# LEGE PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI

## CAPITOLUL I - DISPOZIŢII GENERALE

**Art. 1** - (1) Legea stabileşte cadrul juridic privind organizarea şi desfăşurarea activităţilor din domeniul securităţii cibernetice a României şi asigurarea protejării drepturilor şi libertăţilor fundamentale ale cetăţenilor în spaţiul cibernetic.

(2) Securitatea cibernetică este componentă a securităţii naţionale a României şi se realizează prin adoptarea şi implementarea de politici şi măsuri de securitate la nivelul deţinătorilor de infrastructuri cibernetice în scopul cunoaşterii, prevenirii şi contracarării riscurilor şi ameninţărilor în spaţiul cibernetic.

**Art. 2** - Prezenta lege se aplică:

a) autorităţilor şi instituţiilor publice, persoanelor juridice deţinătoare de infrastructuri cibernetice care susţin servicii publice sau de interes public, ori servicii ale societăţii informaţionale, a căror afectare aduce atingere securităţii naţionale sau prejudicii grave statului român ori cetăţenilor acestuia;

b) persoanelor juridice, deţinătoare de infrastructuri cibernetice care prelucrează date cu caracter personal;

c) furnizorilor de reţele publice de comunicaţii electronice şi furnizorilor de servicii de comunicaţii electronice destinate publicului;

d) furnizorilor de servicii de găzduire internet;

e) furnizorilor de servicii de securitate cibernetică.

**Art. 3** - În sensul prezentei legi, termenii şi expresiile de mai jos au următoarea semnificaţie:

a) ameninţare cibernetică - circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii cibernetice;

b) alertă cibernetică - semnalare referitoare la un posibil incident de securitate cibernetică;

c) apărare cibernetică - acţiuni desfăşurate în spaţiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva ameninţărilor asupra infrastructurilor cibernetice destinate apărării naţionale;

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

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

f) Catalog ICIN - registru de evidenţă a infrastructurilor cibernetice de interes naţional;

g) cerinţe minime de securitate cibernetică - condiţii de natură organizatorică, tehnică sau procedurală,destinate implementării politicilor de securitate;

h) date de jurnalizare - date generate în mod automat de componente software şi hardware care descriu istoricul acţiunilor ce au loc la nivelul acestora;

i) date tehnice - descriere generală a infrastructurii cibernetice, rolul şi funcţionalităţile asigurate de aceasta, arhitectura, tipuri şi număr de utilizatori, fluxuri informaţionale susţinute, descrierea capacităţii de stocare/prelucrare, fişiere de jurnalizare a evenimentelor ce au loc în sistemele de securitate software şi hardware, sistemele de operare şi aplicaţiile software;

j) deţinători de infrastructuri cibernetice - persoane juridice de drept public sau privat care au calitatea de proprietari, administratori sau operatori de infrastructuri cibernetice;

k) furnizori de servicii de găzduire internet - orice persoană juridică ce desfăşoară activităţi pe teritoriul României, care pune la dispoziţie infrastructuri cibernetice, fizice sau virtuale, pentru derularea de activităţi şi servicii ale societăţii informaţionale;

l) furnizor de servicii de securitate cibernetică - orice persoană juridică ce realizează, în vederea protejării infrastructurilor cibernetice, cel puţin una dintre următoarele activităţi: implementare de politici, proceduri şi măsuri, auditare, evaluare, testare a măsurilor implementate, management al incidentelor de securitate;

m) incident de securitate cibernetică - eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;

n) infrastructuri cibernetice - infrastructuri de tehnologia informaţiei, constând în sisteme informatice, aplicaţii aferente, reţele de comunicaţii electronice;

o) infrastructuri cibernetice de interes naţional - infrastructuri cibernetice deţinute de persoane juridice de drept privat, care susţin servicii publice sau de interes public ori servicii ale societăţii informaţionale, sau infrastructuri cibernetice deţinute de autorităţi şi instituţii publice, a căror afectare aduce atingere securităţii naţionale, sau prejudicii grave statului român ori cetăţenilor acestuia;

p) politici de securitate cibernetică - principii şi reguli generale necesar a fi îndeplinite pentru asigurarea securităţii infrastructurilor cibernetice;

q) managementul incidentului de securitate cibernetică - ansamblul proceselor ce prevăd detectarea, raportarea, analiza şi răspunsul la incidentul de securitate cibernetică;

r) risc de securitate în spaţiul cibernetic - probabilitatea ca o ameninţare să se materializeze, exploatând o vulnerabilitate specifică infrastructurii cibernetice;

s) 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, precum şi rezilienţa şi stabilitatea resurselor şi serviciilor publice sau private din spaţiul cibernetic;

t) Sistem de Control Industrial - infrastructuri şi sisteme informatice de comandă şi control utilizate pentru a automatiza procesele industriale;

u) spațiul cibernetic - mediul virtual generat de infrastructurile cibernetice, incluzând conținutul informațional, procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta;

v) vulnerabilitate în spațiul cibernetic - slăbiciune în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare.

**Art. 4** - Principiile care stau la baza prezentei legi sunt:

a) asigurarea protejării, în spațiul cibernetic, a dreptului la viață intimă, familială și privată al cetățenilor, în special a datelor cu caracter personal gestionate de către deținătorii de infrastructuri cibernetice;

b) asigurarea securității cibernetice prin responsabilizarea deținătorilor de infrastructuri cibernetice, astfel încât aceștia să evalueze capabilitățile proprii de securitate cibernetică și nivelul la care se situează;

c) creșterea capacității de reacție la incidentele cibernetice și diminuarea impactului acestora asupra resurselor și serviciilor infrastructurilor cibernetice prin impunerea de cerințe minime de securitate cibernetică și asigurarea rezilienței infrastructurilor cibernetice;

d) asigurarea nivelului de încredere necesar pentru dezvoltarea societății informaționale și a mediului de afaceri în spațiul cibernetic și asigurarea accesului egal și nediscriminatoriu al persoanelor la informații și servicii publice oferite prin intermediul infrastructurilor cibernetice;

e) asigurarea unei guvernanțe participative, democratice și eficiente a spațiului cibernetic prin cooperarea autorităților competente cu sectorul privat;

f) cooperarea la nivel național, între instituțiile cu competențe în materie și internațional, cu persoane juridice de drept public și privat, implicate în asigurarea securității cibernetice.

## CAPITOLUL II - SISTEMUL NAȚIONAL DE SECURITATE CIBERNETICĂ

**Art. 5** - (1) La nivel național activitatea de realizare a securității cibernetice se organizează și se desfășoară în mod unitar, potrivit prezentei legi.

(2) În acest scop, cooperarea în domeniu se organizează ca Sistem Național de Securitate Cibernetică, la care participă autorități și instituții publice cu atribuții și responsabilități potrivit dispozițiilor prezentei legi.

(3) În exercitarea comptetențelor, autoritățile și instituțiile publice cooperează cu sectorul privat și cu mediul academic, asociațiile profesionale și organizațiile neguvernamentale.

**Art. 6** - (1) Coordonarea la nivel strategic a activităților destinate asigurării securității cibernetice desfășurate la nivelul Sistemului Național de Securitate Cibernetică se realizează de către Consiliul Suprem de Apărare a Țării.

(2) Coordonarea activităţilor de realizare a securităţii cibernetice este asigurată, la nivel operaţional, în cadrul Sistemului Naţional de Securitate Cibernetică, de către Consiliul Operativ de Securitate Cibernetică.

(3)Coordonarea tehnică a activităţilor Consiliului Operativ de Securitate Cibernetică, este asigurată de Serviciul Român de Informaţii.

**Art. 7** - (1) Consiliul Operativ de Securitate Cibernetică este format din consilierul prezidenţial pentru probleme de securitate naţională, consilierul Prim-Ministrului pe probleme de securitate naţională, Secretarul Consiliului Suprem de Apărare a Ţării, precum şi reprezentanţi ai: Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului Comunicaţiilor şi pentru Societatea Informaţională, Serviciului Român de Informaţii, Serviciului de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază şi Oficiului Registrului Naţional al Informaţiilor Secrete de Stat.

(2) Atunci când lucrările din cadrul Consiliului Operativ de Securitate Cibernetică, privesc sau pot avea efecte asupra persoanelor prevăzute la art. 2 lit. c), la acestea participă şi reprezentantul Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii.

(3) Conducerea Consiliului Operativ de Securitate Cibernetică este asigurată de un preşedinte- consilierul prezidenţial pentru probleme de securitate naţională şi un vicepreşedinte - consilierul Prim-Ministrului pe probleme de securitate naţională.

(4) Consiliul Operativ de Securitate Cibernetică îşi desfăşoară activitatea pe baza unui Regulament de organizare şi funcţionare care se aprobă de către Consiliul Suprem de Apărare a Ţării.

(5) În cadrul lucrărilor Consiliului Operativ de Securitate Cibernetică pot prezenta puncte de vedere cu privire la problemele aflate pe agenda de lucru, reprezentanţi ai furnizorilor de servicii de securitate cibernetică, ai mediului academic, ai entităţilor de tip CERT private şi ai altor instituţii publice.

(6) În exercitarea atribuţiilor sale, Consiliul Operativ de Securitate Cibernetică analizează şi evaluează starea securităţii cibernetice, formulează şi înaintează Consiliului Suprem de Apărare a Ţării propuneri privind:

a) măsuri de armonizare a reacţiei autorităţilor competente ale statului în situaţii generate de ameninţări şi atacuri 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;

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

e) direcţii de dezvoltare sau programe de investiţii în domeniul securităţii cibernetice.

**Art. 8** - Pentru realizarea securităţii cibernetice, Consiliul Operativ de Securitate Cibernetică cooperează cu organismele de coordonare sau de conducere constituite, la

nivel național, pentru managementul situațiilor de urgență, a acțiunilor in situații de criză în domeniul ordinii publice, pentru prevenirea și combaterea terorismului și pentru apărarea națională.

**Art. 9** - Pentru asigurarea securității cibernetice, instituțiile publice din România au atribuții după cum urmează:

a) Ministerul Comunicațiilor și pentru Societatea Informațională, cu rol de autoritate de reglementare și control al implementării măsurilor privitoare la asigurarea securității cibernetice, cu excepția instituțiilor prevăzute la lit. d) și e);

b) Centrul Național de Răspuns la Incidente de Securitate Cibernetică, desemnat punct național de contact cu entitățile de tip CERT naționale și internaționale și autoritate competentă pentru coordonarea activităților în domeniul securității cibernetice a infrastructurilor cibernetice, altele decât cele menționate la lit. c), d) și e);

c) Serviciul Român de Informații, prin Centrul Național de Securitate Cibernetică, desemnat autoritate competentă pentru coordonarea activităților în domeniul securității cibernetice organizate și desfășurate la nivelul infrastructurilor cibernetice de interes național, cu excepția infrastructurilor cibernetice de interes național aflate în administrarea sau responsabilitatea celorlalte autorități prevăzute la lit. d) și e);

d) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, desemnată autoritate competentă pentru coordonarea activităților în domeniul securității cibernetice a furnizorilor de rețele publice de comunicații electronice sau furnizorilor de servicii de comunicații electronice destinate publicului;

e) Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Autoritatea Națională pentru Admninistrare și Reglementare în Comunicații, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază sunt autorități responsabile de securitate cibernetică cu rol în stabilirea de structuri și implementarea de măsuri proprii privind coordonarea și controlul activităților referitoare la asigurarea securității cibernetice pentru infrastructurile cibernetice, inclusiv infrastructurile cibernetice de interes național, aflate în domeniul lor de activitate și responsabilitate.

**Art. 10** - Cerințele minime de securitate cibernetică și politicile de securitate cibernetică pentru infrastructurile cibernetice de interes național se stabilesc de Ministerul Comunicațiilor și pentru Societatea Informațională, cu sprijinul autorităților prevăzute de art. 9 lit. b) - e), prin normele metodologice de aplicare ale prezentei legi.

**Art. 11** - (1) Autoritatea Națională pentru Administrare și Reglementare în Comunicații stabilește cerințele minime de securitate cibernetică pentru infrastructurile cibernetice, care sunt în competența sa, conform art. 9 litera d).

(2) Ministerul Comunicațiilor și pentru Societatea Informațională stabilește cerințele minime de securitate cibernetică pentru infrastructurile cibernetice, aflate în aria de competență a autorităților prevăzute la art. 9 lit. b).

(3) Fac excepție de la prevederile alin. (1) și (2) infrastructurile cibernetice de interes național.

**Art.12** - (1) Autoritățile prevăzute de art. 9 lit. b) - e) au următoarele obligații:

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

b) să asigure, în cazul instituirii unui nivel de alertă cibernetică, sprijinul pentru implementarea măsurilor aferente deținătorilor de infrastructuri cibernetice;

c) să asigure colectarea notificărilor și evaluarea datelor și informațiilor cu privire la incidente și atacuri cibernetice la adresa infrastructurilor cibernetice, aflate în domeniul lor de competență, activitate sau responsabilitate;

d) să notifice deținătorii de infrastructuri cibernetice aflate în domeniul de competență, activitate sau responsabilitate cu privire la incidente de securitate cibernetică sau vulnerabilități și atacuri cibernetice identificate la nivelul acestora;

e) să coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul infrastructurilor cibernetice aflate în domeniul lor de competență;

f) să acorde sprijin deținătorilor de infrastructuri cibernetice din zona de competență, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgență pentru remedierea efectelor incidentelor de securitate cibernetică;

g) să desfășoare activități de informare și comunicare publică;

h) să organizeze sesiuni de formare și instruire în domeniul securității cibernetice, pentru îmbunătățirea capacităților deținătorilor de infrastructuri cibernetice;

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

j) să coopereze și să-și comunice reciproc date referitoare la securitatea cibernetică, inclusiv către celelalte autorități și instituții publice sau deținători de infrastructuri cibernetice;

k) să solicite convocarea Consiliului Operativ de Securitate Cibernetică, potrivit propriilor competențe, inclusiv pentru ridicarea nivelului de alertă cibernetică.

(2) Autoritățile prevăzute la alin. (1) pot constitui structuri specializate în realizarea de audit de securitate cibernetică și pot constitui și operaționaliza structuri specializate de securitate cibernetică de tip CERT.

**Art. 13** - Autoritățile prevăzute la art. 9 lit. e), pentru infrastructurile cibernetice aflate în domeniul lor de activitate și responsabilitate, au și următoarele obligații specifice:

a) să realizeze periodic evaluări ale stării de securitate cibernetică;

b) să elaboreze politici de securitate cibernetică specifice;

c) să asigure managementul incidentelor de securitate cibernetică identificate.

**Art. 14** - (1) În procesul identificării infrastructurilor cibernetice de interes naţional, deţinătorii de infrastructuri cibernetice au obligaţia de a furniza autorităţilor de la art. 9 datele şi informaţiile necesare pentru întocmirea Catalogului ICIN.

(2) La propunerea autorităţilor prevăzute la art. 9 literele b) - e), Ministerul Comunicaţiilor şi pentru Societatea Informaţională întocmeşte Catalogul ICIN.

(3) Se exceptează de la prevederile alin. (1) şi (2) infrastructurile cibernetice de interes naţional care stochează, procesează sau transmit informaţii clasificate, deţinute, administrate sau utilizate de persoanele juridice de drept public sau privat, care se centralizează la nivelul Oficiului Registrului Naţional al Informaţiilor Secrete de Stat.

(4) Infrastructurile cibernetice de interes naţional prevăzute la alin. (3) se comunică Centrului Naţional de Securitate Cibernetică, cu excepţia celor constituite la nivelul Autorităţilor Desemnate de Securitate, care deţin Structuri Interne INFOSEC acreditate potrivit prevederilor legale în vigoare.

(5) Deţinătorii de infrastructuri cibernetice de interes naţional prevăzuţi la art. 9 litera c) trebuie să notifice Centrul Naţional de Securitate Cibernetică, în termen de 10 zile, cu privire la orice modificare intervenită în statutul juridic al infrastructurilor cibernetice de interes naţional, respectiv în configuraţia acestora.

(6) Informaţiile necesare pentru întocmirea Catalogului ICIN trebuie să cuprindă următoarele:

a) descrierea generală a infrastructurilor cibernetice de interes naţional;

b) rolul şi funcţionalităţile asigurate de infrastructurile cibernetice de interes naţional;

c) arhitectura infrastructurilor cibernetice de interes naţional;

d) tipuri şi număr de utilizatori;

e) fluxuri informaţionale susţinute, precum şi dinamica datelor stocate/prelucrate, capacitatea de stocare/prelucrare.

**Art. 15** - Pentru derularea procesului de identificare a infrastructurilor cibernetice de interes naţional, deţinătorii de infrastructuri cibernetice, sub coordonarea autorităţilor competente, vor evalua măsura în care infrastructurile cibernetice proprii se încadrează în cel puţin una dintre următoarele categorii de potenţiale infrastructuri cibernetice de interes naţional:

a) infrastructuri cibernetice destinate susţinerii actului de guvernare;

b) infrastructuri cibernetice destinate susţinerii administraţiei publice;

c) infrastructuri cibernetice destinate susţinerii serviciilor publice;

d) infrastructuri cibernetice prin intermediul cărora se asigură accesul cetăţenilor şi a mediului de afaceri la servicii publice;

e) infrastructuri cibernetice destinate susţinerii funcţiilor de apărare, ordine publică, justiţie şi securitate naţională;

f) infrastructuri cibernetice destinate tranzacţiilor economice şi financiar-bancare;

g) infrastructuri cibernetice de tip Sistem de Control Industrial;

h) infrastructuri cibernetice care asigură supraveghere, sesizare, avertizare şi alertă;

i) infrastructuri cibernetice care asigură servicii de securitate cibernetică;

j) infrastructuri cibernetice care asigură componenta naţională destinată cooperării în cadrul NATO, UE sau al organizaţiilor la care România este parte;

k) infrastructuri cibernetice pentru navigaţie, radiolocaţie şi identificare;

l) infrastructuri cibernetice care susţin transmisia sau retransmisia serviciilor de programe de televiziune sau radiodifuziune;

m) infrastructuri cibernetice utilizate de către furnizorii de servicii poştale.

**Art. 16** - (1) Evaluarea potenţialului impact asupra securităţii infrastructurilor cibernetice prin compromiterea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii sau a non-repudierii datelor, resurselor şi serviciilor se realizează pe baza următoarelor criterii:

a) prejudiciul adus intereselor statului român;

b) prejudiciul produs în planul securităţii naţionale;

c) afectarea vieţii şi siguranţei cetăţeanului;

d) afectarea încrederii utilizatorilor în serviciile oferite;

e) prejudiciul material sau financiar;

f) întreruperea furnizării serviciului afectat;

g) utilizatorii afectaţi raportat la spaţiul geografic - internaţional, naţional, regional, local;

h) afectarea relaţiilor internaţionale în care România este angrenată;

i) afectarea infrastructurii critice de interes naţional în cazul în care infrastructura cibernetică este parte componentă a acesteia sau în interdependenţă cu aceasta;

j) interdependenţa cu alte infrastructuri cibernetice.

(2) În cadrul analizei de interdependenţă, autorităţile competente pot colabora şi cu alte autorităţi sau persoane juridice în condiţiile în care infrastructurile cibernetice de interes naţional ar putea genera efecte în domeniul de competenţă al acestora.

## CAPITOLUL III - ASIGURAREA SECURITĂŢII CIBERNETICE

**Art. 17** - (1) Sistemul Naţional de Alertă Cibernetică este un ansamblu organizat de măsuri tehnice şi procedurale destinate prevenirii şi contracarării activităţilor de natură să afecteze securitatea cibernetică la nivel naţional.

(2) În cadrul Sistemului Naţional de Alertă Cibernetică, stările de ameninţare reflectă gradul de risc pentru securitatea cibernetică şi sunt identificate prin niveluri de alertă cibernetică. Acestea pot fi instituite pentru întreg teritoriul naţional, pentru o zonă geografică delimitată, pentru un anumit domeniu de activitate sau pentru una sau mai multe persoane juridice de drept public sau privat.

(3) Instituirea nivelurilor de alertă cibernetică, precum şi trecerea de la un nivel la altul se aprobă de către Consiliul Suprem de Apărare a Ţării, la propunerea Consiliul Operativ de Securitate Cibernetică.-

(4) Deţinătorii de infrastructuri cibernetice au obligaţia să sprijine autorităţile competente pentru implementarea măsurilor corespunzătoare fiecărui nivel de alertă cibernetică.

(5) Personale juridice de drept public sau privat deţinători de infrastructuri cibernetice de interes naţional elaborează planuri de acţiune proprii, corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligaţia să le pună în aplicare la instituirea unui nivel de alertă cibernetică.

(6) La modificarea nivelului de alertă cibernetică deţinătorii de infrastructuri cibernetice de interes naţional au obligaţia informării deîndată a Centrului Naţional de Securitate Cibernetică cu privire la gradul de afectare a infrastructurii cibernetice şi măsurile preconizate.

**Art. 18** - (1) Deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) adoptă măsuri organizatorice şi tehnice pentru:

a) evaluarea infrastructurilor cibernetice deţinute în vederea susţinerii demersurilor de întocmire a Catalogului ICIN;

b) elaborarea şi implementarea de politici şi planuri de securitate cibernetică, cu respectarea cerinţelor minime de securitate;

c) managementul incidentelor de securitate cibernetică;

d) prevenirea accesului neautorizat la infrastructurilor cibernetice;

e) garantarea diseminării datelor deţinute la nivelul infrastructurilor cibernetice exclusiv persoanelor autorizate să cunoască conţinutul acestora.

(2) Faţă de cele prevăzute la alin. (1), deţinătorii de infrastructuri cibernetice de interes naţional adoptă, suplimentar, măsuri organizatorice şi tehnice pentru:

a) implementarea unui sistem de management al riscului;

b) elaborarea de planuri de acţiune pe niveluri de alertă cibernetică;

c) auditarea nivelului de securitate cibernetică a infrastructurilor cibernetice de interes naţional.

**Art. 19** - Deţinătorii de infrastructuri cibernetice de la art. 2, lit. a) - c) au următoarele drepturi:

a) să fie informaţi cu privire la orice măsură de securitate cibernetică adoptată de către autorităţile competente care îi vizează;

b) să primească notificări din partea autorităţilor competente cu privire la identificarea unor incidente de securitate cibernetică care afectează sau pot afecta infrastructura cibernetică deţinută;

c) să solicite asistenţă de specialitate autorităţilor competente potrivit prezentei legi, pentru asigurarea securităţii cibernetice în domeniul lor de activitate;

d) să solicite sprijinul autorităţilor competente pentru realizarea de auditări de securitate, sau să utilizeze furnizori de servicii de securitate cibernetică;

e) să decidă în ceea ce priveşte modalitatea de elaborare a politicilor proprii de securitate cibernetică şi implementare a măsurilor necesare în vederea respectării cerinţelor minime de securitate cibernetică;

f) să aleagă modalitatea de management al incidentelor de securitate cibernetică, prin utilizarea resurselor proprii şi a resurselor externe, prin contractarea unor servicii de securitate cibernetică sau solicitarea sprijinului autorităţilor competente.

**Art. 20** - (1) Deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2 lit. a) - c) au următoarele obligaţii:

a) să asigure implementarea cerinţelor minime de securitate cibernetică;

b) să notifice deîndată autoritatea competentă cu privire la incidentele de securitate cibernetică identificate;

c) să se asigure că datele şi/sau informaţiile referitoare la configurarea şi protecţia infrastructurilor cibernetice sunt diseminate exclusiv persoanelor autorizate să le cunoască;

d) să nu permită accesul la datele de conţinut din infrastructurile cibernetice deţinute sau aflate în competenţă, în lipsa unei înştiinţări scrise din partea autorităţilor abilitate, privind existenţa unei autorizaţii emise de judecător, în condiţiile legii;

e) să gestioneze incidentele de securitate cibernetică;

f) să nu afecteze, prin acţiunile proprii, securitatea altor infrastructuri cibernetice.

(2) Faţă de cele prevăzute la alin. (1), deţinătorii de infrastructuri cibernetice de interes naţional au, suplimentar, următoarele obligaţii:

a) să efectueze auditări de securitate cibernetică, anual sau când este necesar;

b) să constituie structuri sau să desemneze persoane responsabile privind coordonarea activităţilor de securitate cibernetică;

c) să transmită autorităţilor competente copie după rapoartele de audit de securitate cibernetică şi date privind evoluţiile în domeniul securităţii cibernetice la nivelul infrastructurilor cibernetice deţinute, trimestrial şi ori de câte ori li se solicită;

d) să elaboreze şi să transmită autorităţii competente planuri de acţiune corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligaţia să le pună în aplicare la instituirea unui nivel de alertă cibernetică;

e) să transmită autorităţilor competente date referitoare la rezultatele măsurilor de contracarare a incidentelor de securitate cibernetică aplicate.

**Art. 21** - (1) Furnizorii de servicii de comunicaţii electronice destinate publicului au obligaţia de a-şi notifica utilizatorii şi abonaţii de îndată ce au fost sesizaţi de autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care au fost sesizaţi de autorităţile competente potrivit prezentei legi, cu privire la situaţiile în care

sistemele informatice utilizate de aceştia au fost implicate în atacuri cibernetice şi de a recomanda măsurile necesare în vederea restabilirii condiţiilor normale de funcţionare.

(2) Notificarea prevăzută la alin. (1) se realizează în scris, prin mijloace electronice, sau prin orice altă modalitate stabilită prin contractul de furnizare de servicii.

**Art. 22** - (1) Furnizorii de servicii de securitate cibernetică ce desfăşoară activităţi pe teritoriul României au obligaţia să notifice autorităţile competente, deîndată dar nu mai târziu de 24 de ore, cu privire la identificarea unor ameninţări sau vulnerabilităţi critice a căror manifestare poate afecta infrastructura cibernetică a deţinătorului sau a unor terţi.

(2) Notificarea prevăzută la alin. (1) se realizează în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord.

(3) Furnizorii de servicii de securitate cibernetică care realizează audit de securitate pentru infrastructuri cibernetice de interes naţional au obligaţia de a se înregistra la Ministerul Comunicaţiilor şi pentru Societatea Informaţională, potrivit normelor aprobate prin ordin al ministrului, care stabilesc condiţiile pentru înregistrarea şi radierea acestora din Registrul Furnizorilor de Audit de Securitate Cibernetică.

**Art. 23** - (1) Furnizorii de servicii de găzduire internet care desfăşoară activităţi pe teritoriul României au obligaţia să acorde sprijin autorităţilor competente, respectiv organelor de urmărire penală, pentru punerea în aplicare, potrivit legii, a oricărui act de autorizare a restrângerii temporare a exerciţiului drepturilor şi libertăţilor persoanelor, emis de judecător.

(2) Furnizorii de servicii de găzduire internet au obligaţia de a înregistra şi stoca date de jurnalizare a activităţilor din sistemele informatice deţinute care fac obiectul actului de autorizare de la alin. (1), pe toată perioada de valabilitate a acestuia.

(3) Persoanele care sunt chemate să acorde spriijn tehnic la punerea în executare a actelor de autorizare, precum şi persoanele care iau la cunoştinţă despre aceasta au obligaţia să păstreze secretul operaţiunii efectuate, sub sancţiunea legii penale.

## CAPITOLUL IV - GESTIONAREA INCIDENTELOR DE SECURITATE CIBERNETICĂ

**Art. 24** - (1) Notificarea incidentelor de securitate cibernetică se transmite în modalitatea stabilită de autoritatea competentă şi trebuie să conţină, în mod obligatoriu, următoarele elemente:

a) elementele de identificare ale infrastructurii cibernetice afectate;

b) descrierea incidentului;

c) perioada de desfăşurare a incidentului;

d) impactul incidentului.

(2) Pentru gestionarea incidentelor de securitate cibernetică, deţinătorii de infrastructuri cibernetice pot solicita sprijinul furnizorilor de servicii de securitate cibernetică sau al autorităţilor prevăzute de art. 9 lit. b) - e), potrivit competenţelor acestora, cărora le pot pune la dispoziţie date tehnice referitoare la incidentele şi

atacurile cibernetice pe care le gestionează, cu asigurarea anonimizării datelor cu caracter personal deţinute.

(3) Datele tehnice transmise în condiţiile prevăzute la alin. (2) nu vor conţine:

a) informaţii clasificate;

b) date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate.

**Art. 25** - Autorităţile competente au obligaţia de a stoca şi a păstra pe un termen de 5 ani notificările primite cu privire la incidentele de securitate cibernetică şi atacurile cibernetice.

**Art. 26** - La primirea unei notificări sau în cazul identificării unui incident de securitate cibernetică sau a unui atac cibernetic, autoritatea competentă are obligaţia:

a) să coordoneze activitatea de management al incidentelor de securitate cibernetică şi să acorde sprijin deţinătorilor de infrastructuri cibernetice din zona sa de competenţă pentru adoptarea de măsuri reactive de primă urgenţă pentru asigurarea integrităţii datelor şi remedierea efectelor incidentelor de securitate;

b) să notifice deţinătorii de infrastructuri cibernetice din domeniul de competenţă şi celelalte autorităţi competente, dacă se constată că pot fi afectate de incidentul de securitate cibernetică.

**Art. 27** - (1) În situaţia în care în cadrul activităţilor de management al incidentului de securitate cibernetică sunt identificate informaţii sau fapte care pot indica săvârşirea unei infracţiuni care vizează infrastructuri cibernetice este obligatorie sesizarea organelor judiciare.

(2) Autoritatea competentă are obligaţia să sprijine activităţile derulate de organele de cercetare penală pentru investigarea infracţiunilor ce vizează sistemele informatice aparţinând unor infrastructuri cibernetice aflate în competenţa acesteia.

**Art. 28** - În baza notificărilor primite şi a rezultatelor propriilor activităţi de identificare a ameninţărilor, riscurilor şi vulnerabilităţilor la adresa securităţii cibernetice, autorităţile competente emit înştiinţări adresate, după caz, publicului, altor autorităţi competente sau deţinătorilor de infrastructuri cibernetice aflaţi în aria de competenţă, cu privire la evenimente sau stări de fapt care afectează securitatea cibernetică a României.

## CAPITOLUL V - APĂRAREA CIBERNETICĂ

**Art. 29** - (1) Apărarea cibernetică cuprinde ansamblul de măsuri şi activităţi adoptate şi desfăşurate de autorităţile cu atribuţii în domeniul apărării ţării şi securităţii naţionale pentru protejarea infrastructurilor cibernetice destinate apărării naţionale şi a infrastructurilor cibernetice naţionale care susţin activităţile NATO şi UE.

(2) Infrastructurile cibernetice destinate apărării naţionale şi măsurile privind apărarea cibernetică a acestora se stabilesc la intrarea în vigoare a prezentei legi şi se actualizează periodic prin hotărâre a Consiliului Suprem de Apărare a Ţării.

**Art. 30** - (1) Activităţile prevăzute la art. 29 alin. (1) se planifică şi se desfăşoară de autorităţile cu atribuţii în domeniul apărării ţării şi securităţii naţionale în strânsă legătură cu activităţile privind apărarea naţională şi planificarea apărării, conform legii şi potrivit obligaţiilor asumate de România la nivel internaţional.

(2) Autorităţile şi instituţiile publice au obligaţia de a identifica şi implementa, în condiţiile legii şi în termenul prevăzut de normele metodologice de aplicare a prezentei legi, măsuri de apărare cibernetică şi răspund de executarea acestora, fiecare în domeniul său de activitate.

**Art. 31** - (1) Ministerul Apărării Naţionale împreună cu celelalte autorităţi şi instituţii publice cu atribuţii în domeniul apărării ţării şi securităţii naţionale asigură, din timp de pace, integrarea într-o concepţie unitară a activităţilor privind apărarea cibernetică desfăşurate de forţele armate participante la acţiunile de apărare a ţării în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război.

(2) Conducerea acţiunilor de apărare cibernetică în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război se realizează de către Centrul Naţional Militar de Comandă în cooperare cu Consiliul Operativ de Securitate Cibernetică.

## CAPITOLUL VI - CONTROL ŞI SANCŢIUNI

**Art. 32** - (1) Autorităţile prevăzute la art. 9, lit. a), d) şi e) au atribuţii de control asupra aplicării prevederilor prezentei legi de către deţinătorii infrastructurilor cibernetice aflate în competenţă sau responsabilitate.

(2) În vederea exercitării atribuţiilor, conducătorii autorităţilor competente desemnează persoanele abilitate să desfăşoare activităţi de control, în baza şi în limitele împuternicirii aprobate.

**Art. 33** - (1) Nerespectarea prevederilor prezentei legi atrage răspunderea contravenţională, potrivit dispoziţiilor legale în vigoare.

(2) Constatarea contravenţiilor şi aplicarea sancţiunilor se realizează potrivit prevederilor Cap. II 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.

(3) Procesul-verbal de contravenţie poate fi contestat în termen de 30 de zile de la data luării la cunoştinţă, conform Cap. IV 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.

(4) Deţinătorii de infrastructuri cibernetice de la art. 2, lit. a) - c) şi e) pot să conteste actele şi măsurile luate de către autorităţile competente, care sunt susceptibile de a le prejudicia drepturile sau interesele legitime.

**Art. 34** - (1) La nivelul instituţiilor publice, aşa cum sunt definite în Legea nr. 500/2002 privind finanţele publice, cu modificările şi completările ulterioare, fondurile necesare organizării şi desfăşurării activităţii în condiţiile prezentei legi se asigură de la bugetul de stat, din venituri proprii sau din alte surse legal constituite, anual, potrivit legii.

(2) Pentru buna desfăşurare a activităţilor specifice pot fi utilizate şi fonduri provenite din credite externe contractate sau garantate de stat şi ale căror rambursare, dobânzi şi alte costuri se asigură din fonduri publice, precum şi din fonduri externe sau europene.

**Art. 35** - Constituie contravenţii următoarele fapte dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate, potrivit legii, infracţiuni:

a) nerespectarea de către deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) a obligaţiilor prevăzute la art. 20 alin. (1), lit. a) şi c);

b) încălcarea de către deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) a obligaţiilor prevăzute la art. 20 alin.(1), lit. d), e) şi f);

c) nerespectarea de către deţinătorii de ICIN a obligaţiei prevăzute la art. 18 alin. (2), precum şi a obligaţiilor prevăzute la art. 20, alin.(2), lit. a) - e);

d) nerespectarea de către furnizorii de servicii de comunicaţii electronice destinate publicului a obligaţiei prevăzute la art. 21;

e) încălcarea de către furnizorii de servicii de securitate cibernetică ce îşi desfăşoară activitatea pe teritoriul României a obligaţiei prevăzute la art. 22, alin. (1);

f) nerespectarea de către deţinătorii de infrastructuri cibernetice a cerinţelor prevăzute la art. 20 alin. (1) lit. b) în condiţiile stabilite de art. 24 alin. (1).

**Art. 36** - Contravenţiile prevăzute la art. **35** se sancţionează astfel:

a) cu amendă de la 500 lei la 5.000 lei, pentru săvârşirea contravenţiilor prevăzute la art. 35 lit. a), e) şi f);

b) cu amendă de la 1.000 lei la 10.000 lei, pentru săvârşirea contravenţiilor prevăzute la art. 35, lit. b) - d).

## CAPITOLUL VII - DISPOZIŢII FINALE

**Art. 37** - (1) În termen de 90 zile de la publicarea prezentei legi în Monitorul Oficial al României, Partea I, Ministerul Comunicaţiilor şi pentru Societatea Informaţională cu sprijinul autorităţilor prevăzute la art. 8 lit. b) - e) iniţiază şi supune aprobării Guvernului organizarea şi funcţionarea Sistemului Naţional de Alertă Cibernetică.

(2) În termen de 90 zile de la publicarea prezentei legi în Monitorul Oficial al României, Partea I, Ministerul Comunicațiilor și pentru Societatea Informațională supune aprobării Guvernului Programul național destinat managementului riscului în domeniul securității cibernetice.

(3) Normele metodologice de aplicare a prezentei legi se elaborează de către Ministerul Comunicațiilor și pentru Societatea Informațională și se supun aprobării Guvernului în termen de 90 zile de la publicarea acesteia în Monitorul Oficial al României, Partea I.

(4) Catalogul infrastructurilor cibernetice de interes național prevăzut la art.14 alin. (2) se aprobă prin hotărâre a Guvernului în termen de 6 luni de la publicarea prezentei legi în Monitorul Oficial al României, Partea I și se va revizui periodic.

(5) Cerințele minime de securitate prevăzute la art.10, alin.1 se aprobă prin decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații, în termen de 90 de zile de la publicarea prezentei legi în Monitorul Oficial al României, Partea I.