

LEGE PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI

CAPITOLUL I - DISPOZIȚII GENERALE

Art. 1 - (1) Legea stabilește cadrul juridic privind organizarea și desfășurarea activităților din domeniul securității cibernetice a României și asigurarea protecției drepturilor și libertăților fundamentale ale cetățenilor în spațiul cibernetic.

(2) Securitatea cibernetică este componentă a securității naționale a României și se realizează prin adoptarea și implementarea de politici și măsuri de securitate la nivelul deținătorilor de infrastructuri cibernetice în scopul cunoașterii, prevenirii și contracarării riscurilor și amenințărilor în spațiul cibernetic.

Art. 2 - Prezenta lege se aplică:

a) autorităților și instituțiilor publice, persoanelor juridice deținătoare de infrastructuri cibernetice care susțin servicii publice sau de interes public, ori servicii ale societății informaționale, a căror afectare aduce atingere securității naționale sau prejudicii grave statului român ori cetățenilor acestuia;

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

c) furnizorilor de rețele publice de comunicații electronice și furnizorilor de servicii de comunicații electronice destinate publicului;

d) furnizorilor de servicii de găzduire internet;

e) furnizorilor de servicii de securitate cibernetică.

Art. 3 - În sensul prezentei legi, termenii și expresiile de mai jos au următoarea semnificație:

a) amenințare cibernetică - circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice;

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

c) apărare cibernetică - acțiuni desfășurate în spațiul cibernetic în scopul protecției, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice destinate apărării naționale;

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

e) audit de securitate cibernetică - activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecție implementate la nivelul unei infrastructuri cibernetice, în vederea identificării disfuncțiilor și vulnerabilităților și a furnizării unor soluții de remediere a acestora;

f) Catalog ICIN - registru de evidență a infrastructurilor cibernetice de interes național;



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

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

i) date tehnice - descriere generală a infrastructurii cibernetice, rolul și funcționalitățile asigurate de aceasta, arhitectura, tipuri și număr de utilizatori, fluxuri informaționale susținute, descrierea capacității de stocare/prelucrare, fișiere de jurnalizare a evenimentelor ce au loc în sistemele de securitate software și hardware, sistemele de operare și aplicațiile software;

j) deținători 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 desfășoară activități pe teritoriul României, care pune la dispoziție infrastructuri cibernetice, fizice sau virtuale, pentru derularea de activități și servicii ale societății informaționale;

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

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

n) infrastructuri cibernetice - infrastructuri de tehnologia informației, constând în sisteme informatice, aplicații aferente, rețele de comunicații electronice;

o) infrastructuri cibernetice de interes național - infrastructuri cibernetice deținute de persoane juridice de drept privat, care susțin servicii publice sau de interes public ori servicii ale societății informaționale, sau infrastructuri cibernetice deținute de autorități și instituții publice, a căror afectare aduce atingere securității naționale, sau prejudicii grave statului român ori cetățenilor acestuia;

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

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

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

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

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



u) spațiul cibernetic - mediul virtual generat de infrastructurile ciberneticе, 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 ciberneticе 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 protecției, 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 ciberneticе;

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

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

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 ciberneticе;

e) asigurarea unei guvernante 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 ciberneticе.

CAPITOLUL II - SISTEMUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Art. 5 - (1) La nivel național activitatea de realizare a securității ciberneticе 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 competențelor, 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 ciberneticе desfășurate la nivelul Sistemului Național de Securitate Cibernetică se realizează de către Consiliul Suprem de Apărare a Țării.



(2) Coordonarea activităților de realizare a securității cibernetice este asigurată, la nivel operațional, în cadrul Sistemului Național de Securitate Cibernetică, de către Consiliul Operativ de Securitate Cibernetică.

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

Art. 7 - (1) Consiliul Operativ de Securitate Cibernetică este format din consilierul prezidențial pentru probleme de securitate națională, consilierul Prim-Ministrului pe probleme de securitate națională, Secretarul Consiliului Suprem de Apărare a Țării, precum și reprezentanți ai: Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului Comunicațiilor și pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază și Oficiului Registrului Național al Informațiilor 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 și reprezentantul Autorității Naționale pentru Administrare și Reglementare în Comunicații.

(3) Conducerea Consiliului Operativ de Securitate Cibernetică este asigurată de un președinte- consilierul prezidențial pentru probleme de securitate națională și un vicepreședinte - consilierul Prim-Ministrului pe probleme de securitate națională.

(4) Consiliul Operativ de Securitate Cibernetică își desfășoară activitatea pe baza unui Regulament de organizare și funcționare care se aprobă de către Consiliul Suprem de Apărare a Țării.

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

(6) În exercitarea atribuțiilor sale, Consiliul Operativ de Securitate Cibernetică analizează și evaluează starea securității cibernetice, formulează și înaintează Consiliului Suprem de Apărare a Țării propuneri privind:

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

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

c) modalitatea de răspuns la solicitările de asistență adresate României din partea altor state sau organizații și organisme internaționale;

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

e) direcții de dezvoltare sau programe de investiții în domeniul securității cibernetice.

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

nivel național, pentru managementul situațiilor de urgență, a acțiunilor în 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 Administrare 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 național, deținătorii de infrastructuri cibernetice au obligația de a furniza autorităților de la art. 9 datele și informațiile necesare pentru întocmirea Catalogului ICIN.

(2) La propunerea autorităților prevăzute la art. 9 literele b) - e), Ministerul Comunicațiilor și pentru Societatea Informațională întocmește Catalogul ICIN.

(3) Se exceptează de la prevederile alin. (1) și (2) infrastructurile cibernetice de interes național care stochează, procesează sau transmit informații clasificate, deținute, administrate sau utilizate de persoanele juridice de drept public sau privat, care se centralizează la nivelul Oficiului Registrului Național al Informațiilor Secrete de Stat.

(4) Infrastructurile cibernetice de interes național prevăzute la alin. (3) se comunică Centrului Național de Securitate Cibernetică, cu excepția celor constituite la nivelul Autorităților Desemnate de Securitate, care dețin Structuri Interne INFOSEC acreditate potrivit prevederilor legale în vigoare.

(5) Deținătorii de infrastructuri cibernetice de interes național prevăzuți la art. 9 litera c) trebuie să notifice Centrul Național de Securitate Cibernetică, în termen de 10 zile, cu privire la orice modificare intervenită în statutul juridic al infrastructurilor cibernetice de interes național, respectiv în configurația acestora.

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

- a) descrierea generală a infrastructurilor cibernetice de interes național;
- b) rolul și funcționalitățile asigurate de infrastructurile cibernetice de interes național;
- c) arhitectura infrastructurilor cibernetice de interes național;
- d) tipuri și număr de utilizatori;
- e) fluxuri informaționale susținute, precum și dinamica datelor stocate/prelucrate, capacitatea de stocare/prelucrare.

Art. 15 - Pentru derularea procesului de identificare a infrastructurilor cibernetice de interes național, deținătorii de infrastructuri cibernetice, sub coordonarea autorităților competente, vor evalua măsura în care infrastructurile cibernetice proprii se încadrează în cel puțin una dintre următoarele categorii de potențiale infrastructuri cibernetice de interes național:

- a) infrastructuri cibernetice destinate susținerii actului de guvernare;
- b) infrastructuri cibernetice destinate susținerii administrației publice;
- c) infrastructuri cibernetice destinate susținerii serviciilor publice;
- d) infrastructuri cibernetice prin intermediul cărora se asigură accesul cetățenilor și a mediului de afaceri la servicii publice;
- e) infrastructuri cibernetice destinate susținerii funcțiilor de apărare, ordine publică, justiție și securitate națională;
- f) infrastructuri cibernetice destinate tranzacțiilor economice și financiar-bancare;
- g) infrastructuri cibernetice de tip Sistem de Control Industrial;



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

i) infrastructuri cibernetice care asigură servicii de securitate cibernetică;

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

k) infrastructuri cibernetice pentru navigație, radiolocație și identificare;

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

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

Art. 16 - (1) Evaluarea potențialului impact asupra securității infrastructurilor cibernetice prin compromiterea confidențialității, integrității, disponibilității, autenticității sau a non-repudierii datelor, resurselor și serviciilor se realizează pe baza următoarelor criterii:

a) prejudiciul adus intereselor statului român;

b) prejudiciul produs în planul securității naționale;

c) afectarea vieții și siguranței cetățeanului;

d) afectarea încrederii utilizatorilor în serviciile oferite;

e) prejudiciul material sau financiar;

f) întreruperea furnizării serviciului afectat;

g) utilizatorii afectați raportat la spațiul geografic - internațional, național, regional, local;

h) afectarea relațiilor internaționale în care România este angrenată;

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

j) interdependența cu alte infrastructuri cibernetice.

(2) În cadrul analizei de interdependență, autoritățile competente pot colabora și cu alte autorități sau persoane juridice în condițiile în care infrastructurile cibernetice de interes național ar putea genera efecte în domeniul de competență al acestora.

CAPITOLUL III - ASIGURAREA SECURITĂȚII CIBERNETICE

Art. 17 - (1) Sistemul Național de Alertă Cibernetică este un ansamblu organizat de măsuri tehnice și procedurale destinate prevenirii și contracarării activităților de natură să afecteze securitatea cibernetică la nivel național.

(2) În cadrul Sistemului Național de Alertă Cibernetică, stările de amenințare reflectă gradul de risc pentru securitatea cibernetică și sunt identificate prin niveluri de alertă cibernetică. Acestea pot fi instituite pentru întreg teritoriul național, 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 și trecerea de la un nivel la altul se aprobă de către Consiliul Suprem de Apărare a Țării, la propunerea Consiliului Operativ de Securitate Cibernetică.-

(4) Deținătorii de infrastructuri cibernetică au obligația să sprijine autoritățile competente pentru implementarea măsurilor corespunzătoare fiecărui nivel de alertă cibernetică.

(5) Personale juridice de drept public sau privat deținători de infrastructuri cibernetică de interes național elaborează planuri de acțiune proprii, corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligația să le pună în aplicare la instituirea unui nivel de alertă cibernetică.

(6) La modificarea nivelului de alertă cibernetică deținătorii de infrastructuri cibernetică de interes național au obligația informării de îndată a Centrului Național de Securitate Cibernetică cu privire la gradul de afectare a infrastructurii cibernetică și măsurile preconizate.

Art. 18 - (1) Deținătorii de infrastructuri cibernetică prevăzuți la art. 2, lit. a) - c) adoptă măsuri organizatorice și tehnice pentru:

a) evaluarea infrastructurilor cibernetică deținute în vederea susținerii demersurilor de întocmire a Catalogului ICIN;

b) elaborarea și implementarea de politici și planuri de securitate cibernetică, cu respectarea cerințelor minime de securitate;

c) managementul incidentelor de securitate cibernetică;

d) prevenirea accesului neautorizat la infrastructurilor cibernetică;

e) garantarea diseminării datelor deținute la nivelul infrastructurilor cibernetică exclusiv persoanelor autorizate să cunoască conținutul acestora.

(2) Față de cele prevăzute la alin. (1), deținătorii de infrastructuri cibernetică de interes național adoptă, suplimentar, măsuri organizatorice și tehnice pentru:

a) implementarea unui sistem de management al riscului;

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

c) auditarea nivelului de securitate cibernetică a infrastructurilor cibernetică de interes național.

Art. 19 - Deținătorii de infrastructuri cibernetică de la art. 2, lit. a) - c) au următoarele drepturi:

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

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

c) să solicite asistență de specialitate autorităților competente potrivit prezentei legi, pentru asigurarea securității cibernetică în domeniul lor de activitate;



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

e) să decidă în ceea ce privește modalitatea de elaborare a politicilor proprii de securitate cibernetică și implementare a măsurilor necesare în vederea respectării cerințelor minime de securitate cibernetică;

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

Art. 20 - (1) Deținătorii de infrastructuri cibernetică prevăzuți la art. 2 lit. a) - c) au următoarele obligații:

a) să asigure implementarea cerințelor minime de securitate cibernetică;

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

c) să se asigure că datele și/sau informațiile referitoare la configurarea și protecția infrastructurilor cibernetică sunt diseminate exclusiv persoanelor autorizate să le cunoască;

d) să nu permită accesul la datele de conținut din infrastructurile cibernetică deținute sau aflate în competență, în lipsa unei înștiințări scrise din partea autorităților abilitate, privind existența unei autorizații emise de judecător, în condițiile legii;

e) să gestioneze incidentele de securitate cibernetică;

f) să nu afecteze, prin acțiunile proprii, securitatea altor infrastructuri cibernetică.

(2) Față de cele prevăzute la alin. (1), deținătorii de infrastructuri cibernetică de interes național au, suplimentar, următoarele obligații:

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

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

c) să transmită autorităților competente copie după rapoartele de audit de securitate cibernetică și date privind evoluțiile în domeniul securității cibernetică la nivelul infrastructurilor cibernetică deținute, trimestrial și ori de câte ori li se solicită;

d) să elaboreze și să transmită autorității competente planuri de acțiune corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligația să le pună în aplicare la instituirea unui nivel de alertă cibernetică;

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

Art. 21 - (1) Furnizorii de servicii de comunicații electronice destinate publicului au obligația de a-și notifica utilizatorii și abonații de îndată ce au fost sesizați de autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care au fost sesizați de autoritățile competente potrivit prezentei legi, cu privire la situațiile în care



sistemele informatice utilizate de aceștia au fost implicate în atacuri cibernetice și de a recomanda măsurile necesare în vederea restabilirii condițiilor normale de funcționare.

(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 desfășoară activități pe teritoriul României au obligația să notifice autoritățile competente, de îndată dar nu mai târziu de 24 de ore, cu privire la identificarea unor amenințări sau vulnerabilități critice a căror manifestare poate afecta infrastructura cibernetică a deținătorului sau a unor terți.

(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 național au obligația de a se înregistra la Ministerul Comunicațiilor și pentru Societatea Informațională, potrivit normelor aprobate prin ordin al ministrului, care stabilesc condițiile pentru înregistrarea și radierea acestora din Registrul Furnizorilor de Audit de Securitate Cibernetică.

Art. 23 - (1) Furnizorii de servicii de găzduire internet care desfășoară activități pe teritoriul României au obligația să acorde sprijin autorităților competente, respectiv organelor de urmărire penală, pentru punerea în aplicare, potrivit legii, a oricărui act de autorizare a restrângerii temporare a exercițiului drepturilor și libertăților persoanelor, emis de judecător.

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

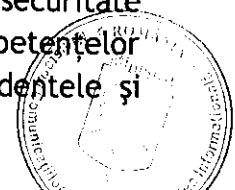
(3) Persoanele care sunt chemate să acorde sprijin tehnic la punerea în executare a actelor de autorizare, precum și persoanele care iau la cunoștință despre aceasta au obligația să păstreze secretul operațiunii efectuate, sub sancțiunea legii penale.

CAPITOLUL IV - GESTIONAREA INCIDENTELOR DE SECURITATE CIBERNETICĂ

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

- a) elementele de identificare ale infrastructurii cibernetice afectate;
- b) descrierea incidentului;
- c) perioada de desfășurare a incidentului;
- d) impactul incidentului.

(2) Pentru gestionarea incidentelor de securitate cibernetică, deținătorii de infrastructuri cibernetice pot solicita sprijinul furnizorilor de servicii de securitate cibernetică sau al autorităților prevăzute de art. 9 lit. b) - e), potrivit competențelor acestora, cărora le pot pune la dispoziție date tehnice referitoare la incidente și



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

(3) Datele tehnice transmise în condițiile prevăzute la alin. (2) nu vor conține:

a) informații clasificate;

b) date care pot aduce atingere drepturilor și libertăților cetățenești ori intereselor legitime ale unor terțe entități implicate.

Art. 25 - Autoritățile competente au obligația de a stoca și a păstra pe un termen de 5 ani notificările primite cu privire la incidentele de securitate cibernetică și 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 obligația:

a) să coordoneze activitatea de management al incidentelor de securitate cibernetică și să acorde sprijin deținătorilor de infrastructuri cibernetice din zona sa de competență pentru adoptarea de măsuri reactive de primă urgență pentru asigurarea integrității datelor și remedierea efectelor incidentelor de securitate;

b) să notifice deținătorii de infrastructuri cibernetice din domeniul de competență și celelalte autorități competente, dacă se constată că pot fi afectate de incidentul de securitate cibernetică.

Art. 27 - (1) În situația în care în cadrul activităților de management al incidentului de securitate cibernetică sunt identificate informații sau fapte care pot indica săvârșirea unei infracțiuni care vizează infrastructuri cibernetice este obligatorie sesizarea organelor judiciare.

(2) Autoritatea competentă are obligația să sprijine activitățile derulate de organele de cercetare penală pentru investigarea infracțiunilor ce vizează sistemele informatice aparținând unor infrastructuri cibernetice aflate în competența acesteia.

Art. 28 - În baza notificărilor primite și a rezultatelor propriilor activități de identificare a amenințărilor, riscurilor și vulnerabilităților la adresa securității cibernetice, autoritățile competente emit înștiințări adresate, după caz, publicului, altor autorități competente sau deținătorilor de infrastructuri cibernetice aflați în aria de competență, 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 și activități adoptate și desfășurate de autoritățile cu atribuții în domeniul apărării țării și securității naționale pentru protejarea infrastructurilor cibernetice destinate apărării naționale și a infrastructurilor cibernetice naționale care susțin activitățile NATO și UE.



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

Art. 30 - (1) Activitățile prevăzute la art. 29 alin. (1) se planifică și se desfășoară de autoritățile cu atribuții în domeniul apărării țării și securității naționale în strânsă legătură cu activitățile privind apărarea națională și planificarea apărării, conform legii și potrivit obligațiilor asumate de România la nivel internațional.

(2) Autoritățile și instituțiile publice au obligația de a identifica și implementa, în condițiile legii și în termenul prevăzut de normele metodologice de aplicare a prezentei legi, măsuri de apărare cibernetică și răspund de executarea acestora, fiecare în domeniul său de activitate.

Art. 31 - (1) Ministerul Apărării Naționale împreună cu celelalte autorități și instituții publice cu atribuții în domeniul apărării țării și securității naționale asigură, din timp de pace, integrarea într-o concepție unitară a activităților privind apărarea cibernetică desfășurate de forțele armate participante la acțiunile de apărare a țării în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război.

(2) Conducerea acțiunilor 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 Național Militar de Comandă în cooperare cu Consiliul Operativ de Securitate Cibernetică.

CAPITOLUL VI - CONTROL ȘI SANCTIUNI

Art. 32 - (1) Autoritățile prevăzute la art. 9, lit. a), d) și e) au atribuții de control asupra aplicării prevederilor prezentei legi de către deținătorii infrastructurilor cibernetice aflate în competență sau responsabilitate.

(2) În vederea exercitării atribuțiilor, conducătorii autorităților competente desemnează persoanele abilitate să desfășoare activități de control, în baza și în limitele împuternicirii aprobate.

Art. 33 - (1) Nerespectarea prevederilor prezentei legi atrage răspunderea contravențională, potrivit dispozițiilor legale în vigoare.

(2) Constatarea contravențiilor și aplicarea sancțiunilor se realizează potrivit prevederilor Cap. II din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.

(3) Procesul-verbal de contravenție poate fi contestat în termen de 30 de zile de la data luării la cunoștință, conform Cap. IV din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.



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

Art. 34 - (1) La nivelul instituțiilor publice, așa cum sunt definite în Legea nr. 500/2002 privind finanțele publice, cu modificările și completările ulterioare, fondurile necesare organizării și desfășurării activității în condițiile prezentei legi se asigură de la bugetul de stat, din venituri proprii sau din alte surse legal constituite, anual, potrivit legii.

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

Art. 35 - Constituie contravenții următoarele fapte dacă nu au fost săvârșite în astfel de condiții încât să fie considerate, potrivit legii, infracțiuni:

a) nerespectarea de către deținătorii de infrastructuri cibernetice prevăzuți la art. 2, lit. a) - c) a obligațiilor prevăzute la art. 20 alin. (1), lit. a) și c);

b) încălcarea de către deținătorii de infrastructuri cibernetice prevăzuți la art. 2, lit. a) - c) a obligațiilor prevăzute la art. 20 alin. (1), lit. d), e) și f);

c) nerespectarea de către deținătorii de ICIN a obligației prevăzute la art. 18 alin. (2), precum și a obligațiilor prevăzute la art. 20, alin. (2), lit. a) - e);

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

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

f) nerespectarea de către deținătorii de infrastructuri cibernetice a cerințelor prevăzute la art. 20 alin. (1) lit. b) în condițiile stabilite de art. 24 alin. (1).

Art. 36 - Contravențiile prevăzute la art. 35 se sancționează astfel:

a) cu amendă de la 500 lei la 5.000 lei, pentru săvârșirea contravențiilor prevăzute la art. 35 lit. a), e) și f);

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

CAPITOLUL VII - DISPOZIȚII FINALE

Art. 37 - (1) În termen de 90 zile de la publicarea prezentei legi în Monitorul Oficial al României, Partea I, Ministerul Comunicațiilor și pentru Societatea Informațională cu sprijinul autorităților prevăzute la art. 8 lit. b) - e) inițiază și supune aprobării Guvernului organizarea și funcționarea Sistemului Național 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.

