor publice din domeniul apărării, ordinii publice, securităţii naţionale, justiţiei, situaţiilor de urgenţă, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat;

b) reţelele şi sistemele informatice deţinute de persoanele fizice şi juridice de drept privat şi utilizate în vederea furnizării de servicii de comunicaţii electronice către autorităţile şi instituţiile administraţiei publice centrale şi locale;

c) reţelele şi sistemele informatice deţinute, organizate, administrate sau utilizate de autorităţi şi instituţii ale administraţiei publice centrale şi locale, altele decât cele prevăzute la lit. a), precum şi de persoane fizice şi juridice care 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 reţelele şi sistemele informatice specifice apărării naţionale.

ART. 4

Obiectivele prezentei legi sunt:

a) asigurarea rezilienţei şi protecţiei reţelelor şi sistemelor informatice ce susţin funcţiile de apărare, securitate naţională, ordine publică şi guvernare;

b) desemnarea autorităţilor competente şi stabilirea cadrului legal de dezvoltare a capabilităţilor necesare îndeplinirii responsabilităţilor acestora în domeniile securităţii şi apărării cibernetice;

c) menţinerea sau restabilirea climatului de securitate cibernetică la nivel naţional, prin cooperarea între autorităţile competente şi asigurarea coordonării unitare de către Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC, a persoanelor juridice responsabile de securitatea cibernetică proprie şi asigurarea unei reacţii rapide şi eficiente la ameninţările provenite din spaţiul cibernetic;

d) stabilirea şi separarea responsabilităţilor şi/sau atribuţiilor funcţionale între furnizorii de reţele, sisteme şi servicii informatice, autorităţile de aplicare a legii, structurile din cadrul instituţiilor cu atribuţii în domeniul securităţii şi apărării cibernetice, astfel încât să se asigure un nivel ridicat de securitate cibernetică la nivel naţional;

e) dezvoltarea şi consolidarea unei culturi de securitate cibernetică la nivel naţional, prin conştientizarea vulnerabilităţilor, riscurilor şi ameninţărilor, respectiv formarea unei conduite proactive şi preventive.

ART. 5

Asigurarea securităţii şi apărării cibernetice se realizează conform următoarelor principii:

a) principiul personalităţii - responsabilitatea asigurării securităţii cibernetice şi/sau apărării cibernetice a unui sistem, a unei reţele şi/sau a unui serviciu informatic revine persoanei fizice sau juridice care le deţine în proprietate, le organizează, administrează şi/sau utilizează, după caz;

b) principiul protecţiei depline - persoana fizică sau juridică responsabilă de securitatea şi/sau apărarea cibernetică a unui sistem, a unei reţele şi/sau a unui serviciu informatic răspunde de managementul riscurilor asociate acestora şi conexiunilor acestora cu alte sisteme, reţele şi/sau servicii informatice terţe, precum şi de implementarea măsurilor tehnice şi organizaţionale necesare protecţiei cibernetice;

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

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

CAPITOLUL II

**Sistemul naţional de securitate cibernetică**

ART. 6

(1) În scopul organizării şi desfăşurării în mod unitar la nivel naţional a activităţilor specifice securităţii cibernetice se înfiinţează Sistemul naţional de securitate cibernetică, denumit în continuare SNSC, drept cadrul general de cooperare care reuneşte autorităţile prevăzute la art. 10 alin. (1), precum şi alte autorităţi şi instituţii publice cu responsabilităţi şi capabilităţi în domeniile de aplicare a prezentei legi, în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii cibernetice.

(2) În exercitarea competenţelor, instituţiile şi autorităţile publice prevăzute la alin. (1) cooperează cu sectorul privat, mediul academic, asociaţiile profesionale şi cu organizaţiile neguvernamentale.

ART. 7

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

(2) Activităţile SNSC sunt coordonate unitar, la nivel operaţional, de către COSC.

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

ART. 8

(1) COSC este un organ consultativ, fără personalitate juridică, în coordonarea CSAT, format din consilierul prezidenţial pentru probleme de securitate naţională, consilierul prim-ministrului pe probleme de securitate naţională, secretarul CSAT, precum şi reprezentanţi ai: Ministerului Apărării Naţionale, denumit în continuare MApN, Ministerului Afacerilor Interne, denumit în continuare MAI, Ministerului Afacerilor Externe, denumit în continuare MAE, Ministerului Cercetării, Inovării şi Digitalizării, denumit în continuare MCID, SRI, Serviciului de Informaţii Externe, denumit în continuare SIE, Serviciului de Telecomunicaţii Speciale, denumit în continuare STS, Serviciului de Protecţie şi Pază, denumit în continuare SPP, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, denumit în continuare ORNISS, Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii, denumit în continuare ANCOM, şi ai Directoratului Naţional de Securitate Cibernetică, denumit în continuare DNSC.

(2) COSC emite avize consultative şi recomandări, adoptate prin consens, care se adresează autorităţilor prevăzute la alin. (1), conform competenţelor legale.

(3) Conducerea COSC este asigurată de un preşedinte - consilierul prezidenţial pentru probleme de securitate naţională şi un vicepreşedinte - consilierul prim-ministrului pe probleme de securitate naţională.

(4) În funcţie de natura şi evoluţia ameninţărilor cibernetice sunt invitaţi să participe în cadrul şedinţelor COSC, fără a avea drept de vot, şi reprezentanţi ai altor entităţi - autorităţi, instituţii publice, persoane juridice de drept public sau privat - care pot contribui la soluţionarea problemelor de securitate cibernetică.

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

ART. 9

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

a) armonizarea reacţiei autorităţilor competente ale statului în situaţii generate de ameninţări cibernetice, care necesită schimbarea nivelului de alertă cibernetică;

b) solicitarea, în caz de necesitate, de asistenţă din partea altor state sau organizaţii şi organisme internaţionale;

c) modalitatea de răspuns la solicitările de asistenţă adresate României din partea altor state sau organizaţii şi organisme internaţionale, altele decât cele din domeniul apărării naţionale;

d) planuri sau direcţii de acţiune, în funcţie de concluziile rezultate şi evoluţia climatului de securitate în spaţiul cibernetic;

e) direcţii de dezvoltare şi investiţii în domeniul securităţii cibernetice;

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

g) modalităţi de gestionare şi răspuns la ameninţări şi atacuri cibernetice.

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

(3) Pentru realizarea securităţii cibernetice, COSC cooperează, după caz, cu organismele de coordonare sau de conducere constituite, la nivel naţional, pentru managementul situaţiilor de urgenţă, acţiuni în situaţii de criză în domeniul ordinii publice, prevenirea şi combaterea terorismului, securitate şi apărare naţională.

CAPITOLUL III

**Autorităţi competente şi responsabilităţi**

ART. 10

(1) Sunt autorităţi competente în sensul prezentei legi:

a) DNSC, pentru spaţiul cibernetic naţional civil, conform prevederilor prezentei legi şi ale Ordonanţei de urgenţă a Guvernului nr. 104/2021, aprobată cu modificări şi completări prin Legea nr. 11/2022, cu modificările ulterioare;

b) MCID, pentru elaborarea şi iniţierea actelor normative şi politicilor publice naţionale în domeniul securităţii cibernetice, al transformării digitale, societăţii informaţionale, comunicaţiilor, cercetării, dezvoltării şi inovării;

c) ANCOM, pentru coordonarea activităţilor desfăşurate în vederea asigurării securităţii cibernetice a reţelelor şi sistemelor informatice proprii şi a celor prevăzute la art. 3 alin. (1) lit. b);

d) MApN, MAI, MAE, SRI, SIE, STS, SPP şi ORNISS, conform atribuţiilor prevăzute la art. 11 - 18.

(2) Autorităţile prevăzute la alin. (1) au următoarele obligaţii:

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

b) să acorde sprijin, în limita atribuţiilor, la solicitarea proprietarilor de reţele şi sisteme informatice aflate în domeniul lor de competenţă, activitate sau responsabilitate, pentru implementarea măsurilor corespunzătoare nivelurilor de alertă cibernetică;

c) să desfăşoare activităţi de informare şi comunicare publică, în limita atribuţiilor;

d) să organizeze sesiuni de formare şi instruire în domeniul securităţii cibernetice, în limita atribuţiilor;

e) să organizeze sau să participe la exerciţii naţionale de securitate cibernetică;

f) să comunice reciproc date de interes referitoare la securitatea cibernetică, inclusiv către celelalte autorităţi şi instituţii publice care deţin, organizează, administrează, utilizează sau au în competenţă reţele şi sisteme informatice.

(3) Autorităţile prevăzute la alin. (1) pot elabora strategii şi norme proprii, prin acte administrative ale conducătorilor autorităţilor, pentru reglementarea activităţilor de securitate cibernetică, la nivel instituţional.

ART. 11

MApN este autoritate competentă la nivel naţional în domeniul apărării cibernetice, iar în sensul prezentei legi are atribuţii în domeniul securităţii cibernetice pentru reţelele şi sistemele informatice care susţin capabilităţile militare de apărare.

ART. 12

MAI, prin structura specializată, este autoritate competentă la nivel naţional în domeniul securităţii cibernetice pentru cunoaşterea, prevenirea, identificarea şi contracararea ameninţărilor, vulnerabilităţilor şi riscurilor cibernetice la adresa sistemelor informatice, reţelelor de comunicaţii şi serviciilor electronice din domeniul de competenţă.

ART. 13

(1) MAE este autoritate competentă, la nivel naţional, în domeniul diplomaţiei cibernetice, pentru asigurarea componenţei diplomatice şi de relaţii internaţionale aferente securităţii cibernetice, şi îndeplineşte următoarele atribuţii:

a) asigură şi coordonează reprezentarea intereselor României în cadrul formatelor internaţionale de negociere şi dialog politic la care România este parte şi al căror obiect de activitate poate produce implicaţii în plan naţional şi internaţional din perspectiva regulilor, principiilor şi normelor de utilizare a tehnologiilor de informaţii şi telecomunicaţii şi a parametrilor conduitei responsabile a statelor în spaţiul cibernetic;

b) sprijină şi promovează colaborarea şi coordonarea strategică, precum şi dialogul României în domeniul securităţii şi apărării cibernetice cu principalii parteneri internaţionali, atât în plan bilateral, cât şi în cadrul formatelor internaţionale la care România este parte, precum şi cu privire la deciziile de politică cu implicaţii naţionale şi internaţionale privind spaţiul cibernetic;

c) promovează şi contribuie la înţelegerea, însuşirea şi aplicarea la nivel naţional şi internaţional a principiilor, regulilor şi normelor de comportament responsabil în spaţiul cibernetic agreate la nivelul ONU, aplicarea dreptului internaţional în materie şi utilizarea setului de instrumente de diplomaţie cibernetică de la nivel UE;

d) promovează interesele României în plan internaţional într-o manieră conformă cadrului naţional de valori democratice şi apartenenţei României la Alianţa Nord-Atlantică (NATO) şi Uniunea Europeană (UE), prin susţinerea şi protejarea caracterului global, deschis, liber, stabil şi sigur al spaţiului cibernetic, a aplicabilităţii depline a dreptului internaţional - inclusiv a dreptului internaţional umanitar şi a legislaţiei internaţionale privind drepturile omului - în acest spaţiu, precum şi a respectării depline a normelor de conduită responsabilă a statelor în spaţiul cibernetic agreate în sistemul ONU, în vederea menţinerii stabilităţii, prevenirii conflictelor şi atenuării ameninţărilor cibernetice.

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

a) asigurării componenţei diplomatice a securităţii cibernetice;

b) promovării unitare a intereselor României şi a unui mesaj coerent în acţiunea externă a României;

c) participării în ecosistemul securităţii cibernetice la nivel internaţional;

d) asigurării răspunsului unitar şi prompt în abordarea de politică externă a evoluţiilor şi situaţiilor nou-apărute din domeniul securităţii cibernetice care pot produce consecinţe pentru securitatea şi apărarea cibernetică.

ART. 14

(1) SRI este autoritate competentă la nivel naţional în domeniul cyber intelligence, precum şi pentru cunoaşterea, analizarea, prevenirea şi contracararea incidentelor şi atacurilor cibernetice care reprezintă ameninţări, riscuri şi vulnerabilităţi la adresa securităţii naţionale a României.

(2) Prevenirea şi combaterea ameninţărilor de tip APT la adresa reţelelor şi sistemelor informatice din domeniul de competenţă, activitate sau responsabilitate, după caz, ale instituţiilor şi autorităţilor prevăzute la art. 10 alin. (1) se realizează astfel:

a) de către MApN în limita competenţelor prevăzute la art. 11;

b) de către MAI în limita competenţelor prevăzute la art. 12;

c) de către SIE în limita competenţelor prevăzute la art. 15;

d) de către STS în limita competenţelor prevăzute la art. 16;

e) de către SPP în limita competenţelor prevăzute la art. 17;

f) de către SRI, în toate celelalte cazuri.

(3) În situaţia existenţei unor ameninţări cibernetice la adresa reţelelor şi sistemelor informatice prevăzute la art. 3 alin. (1) lit. b) şi c), care ar aduce atingere securităţii naţionale, SRI informează ANCOM şi DNSC, în condiţiile legii.

ART. 15

SIE este autoritate competentă pentru cunoaşterea, analizarea, prevenirea şi contracararea incidentelor şi atacurilor cibernetice care reprezintă ameninţări, riscuri şi vulnerabilităţi cibernetice la adresa reţelelor şi sistemelor informatice din responsabilitate.

ART. 16

STS este autoritate competentă în domeniul securităţii cibernetice pentru infrastructurile, reţelele, sistemele, serviciile proprii şi spectrul de frecvenţe radio proprii, precum şi pentru cele reglementate prin legi speciale.

ART. 17

SPP este autoritate competentă în domeniul securităţii cibernetice pentru infrastructurile, reţelele, sistemele şi serviciile proprii, coordonează măsurile de securitate cibernetică pentru demnitarii cărora le asigură protecţie şi acţionează, independent sau în cooperare cu celelalte structuri din domeniile apărării, ordinii publice şi securităţii naţionale, pentru implementarea acestora.

ART. 18

ORNISS coordonează activităţile desfăşurate în vederea asigurării securităţii cibernetice a reţelelor şi sistemelor informatice care stochează, procesează sau transmit informaţii clasificate, conform atribuţiilor prevăzute în Ordonanţa de urgenţă a Guvernului nr. 153/2002 privind organizarea şi funcţionarea Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, aprobată prin Legea nr. 101/2003, cu modificările şi completările ulterioare.

ART. 19

(1) Autorităţile prevăzute la art. 10 constituie şi operaţionalizează structuri specializate în realizarea de audit de securitate cibernetică şi structuri specializate de securitate cibernetică pentru gestionarea ameninţărilor cibernetice la adresa reţelelor şi sistemelor informatice din responsabilitate.

(2) Structurile prevăzute la alin. (1) se înfiinţează, se organizează şi funcţionează prin act administrativ al conducătorului autorităţilor prevăzute la art. 10.

CAPITOLUL IV

**Managementul incidentelor şi rezilienţa în spaţiul cibernetic**

SECŢIUNEA 1

**Managementul incidentelor de securitate cibernetică**

ART. 20

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

(2) Autorităţile prevăzute la art. 10 au acces la PNRISC, pentru îndeplinirea responsabilităţilor care le revin.

(3) Procesarea informaţiilor din PNRISC se realizează cu respectarea politicilor de confidenţialitate şi transparenţă stabilite şi implementate de DNSC.

ART. 21

(1) Persoanele prevăzute la art. 3 alin. (1) lit. b) şi c) au obligaţia 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 iniţială, informaţiile putând fi completate şi ulterior cu cele care reies din investigaţiile realizate pe baza evenimentului.

(3) Fără a aduce atingere normelor aplicabile în materie de raportare, confidenţialitate, secret profesional şi protecţia informaţiilor clasificate, autorităţile care au în responsabilitate reţele şi sisteme informatice prevăzute la art. 3 alin. (1) lit. a) notifică incidentele de securitate cibernetică prin intermediul PNRISC.

ART. 22

Incidentele de securitate cibernetică sunt notificate în PNRISC în condiţiile capitolului IV secţiunea a 2-a din Legea nr. 362/2018, cu modificările şi completările ulterioare.

ART. 23

În domeniul managementului incidentelor de securitate cibernetică, autorităţile prevăzute la art. 10 alin. (1) lit. c) şi d) au următoarele responsabilităţi:

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

b) să evalueze datele şi informaţiile cu privire la incidentele şi atacurile cibernetice la adresa reţelelor şi sistemelor informatice aflate în domeniul lor de competenţă, activitate sau responsabilitate;

c) să coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul reţelelor şi sistemelor informatice aflate în domeniul lor de competenţă, activitate sau responsabilitate;

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

e) să păstreze pe o perioadă de 5 ani datele referitoare la incidentele de securitate cibernetică şi rezultatele măsurilor de contracarare a acestora, fără a colecta date de conţinut.

SECŢIUNEA a 2-a

**Rezilienţa în spaţiul cibernetic**

ART. 24

(1) Asigurarea rezilienţei în spaţiul cibernetic se realizează prin implementarea de măsuri proactive şi reactive de către instituţiile şi persoanele prevăzute la art. 3.

(2) Măsurile proactive sunt destinate prevenirii incidentelor de securitate cibernetică şi descurajării autorilor atacurilor din spaţiul cibernetic şi includ:

a) constituirea şi 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 şi măsuri de control tehnic privind apărarea şi securitatea cibernetică;

c) constituirea şi operarea centrelor operaţionale de securitate;

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

e) dezvoltarea unor capabilităţi proactive, care să permită cunoaşterea anticipativă a ameninţărilor din spaţiul cibernetic;

f) finanţarea pentru dezvoltarea capabilităţilor de securitate şi apărare cibernetică, inclusiv din perspectiva cercetării, dezvoltării, inovării şi digitalizării în domeniu şi asimilării tehnologiilor emergente;

g) cooperarea şi schimbul de informaţii între autorităţile competente şi sectorul privat pentru identificarea ameninţărilor cibernetice;

h) identificarea serviciilor, reţelelor şi sistemelor informatice, conform competenţelor fiecărei instituţii responsabile de administrare şi asigurarea managementului acestora;

i) implementarea de soluţii de securitate cibernetică, care să crească capacitatea de detecţie şi capabilităţile de prevenţie la atacuri cibernetice;

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

k) demonstrarea nivelului de maturitate atins de capabilităţile de securitate cibernetică în cadrul exerciţiilor organizate la nivel naţional sau internaţional;

l) instruirea personalului din cadrul persoanelor prevăzute la art. 3 în domeniul securităţii cibernetice, prin realizarea periodică de campanii de informare, conştientizare şi igienă cibernetică la nivel organizaţional.

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

a) punerea în aplicare a planurilor de răspuns la incidente şi de contingenţă în domeniul securităţii cibernetice;

b) utilizarea rezervei de resurse şi de capabilităţi de securitate cibernetică;

c) restabilirea funcţionalităţii reţelelor şi sistemelor informatice din cadrul instituţiilor afectate;

d) diseminarea informaţiilor despre evenimentele cibernetice prin alerte în mediul interinstituţional pentru evaluarea riscului şi diminuarea posibilităţilor de exploatare a vulnerabilităţilor;

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

ART. 25

(1) Furnizorii de servicii tehnice de securitate cibernetică au obligaţia de a pune la dispoziţia autorităţilor prevăzute la art. 10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date şi informaţii privind incidente, respectiv, în maximum 5 zile de la data primirii solicitării, cu privire la ameninţări, riscuri sau vulnerabilităţi a căror manifestare poate afecta o reţea sau un sistem informatic dintre cele prevăzute la art. 3 alin. (1), precum şi interconectarea acestora cu terţii şi cu utilizatorii finali.

(2) Datele şi informaţiile prevăzute la alin. (1) nu vizează, prin scopul solicitării, date cu caracter personal şi date de conţinut.

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

ART. 26

Pentru creşterea nivelului de rezilienţă cibernetică şi realizarea descurajării în spaţiul cibernetic la nivel naţional, DNSC şi instituţiile din domeniile apărării, ordinii publice şi securităţii naţionale iau măsuri pentru:

a) realizarea unui cadru interinstituţional de securitate cibernetică care să permită instruirea comună, transferul de cunoştinţe, schimbul de informaţii, sprijinul de specialitate şi federalizarea de resurse şi capabilităţi de securitate cibernetică;

b) îmbunătăţirea şi extinderea capabilităţilor de protecţie şi detecţie automată a atacurilor, prin implementarea de instrumente de analiză inteligentă a ameninţărilor şi distribuirea oportună a indicatorilor şi avertizărilor privind iminenţa unor atacuri cibernetice asupra reţelelor şi sistemelor informatice naţionale;

c) elaborarea de manuale cu tehnici, tactici şi proceduri, precum şi a planurilor de contingenţă şi exersarea lor în cadrul exerciţiilor de securitate cibernetică în scopul întăririi rezilienţei în spaţiul cibernetic;

d) constituirea de echipe de intervenţie la incidente de securitate cibernetică de tip computer security incident response team, denumit în continuare CSIRT, echipe de protecţie cibernetică şi/sau alte forţe specializate în desfăşurarea de acţiuni în spaţiul cibernetic.

CAPITOLUL V

**Sistemul Naţional de Alertă Cibernetică**

ART. 27

(1) Sistemul Naţional de Alertă Cibernetică, denumit în continuare SNAC, constă într-un ansamblu de măsuri tehnice şi procedurale destinate prevenirii, descurajării şi combaterii acţiunilor sau inacţiunilor ce se pot constitui în vulnerabilităţi, riscuri sau ameninţări la adresa securităţii cibernetice a României.

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

ART. 28

(1) Nivelurile de alertă cibernetică şi modalităţile de acţiune în situaţii de alertă cibernetică se stabilesc printr-o metodologie elaborată de DNSC, avizată conform de COSC şi aprobată prin ordin al directorului DNSC.

(2) Instituirea nivelurilor de alertă, precum şi trecerea de la un nivel la altul se decid de către directorul DNSC, cu avizul consultativ şi 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 obligaţia să elaboreze planuri proprii de acţiune pentru fiecare tip de alertă cibernetică, potrivit metodologiei prevăzute la art. 28 alin. (1).

(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 atribuţii:

a) apără şi protejează sistemele şi reţelele informatice aparţinând MApN;

b) planifică şi conduce operaţii în spaţiul cibernetic prin Centrul Naţional Militar de Comandă, potrivit legii;

c) planifică şi execută operaţii defensive în spaţiul cibernetic, pe timp de pace, prin Comandamentul Apărării Cibernetice;

d) dezvoltă şi implementează capabilităţi militare de execuţie a operaţiilor în spaţiul cibernetic prin Comandamentul Apărării Cibernetice;

e) desfăşoară operaţii de cyber intelligence şi cyber counter-intelligence în spaţiul cibernetic în scopul cunoaşterii, monitorizării şi contracarării ameninţărilor la adresa apărării naţionale, la adresa structurilor MApN şi a forţelor aliate;

f) dezvoltă capabilităţi de răspuns ofensiv, în mod individual sau ca parte dintr-o coaliţie ori alianţă, utilizabile în caz de atacuri cibernetice care contravin dreptului internaţional;

g) participă la activităţi de descurajare în spaţiul cibernetic;

h) asigură punctul unic de contact în relaţia cu NATO pentru operaţiuni militare în spaţiul cibernetic;

i) elaborează şi implementează politici şi standarde în domeniul apărării cibernetice, în acord cu interesul naţional, precum şi cu standardele şi cerinţele ce decurg din aderarea României la NATO, UE şi Organizaţia pentru Cooperare şi Dezvoltare Economică.

(2) MApN cooperează cu celelalte structuri din cadrul sistemului naţional de apărare, ordine publică şi securitate naţională pentru asigurarea apărării cibernetice a reţelelor şi sistemelor informatice din domeniul lor de competenţă, activitate sau responsabilitate.

(3) Activităţile de apărare cibernetică şi operaţiunile în spaţiul cibernetic, dezvoltarea de capabilităţi de răspuns ofensiv şi activităţile de descurajare în spaţiul cibernetic prevăzute la alin. (1) se organizează, planifică şi desfăşoară cu respectarea dreptului internaţional, inclusiv a dreptului internaţional umanitar, a normelor de conduită responsabilă a statelor în spaţiul cibernetic agreate în sistemul ONU, precum şi a celorlalte tratate la care România este parte.

ART. 31

MApN stabileşte, prin hotărâre a Guvernului, condiţiile concrete de recrutare/selecţie, modalităţile de formare şi instruire periodică, măsurile de stimulare ale persoanelor juridice de drept privat, precum şi condiţiile necesare constituirii şi utilizării rezervei de specialişti în domeniul apărării cibernetice.

CAPITOLUL VII

**Cercetare, dezvoltare şi inovare în domeniul securităţii cibernetice**

ART. 32

(1) Cercetarea, dezvoltarea şi inovarea în domeniul securităţii cibernetice sunt parte integrantă a sistemului naţional de cercetare, dezvoltare şi inovare şi se aliniază măsurilor promovate de MCID pentru încadrarea spaţiului românesc al cercetării în Spaţiul European al Cercetării.

(2) MCID elaborează un program multianual de finanţare a proiectelor de cercetare, dezvoltare şi inovare în domeniul securităţii cibernetice, la care pot participa organizaţii de cercetare publice şi private, precum şi autorităţi şi instituţii publice cu atribuţii în domeniul securităţii cibernetice.

(3) Prin derogare de la prevederile art. 30 alin. (2) din Legea responsabilităţii fiscal-bugetare nr. 69/2010, republicată, cu modificările şi completările ulterioare, bugetul anual alocat programului prevăzut la alin. (2) este de minimum 10% din bugetul alocat programelor de cercetare finanţate de MCID pentru anul respectiv.

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

ART. 33

(1) Autorităţile prevăzute la art. 10 dezvoltă strategii şi politici proprii privind cercetarea, dezvoltarea şi inovarea în domeniile securităţii şi apărării cibernetice, în funcţie de potenţialul ştiinţific avut la dispoziţie, de competenţele sau de misiunile specifice.

(2) La nivelul fiecărei autorităţi prevăzute la art. 10 se desemnează de către conducătorul instituţiei entitatea responsabilă pentru managementul activităţilor de cercetare, dezvoltare şi inovare în domeniile securităţii şi apărării cibernetice.

(3) Autorităţile prevăzute la art. 10 cooperează cu mediul academic, industria de profil şi Centrul european de competenţe în domeniul industrial, tehnologic şi de cercetare în materie de securitate cibernetică, precum şi cu Reţeaua de centre naţionale de coordonare, pentru implementarea următoarelor linii de efort în domeniul cercetării, dezvoltării, inovării şi digitalizării:

a) menţinerea unei poziţii avansate în rândul instituţiilor ce investesc şi valorifică rezultatele activităţilor de cercetare, dezvoltare şi inovare desfăşurate în domeniul securităţii cibernetice;

b) dezvoltarea şi menţinerea de parteneriate eficiente în domeniul cercetării, dezvoltării, inovării şi digitalizării;

c) promovarea de noi tehnologii, de prototipuri şi demonstratoare tehnologice în domeniile securităţii şi apărării cibernetice;

d) dezvoltarea reţelelor de experţi în domeniu la nivel naţional şi interinstituţional.

CAPITOLUL VIII

**Cooperare în domeniul securităţii şi apărării cibernetice**

SECŢIUNEA 1

**La nivel naţional**

ART. 34

(1) Cooperarea în domeniul securităţii şi apărării cibernetice, la nivel naţional, are următoarele obiective:

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

b) valorificarea experienţei şi bunelor practici în domeniile securităţii şi apărării cibernetice;

c) implementarea unui mediu deschis, transparent, colaborativ şi de încredere între instituţiile cu responsabilităţi în domeniile securităţii şi apărării cibernetice la nivel naţional;

d) acceptarea şi promovarea standardelor de securitate cibernetică în parteneriat cu industria naţională de profil;

e) dezvoltarea şi implementarea de soluţii de securitate cibernetică de către toate autorităţile şi instituţiile publice;

f) dezvoltarea unei culturi de securitate cibernetică şi implementarea bunelor practici de igienă cibernetică la nivel naţional;

g) asigurarea comunicării publice coordonate şi unitare, atunci când situaţia o impune, în cadrul situaţiilor de alertă cibernetică, atacuri cibernetice cu impact semnificativ sau a ameninţărilor nou-apărute din spaţiul cibernetic;

h) conştientizarea situaţională şi comunicarea către public a măsurilor recomandate spre implementare, în vederea facilitării managementului situaţiilor de criză cibernetică.

(2) Activităţile de cooperare la nivel naţional includ cel puţin următoarele:

a) dezvoltare de capabilităţi de securitate şi apărare cibernetică;

b) raportarea de incidente cibernetice şi cooperarea în situaţii de alertă cibernetică;

c) programe de cercetare, dezvoltare, inovare şi digitalizare;

d) cursuri de formare profesională sau de specializare;

e) exerciţii de securitate cibernetică;

f) conferinţe şi alte manifestări ştiinţifice.

SECŢIUNEA a 2-a

**La nivel internaţional**

ART. 35

Cooperarea internaţională în domeniile securităţii şi apărării cibernetice are următoarele obiective:

a) informarea reciprocă privind ameninţările din spaţiul cibernetic;

b) creşterea capacităţii de reacţie la ameninţările cibernetice şi formarea coeziunii de acţiune a echipelor specializate, în cadrul exerciţiilor multinaţionale de securitate şi apărare cibernetică;

c) verificarea şi validarea nivelului de maturitate atins de capabilităţile de securitate şi apărare cibernetică implementate la nivel naţional;

d) realizarea interoperabilităţii tehnice şi procedurale a forţelor de apărare cibernetică;

e) dezvoltarea şi exersarea mecanismelor de avertizare şi schimb de informaţii privind ameninţările de natură cibernetică, precum şi ale celor de descurajare;

f) dezvoltarea de proiecte comune de cercetare, dezvoltare şi inovare în domeniile securităţii şi apărării cibernetice;

g) evaluarea şi implementarea de soluţii revoluţionare de securitate cibernetică, precum şi adoptarea de concepte noi de proiectare şi utilizare a tehnologiilor emergente în spaţiul cibernetic;

h) creşterea contribuţiei naţionale la activităţi de transfer de cunoştinţe, de creştere a încrederii şi de dezvoltare a capacităţii în domeniul securităţii şi apărării cibernetice;

i) reprezentarea intereselor României în cadrul formatelor internaţionale de negociere şi dialog al căror obiect de activitate poate produce implicaţii în plan naţional şi internaţional din perspectiva regulilor, principiilor şi normelor de utilizare a tehnologiilor de informaţii şi telecomunicaţii şi a parametrilor conduitei responsabile a statelor în spaţiul cibernetic, precum şi în acţiunile comune cu partenerii strategici şi de la nivelul NATO şi UE în aplicarea instrumentelor diplomaţiei cibernetice pentru descurajarea atacurilor, ameninţărilor, riscurilor şi vulnerabilităţilor cibernetice la nivel internaţional.

ART. 36

(1) Autorităţile prevăzute la art. 10 cooperează cu autorităţile şi instituţiile din statele membre, cu organismele, agenţiile şi instituţiile UE şi ale NATO cu atribuţii în domeniul securităţii şi apărării cibernetice, inclusiv cu autorităţi şi instituţii din alte state partenere, conform domeniilor de competenţă.

(2) Cooperarea în domeniul apărării cibernetice cu instituţiile NATO, cu armatele ţărilor membre UE şi ale statelor aliate se realizează prin MApN.

(3) Pentru asigurarea coordonării şi a dialogului interinstituţional în vederea asigurării unei reprezentări adecvate şi a unui mesaj coerent în acţiunea externă a României, precum şi pentru realizarea atribuţiilor prevăzute la art. 13, activităţile prevăzute la alin. (1) se realizează în cooperare cu MAE.

CAPITOLUL IX

**Formarea profesională, educaţia, instruirea**

ART. 37

Persoanele prevăzute la art. 3 au obligaţia de a asigura, pentru personalul propriu, formarea profesională, educaţia şi instruirea în domeniul securităţii şi apărării cibernetice prin cursuri, exerciţii, conferinţe, seminarii, precum şi alte tipuri de activităţi.

ART. 38

(1) Autorităţile şi instituţiile din domeniile apărării, ordinii publice şi securităţii naţionale pot organiza, la nivel instituţional sau interinstituţional, exerciţii de securitate şi apărare cibernetică.

(2) Autorităţile şi instituţiile prevăzute la alin. (1) elaborează şi adoptă un plan anual şi multianual de exerciţii de securitate şi apărare cibernetică.

ART. 39

(1) Autorităţile şi instituţiile din domeniile apărării, ordinii publice şi securităţii naţionale participă la exerciţii de securitate şi apărare cibernetică organizate la nivel internaţional, respectiv la nivelul UE şi NATO.

(2) Participarea la exerciţiile de apărare cibernetică organizate în cadrul NATO se realizează sub coordonarea MApN.

ART. 40

DNSC şi autorităţile şi instituţiile din domeniile apărării, ordinii publice şi securităţii naţionale au următoarele atribuţii:

a) asigură informarea şi pregătirea, la nivel naţional, a populaţiei, precum şi a tuturor persoanelor fizice şi juridice care acţionează în spaţiul cibernetic naţional, inclusiv a operatorilor economici din sectoarele stabilite potrivit dispoziţiilor Legii nr. 362/2018, cu modificările şi completările ulterioare, şi din sectorul public cu privire la riscurile, ameninţările şi vulnerabilităţile de securitate cibernetică identificate;

b) promovează dezvoltarea unui comportament responsabil în spaţiul cibernetic pentru persoanele fizice şi juridice prin conştientizarea efectelor atacurilor cibernetice şi a modalităţii de semnalare a acestora;

c) emit informări privind obligaţiile care derivă din calitatea de proprietar, administrator, organizator, furnizor sau utilizator al reţelelor şi sistemelor informatice, privind atitudinea în faţa unor posibile atacuri cibernetice, privind conştientizarea cetăţenilor şi instituţiilor publice şi private, despre necesitatea semnalării/notificării atacurilor cibernetice;

d) dezvoltă cadrul naţional de conştientizare a populaţiei în cooperare cu mediul public, privat şi academic, în scopul pregătirii populaţiei privind modalităţile de comportament, reacţie şi apărare în mediul online;

e) desfăşoară şi participă la campanii/acţiuni de prevenire şi conştientizare a cauzelor şi consecinţelor atacurilor cibernetice asupra reţelelor şi sistemelor informatice civile, la nivel internaţional, naţional şi regional.

CAPITOLUL X

**Securitatea lanţului de aprovizionare**

ART. 41

(1) Persoanele prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanţului de aprovizionare, în conformitate cu prevederile art. 52 alin. (1).

(2) Riscurile lanţului de aprovizionare includ cel puţin următoarele:

a) livrarea de soluţii informatice false sau contrafăcute;

b) producţie neautorizată;

c) manipulare frauduloasă a produselor şi serviciilor software şi hardware, respectiv a sistemelor şi reţelelor informatice;

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

e) servicii software şi hardware periculoase pentru funcţionare;

f) spionaj cibernetic;

g) compromiteri neintenţionate ale sistemelor şi reţelelor informatice;

h) practici deficitare de fabricaţie şi dezvoltare de produse software şi hardware.

ART. 42

Persoanele prevăzute la art. 3 desemnează responsabili de securitate cibernetică, în conformitate cu prevederile art. 52 alin. (1), pentru:

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

b) includerea în conţinutul politicilor, strategiilor şi proceselor existente a cerinţelor noi şi emergente privind managementul riscurilor cibernetice specifice lanţului de aprovizionare;

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

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

e) stabilirea metodologiilor şi aplicaţiilor folosite în evaluarea riscurilor de securitate cibernetică, specifice lanţului de aprovizionare;

f) schimbul de informaţii cu celelalte instituţii referitoare la ameninţările, riscurile şi vulnerabilităţile de natură cibernetică specifice lanţului de aprovizionare;

g) elaborarea metodologiei de evaluare a nivelului de maturitate şi a capacităţii operatorilor de pe lanţurile de aprovizionare de a realiza managementul riscurilor de securitate cibernetică;

h) colectarea şi actualizarea datelor referitoare la eficienţa 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 lanţului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor şi programelor de instruire existente.

ART. 44

Persoanele prevăzute la art. 3 pot dezvolta capabilităţi avansate de testare şi evaluare a riscurilor de securitate cibernetică în scopul identificării vulnerabilităţilor cibernetice ale echipamentelor, produselor software sau pieselor componente achiziţionate sau dezvoltate la nivel instituţional.

CAPITOLUL XI

**Confidenţialitatea şi protecţia securităţii datelor şi informaţiilor persoanelor fizice şi juridice**

ART. 45

(1) Autorităţile prevăzute la art. 10 care solicită şi primesc date şi informaţii de la orice persoană fizică şi juridică în temeiul prezentei legi iau măsuri adecvate pentru a proteja interesele de securitate şi comerciale ale acestora, ale persoanelor care furnizează datele şi informaţiile respective, precum şi ale persoanelor la care se referă datele şi informaţiile respective.

(2) Transmiterea de date şi informaţii obţinute potrivit prezentei legi de la orice persoană fizică şi juridică de drept privat poate fi efectuată numai pentru îndeplinirea atribuţiilor legale ale autorităţilor şi instituţiilor care obţin aceste date şi informaţii, cu garantarea păstrării confidenţialităţii datelor cu caracter personal şi a protecţiei intereselor şi secretelor comerciale ale persoanelor fizice şi 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 (Regulamentul general privind protecţia datelor).

(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, autorităţile 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, 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

**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 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 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 a 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 1% 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 3% 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 unu şi maximum 25 de salarii minime brute pe economie.

(7) În măsura în care prezenta lege nu prevede altfel, contravenţiilor prevăzute la alin. (1) li se aplică dispoziţiile Ordonanţei Guvernului nr. 2/2001, 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 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) Actele administrative prevăzute 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 prevăzute la 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. 25 alin. (2) 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. (1) sau (2) se comunică contravenientului în termen de 15 zile de la data emiterii acestuia.

(6) Odată cu actul administrativ prevăzut la alin. (1) sau (2), 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. (1) sau (2), neatacat în termenul prevăzut la alin. (9), precum şi hotărârea judecătorească definitivă prin care s-a soluţionat acţiunea în contencios administrativ constituie titlu executoriu, fără vreo altă formalitate. Acţiunea în contencios administrativ în condiţiile prevăzute la 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. (1) sau (2), neatacat în termenul prevăzut la alin. (9), 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, actele administrative şi deciziile adoptate potrivit dispoziţiilor prezentei legi 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.

(10) 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, executarea sancţiunilor contravenţionale aplicate se prescrie dacă actul administrativ prevăzut la alin. (1) sau (2) nu a fost comunicat contravenientului în termen de 15 zile de la data aplicării sancţiunii.

CAPITOLUL XIII

**Dispoziţii privind completarea art. 3 din Legea nr. 51/1991 privind securitatea naţională a României, republicată, cu modificările şi completările ulterioare, precum şi pentru modificarea Ordonanţei de urgenţă a Guvernului nr. 1/1999 privind regimul stării de asediu şi regimul stării de urgenţă, aprobată cu modificări şi completări prin Legea nr. 453/2004, cu modificările şi completările ulterioare**

ART. 50

La articolul 3 din Legea nr. 51/1991 privind securitatea naţională a României, republicată în Monitorul Oficial al României, Partea I, nr. 190 din 18 martie 2014, cu modificările şi completările ulterioare, după litera m) se introduc trei noi litere, literele n) - p), cu 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 rezilienţa statului în raport cu riscurile şi ameninţările 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 a Guvernului 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, aprobată cu modificări şi completări prin Legea nr. 453/2004, cu modificările şi completările ulterioare, se modifică după cum urmează:

**1. Articolul 2 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) va avea următorul cuprins:**

"a) existenţa unor pericole grave actuale sau iminente privind securitatea naţională a României, inclusiv securitatea cibernetică pentru raţiuni de securitate naţională, ori funcţionarea democraţiei constituţionale;".

**3. Articolul 23 va avea următorul cuprins:**

"ART. 23

(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 al Apărării, 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 al Apărării, când starea de asediu a fost instituită în anumite unităţi administrativ-teritoriale;

2. pe durata stării de urgenţă:

a) de ministrul afacerilor interne 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 afacerilor interne sau de înlocuitorii legali ai acestora, când starea de urgenţă a fost instituită în anumite unităţi administrativ-teritoriale.

(2) În situaţia instituirii măsurii excepţionale pentru cauze ce privesc securitatea sau apărarea cibernetică în condiţiile art. 2 şi art. 3 lit. a), emitenţii ordonanţelor militare solicită avizul prealabil şi consultativ al Consiliului Operativ de Securitate Cibernetică."

CAPITOLUL XIV

**Dispoziţii tranzitorii şi finale**

ART. 52

(1) Categoriile de persoane prevăzute la art. 3 alin. (1) lit. c) se stabilesc prin hotărâre a Guvernului, iniţiată de MCID, adoptată în maximum 60 de zile de la data intrării în vigoare a prezentei legi.

(2) Actele administrative prevăzute la art. 19 alin. (2) se emit în maximum 90 de zile de la data intrării în vigoare a prezentei legi.

(3) În vederea aplicării prevederilor art. 20 alin. (3), politicile de confidenţialitate şi transparenţă 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, autorităţile prevăzute la art. 10 adoptă măsuri proprii de rezilienţă în spaţiul cibernetic în maximum 120 de zile de la data intrării în vigoare a prezentei legi.

(5) Normele metodologice privind solicitarea şi comunicarea datelor şi informaţiilor prevăzute la art. 25 alin. (1) se stabilesc prin hotărâre a Guvernului, iniţiată de MCID, adoptată în maximum 90 de zile de la data intrării în vigoare a prezentei legi.

(6) 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.

(7) În vederea aplicării prevederilor art. 31, Guvernul adoptă respectiva hotărâre în maximum 90 de zile de la data intrării în vigoare a prezentei legi.

(8) În vederea aplicării prevederilor art. 32 alin. (2) - (4), ministrul cercetării, inovării şi digitalizării emite respectivul ordin în maximum 120 de zile de la data intrării în vigoare a prezentei legi.

ART. 53

Prevederile art. 48 şi 49 intră în vigoare la 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.

p. PREŞEDINTELE CAMEREI DEPUTAŢILOR,

**CIPRIAN-CONSTANTIN ŞERBAN**

p. PREŞEDINTELE SENATULUI,

**VIRGIL GURAN**

Bucureşti, 14 martie 2023.

Nr. 58.

---------------