PARLAMENTUL ROMÂNIEI

SENATUL **CAMERA DEPUTAŢILOR**

LEGE
privind securitatea şi apărarea cibernetică a României

Parlamentul României adoptă prezenta lege.

CAPITOLUL I
Dispoziţii generale

Art. 1. – (1) Legea stabileşte cadrul juridic şi instituţional privind organizarea şi desfăşurarea activităţilor din domeniile securitate cibernetică şi apărare cibernetică a României.

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

(3) Obiectivele prezentei legi sunt:

a) acoperirea nevoilor de securitate şi apărare cibernetică prin asigurarea rezilienţei şi protecţiei infrastructurilor cibernetice care susţin funcţiile de securitate, apărare şi guvernare ale statului;

b) menţinerea sau restabilirea climatului de securitate cibernetică la nivel naţional prin cooperarea între autorităţile competente în vederea asigurării unei reacţii rapide şi eficiente;

c) crearea şi dezvoltarea unei culturi de securitate cibernetică în cadrul administraţiei publice, prin conştientizarea ameninţărilor şi riscurilor şi formarea unei conduite preventive adecvate.

Art. 2. – (1) În domeniul securităţii cibernetice, prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru:

a) infrastructurile cibernetice deţinute, organizate, administrate, utilizate sau aflate în competenţa instituţiilor din domeniul apărării, ordinii publice, securităţii naţionale, justiţiei,

situaţiilor de urgenţă, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, precum şi cele puse la dispoziţia beneficiarilor acestora;

b) infrastructurile cibernetice deţinute de persoanele juridice de drept privat şi utilizate în vederea furnizării de servicii de comunicaţii electronice instituţiilor şi autorităţilor administraţiei publice centrale si locale;

c) infrastructurile cibernetice deţinute, organizate, administrate sau utilizate de instituţii sau autorităţi ale administraţiei publice centrale şi locale, altele decât cele prevăzute la lit. a), precum şi de persoane juridice care desfăşoară activităţi industriale, de cercetare ştiinţifică sau furnizează servicii publice ori de interes public, servicii ale societăţii informaţionale, altele decât cele de la lit. b), a căror afectare aduce atingere ordinii publice, securităţii şi apărării naţionale ori produce un impact conform prevederilor de la art.14 lit. b).

(2) În domeniul apărării cibernetice, prezenta lege are ca obiect stabilirea cadrului general de reglementare pentru infrastructurile cibernetice specifice apărării naţionale.

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

a) apărarea cibernetică cuprinde ansamblul de decizii adoptate, măsuri şi acţiuni desfăşurate de statul român, prin autorităţile şi instituţiile menţionate la art. 2, atât în context naţional cât şi în contextul apărării colective în cadrul Alianţei Nord-Atlantice şi al apărării comune în cadrul Uniunii Europene, în scopul prevenirii, detectării, monitorizării atacurilor cibernetice şi asigurării reacţiei la producerea acestora în infrastructurile cibernetice specifice apărării naţionale în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război, precum şi în scopul contracarării agresiunilor cibernetice de natură a afecta capacitatea de apărare a statului român;

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

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

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

e) cerinţe minime de securitate cibernetică – măsuri de natură organizatorică, tehnică sau procedurală destinate asigurării confidenţialităţii, integrităţii, disponibilităţii, autenticităţii şi nonrepudierii datelor stocate şi prelucrate în cadrul unei infrastructuri cibernetice;

f) date tehnice – descriere generală a infrastructurii cibernetice, rolul şi funcţionalităţile asigurate de aceasta, arhitectură, 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;

g) 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;

h) 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;

i) incident de securitate cibernetică – eveniment survenit în spaţiul cibernetic care perturbă funcţionarea uneia sau mai multor infrastructuri cibernetice şi ale cărui consecinţe sunt de natură a afecta securitatea cibernetică;

j) infrastructuri cibernetice – infrastructuri de tehnologie a informaţiei şi comunicaţii, constând în sisteme informatice, aplicaţii aferente şi reţele de comunicaţii electronice;

k) infrastructuri cibernetice specifice apărării naţionale – infrastructurile cibernetice aparţinând Ministerului Apărării Naţionale, infrastructurile cibernetice naţionale care susţin activităţile militare ale NATO şi UE, precum şi infrastructurile cibernetice de interes pentru apărarea naţională date în responsabilitatea Ministerului Apărării Naţionale în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război;

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

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

n) risc de securitate cibernetică – probabilitatea ca o ameninţare să se materializeze, exploatând o vulnerabilitate specifică infrastructurii cibernetice;

o) 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;

p) spaţiul cibernetic – mediul virtual generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta;

q) vulnerabilitate în spaţiul cibernetic – slăbiciune în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o ameninţare.

CAPITOLUL II
Sistemul Naţional de Securitate Cibernetică

Art. 4. – (1) La nivel naţional, activităţile specifice securităţii cibernetice se organizează şi se desfăşoară în mod unitar, potrivit prezentei legi.

(2) În acest scop, cooperarea în domeniu se realizează ca Sistem Naţional de Securitate Cibernetică, denumit în continuare SNSC, la care participă autorităţi şi instituţii publice care au competenţe în domeniu, potrivit prezentei legi.

(3) În exercitarea competenţelor, instituţiile şi autorităţile administraţiei publice cooperează cu sectorul privat şi cu mediul academic, cu asociaţiile profesionale şi cu organizaţiile neguvernamentale.

Art. 5. – (1) Activităţile SNSC sunt coordonate, la nivel strategic, de către Consiliul Suprem de Apărare a Ţării.

(2) Activităţile SNSC sunt coordonate, la nivel operaţional, de către Consiliul Operativ de Securitate Cibernetică.

(3) Coordonarea secretariatului tehnic al Consiliului Operativ de Securitate Cibernetică este asigurată de către Serviciul Român de Informaţii.

Art. 6. – (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 Societăţii Informaţionale, 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) 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.

(3) Conducerea Consiliului Operativ de Securitate Cibernetică este asigurată de un preşedinte – consilierul prezidenţial pe probleme de securitate naţională – şi un vicepreşedinte – consilierul prim-ministrului pe probleme de securitate naţională.

(4) Atunci când lucrările Consiliului Operativ de Securitate Cibernetică privesc sau pot avea efecte asupra infrastructurilor cibernetice prevăzute la art. 2 alin. (1) lit. b) şi c), participă şi reprezentantul Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii, denumită în continuare ANCOM, respectiv reprezentantul Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică, denumit în continuare CERT-RO, după caz.

(5) În funcţie de natura şi evoluţia ameninţărilor cibernetice, sunt invitaţi să participe în cadrul Consiliului Operativ de Securitate Cibernetică şi reprezentanţi ai altor entităţi – instituţii, autorităţi publice, persoane juridice de drept public sau privat – care pot contribui la soluţionarea problemelor de securitate cibernetică.

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

a) instituirea sau modificarea nivelurilor de alertă cibernetică la nivel naţional;

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

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

d) 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;

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

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

g) linii de mandat privind adoptarea unor rezoluţii la nivel internaţional cu privire la securitatea cibernetică care au impact pentru România.

Art. 7. – Pentru realizarea securităţii cibernetice, Consiliul Operativ de Securitate Cibernetică cooperează cu organismele de coordonare sau de conducere constituite, la nivel naţional, pentru: managementul situaţiilor de urgenţă, al acţiunilor în situaţii de criză în domeniul ordinii publice, prevenirea şi combaterea terorismului şi apărarea naţională.

Art. 8. – (1) Ministerul Comunicaţiilor şi Societăţii Informaţionale, denumit în continuare MCSI, asigură coordonarea strategică la nivel naţional pentru infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. c) prin elaborarea şi diseminarea de politici publice şi exercitarea iniţiativei legislative în domeniu.

(2) Sunt autorităţi competente în sensul prezentei legi:

a) CERT-RO pentru securitatea cibernetică a infrastructurilor prevăzute la art. 2 alin. (1) lit. c), fără a aduce atingere competenţelor celorlalte instituţii şi autorităţi cu atribuţii în domeniu;

b) ANCOM pentru coordonarea activităţilor desfăşurate în vederea asigurării securităţii cibernetice a infrastructurilor cibernetice proprii şi a celor prevăzute la art. 2 alin. (1) lit. b);

c) Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale şi Serviciul de Protecţie şi Pază pentru asigurarea securităţii şi apărării cibernetice, respectiv pentru cunoaşterea, prevenirea şi contracararea ameninţărilor cibernetice la adresa infrastructurilor cibernetice prevăzute la art. 2 alin. (1) lit. a) din domeniul lor de competenţă, activitate sau responsabilitate. În acest sens, stabilesc structuri şi măsuri tehnice şi organizatorice privind coordonarea şi controlul activităţilor de securitate şi apărare cibernetică;

d) Serviciul Român de Informaţii pentru cunoaşterea, prevenirea şi contracararea ameninţărilor cibernetice la adresa infrastructurilor cibernetice a căror afectare aduce atingere securităţii naţionale, cu excepţia infrastructurilor cibernetice din domeniul de competenţă, activitate sau responsabilitate a autorităţilor prevăzute la lit. c).

(3) În situaţia existenţei unor ameninţări cibernetice la adresa infrastructurilor cibernetice prevăzute la art. 2 alin. (1) lit. b), care ar aduce atingere securităţii naţionale, Serviciul Român de Informaţii va informa şi ANCOM, în condiţiile legii.

Art. 9. – (1) Cerinţele minime de securitate cibernetică pentru infrastructurile cibernetice prevăzute la art. 2 alin. (1), precum şi modalitatea de notificare a incidentelor de

securitate cibernetică se stabilesc, potrivit competenţelor, de către instituţiile prevăzute la art. 8 alin. (2) lit. a)-c).

(2) Pentru infrastructurile cibernetice de la art. 2 alin. (1), cerinţele minime de securitate cibernetică au în vedere cel puţin următoarele categorii de activităţi:

a) managementul drepturilor de acces şi jurnalizarea acestora;

b) conştientizarea şi instruirea continuă a utilizatorilor şi verificarea cunoştinţelor acestora;

c) jurnalizarea şi asigurarea trasabilităţii activităţilor în cadrul infrastructurilor cibernetice;

d) testarea şi evaluarea periodică a securităţii infrastructurilor cibernetice;

e) managementul configuraţiilor infrastructurilor cibernetice;

f) asigurarea disponibilităţii şi a rezilienţei infrastructurilor cibernetice;

g) managementul identificării şi autentificării utilizatorilor;

h) răspunsul la incidente;

i) mentenanţa reţelelor şi sistemelor informatice;

j) managementul mediilor de stocare;

k) asigurarea protecţiei fizice a infrastructurilor cibernetice;

l) realizarea planurilor de securitate;

m) asigurarea securităţii personalului;

n) analizarea şi evaluarea riscurilor;

o) asigurarea protecţiei produselor şi serviciilor aferente infrastructurilor cibernetice;

p) managementul vulnerabilităţilor şi alertelor de securitate;

q) managementul parolelor, inclusiv pentru conturile privilegiate de utilizatori sau aplicaţii;

r) managementul accesului si jurnalizarea, distinct pentru activitatea la nivelul bazelor de date;

s) asigurarea protecţiei aplicaţiilor web;

t) asigurarea prevenirii accesului neautorizat şi a intruziunilor.

Art. 10. – Autorităţile prevăzute de art. 8 alin. (2) au următoarele obligaţii:

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

b) să acorde sprijin, la solicitarea deţinătorilor de infrastructuri cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate, pentru implementarea măsurilor corespunzătoare nivelurilor de alertă cibernetică;

c) să colecteze notificările cu privire la incidente de securitate cibernetică din cadrul infrastructurilor cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate;

d) să evalueze datele şi informaţiile cu privire la incidente şi atacuri cibernetice la adresa infrastructurilor cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate;

e) să notifice deţinătorii de infrastructuri cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate cu privire la incidente de securitate cibernetică sau vulnerabilităţi şi atacuri cibernetice identificate la nivelul acestora;

f) să coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul infrastructurilor cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate;

g) să acorde sprijin, la solicitare sau după notificarea prevăzută la lit. e), deţinătorilor de infrastructuri cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgenţă pentru remedierea efectelor incidentelor de securitate cibernetică;

h) să desfăşoare activităţi de informare şi comunicare publică;

i) să organizeze sesiuni de formare şi instruire în domeniul securităţii cibernetice;

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

k) să-şi comunice reciproc date de interes referitoare la securitatea cibernetică, inclusiv către celelalte autorităţi şi instituţii publice sau deţinători de infrastructuri cibernetice;

l) să solicite convocarea Consiliului Operativ de Securitate Cibernetică, potrivit competenţelor prevăzute în prezenta lege.

Art. 11. – Autorităţile prevăzute la art. 8 alin. (2) pot constitui şi operaţionaliza structuri specializate în realizarea de audit de securitate cibernetică şi structuri specializate de securitate cibernetică.

Art. 12. – Pentru infrastructurile cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate, autorităţile prevăzute la art. 8 alin. (2) lit. c) au şi următoarele obligaţii 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. 13. – (1) In scopul prezentei legi, la nivelul MCSI se constituie un registru în care sunt evidenţiate infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. b) şi c).

(2) În procesul identificării infrastructurilor cibernetice prevăzute la art. 2 alin. (1) lit. c), instituţiile şi autorităţile administraţiei publice centrale şi locale, altele decât cele ale căror infrastructuri sunt prevăzute la art. 2 alin. (1) lit. a), precum şi persoanele juridice care desfăşoară activităţi industriale, de cercetare ştiinţifică sau furnizează servicii publice ori de interes public sau ale societăţii informaţionale, au obligaţia de a furniza MCSI datele tehnice necesare.

(3) Pentru identificarea şi inventarierea infrastructurilor cibernetice de la art. 2 alin. (1) lit. b), persoanele care deţin, organizează sau administrează aceste infrastructuri, transmit ANCOM datele tehnice necesare, în condiţiile şi formatul stabilite de către această autoritate.

(4) ANCOM transmite MCSI inventarul realizat conform alin. (3) în vederea completării registrului.

(5) Datele tehnice necesare pentru întocmirea registrului trebuie să cuprindă următoarele:

a) serviciile publice ori de interes public sau ale societăţii informaţionale furnizate, precum şi beneficiarii acestora;

b) descrierea generală a infrastructurilor cibernetice;

c) rolul şi funcţionalităţile asigurate;

d) informaţii privind punctul de contact.

(6) Se exceptează de la alin. (2) infrastructurile cibernetice constituite la nivelul Autorităţilor Desemnate de Securitate care deţin structuri interne INFOSEC potrivit reglementărilor în domeniu, precum şi infrastructurile cibernetice 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.

(7) Registrul nu va conţine date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate.

(8) Orice modificare cu privire la datele prevăzute la alin. (5) se comunică MCSI sau, după caz, ANCOM, în termen de 30 de zile de la apariţia acesteia.

Art. 14. – La evaluarea infrastructurilor cibernetice în vederea includerii în registru vor fi avute în vedere, cumulativ, următoarele criterii:

a) Infrastructurile cibernetice se încadrează în cel puţin una dintre următoarele categorii:

1. să fie utilizate pentru susţinerea activităţii autorităţilor administraţiei publice sau furnizarea de servicii acestora;

2. să fie destinate susţinerii serviciilor publice ori de interes public sau ale societăţii informaţionale;

3. să susţină procese industriale;

4. să susţină activităţi de cercetare ştiinţifică;

5. să susţină tranzacţii economice şi financiar-bancare.

b) Impactul incidentelor de securitate cibernetică asupra respectivelor infrastructuri cibernetice este de natură să afecteze cel puţin:

1. capacitatea de guvernare a statului;

2. securitatea naţională;

3. relaţiile internaţionale ale statului;

4. viaţa, sănătatea sau integritatea corporală a cetăţenilor;

5. furnizarea serviciului public ori de interes public;

6. interdependenţa cu alte infrastructuri cibernetice de acelaşi nivel;

7. accesul cetăţenilor şi al mediului de afaceri la servicii publice;

8. mediul economic al statului, resursele economice naţionale, dreptul de proprietate intelectuală.

Art. 15. – (1) Identificarea infrastructurilor cibernetice de la art. 2 alin. (1) lit. c) în vederea includerii în registru se realizează în condiţiile art. 13 şi 14, sau din oficiu, de către MCSI, în condiţiile prezentei legi.

(2) Infrastructurile cibernetice care nu mai îndeplinesc condiţiile şi criteriile prevăzute la art. 14 se radiază de MCSI din registru, din oficiu sau la notificarea persoanelor juridice care le deţin, administrează, organizează sau utilizează.

(3) Persoanele juridice care deţin, administrează, organizează sau utilizează infrastructuri cibernetice pot solicita MCSI asistenţă pentru includerea în registru.

(4) MCSI notifică de îndată persoanele juridice care deţin, administrează, organizează sau utilizează infrastructurile cibernetice de la art. 2 alin. (1) lit. c), precum şi ANCOM, în cazul persoanelor care deţin infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. b), cu privire la includerea sau radierea acestora în registru din oficiu.

Art. 16. – Persoanele juridice care deţin, administrează, organizează sau utilizează infrastructuri cibernetice înscrise în registru au următoarele drepturi:

a) să fie informate 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, administrată, organizată sau utilizată;

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 acreditaţi;

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

f) să realizeze managementul incidentelor de securitate cibernetică, prin utilizarea resurselor proprii, prin contractarea unor servicii de securitate cibernetică sau prin solicitarea sprijinului autorităţilor competente;

g) să fie notificate cu privire la includerea sau radierea din oficiu în registru.

Art. 17. – Persoanele juridice înscrise în registru au următoarele obligaţii:

a) să notifice de îndată autoritatea competentă, iar în cazul persoanelor prevăzute la art. 2 alin. (1) lit. b), şi instituţiile şi autorităţile cărora le furnizează servicii de comunicaţii electronice potenţial a fi afectate, cu privire la incidentele de securitate cibernetică identificate;

b) să se asigure că accesul la datele şi informaţiile referitoare la configurarea şi protecţia infrastructurilor cibernetice este jurnalizat, iar datele şi informaţiile respective sunt diseminate exclusiv persoanelor autorizate;

c) să nu permită accesul la conţinutul informaţiilor stocate, prelucrate sau transmise în cadrul sau prin infrastructurile cibernetice deţinute, administrate sau utilizate, în lipsa unei autorizaţii emise în condiţiile legii;

d) să îşi gestioneze incidentele de securitate cibernetică;

e) să întreprindă măsuri astfel încât, prin acţiunile proprii, să nu afecteze securitatea altor infrastructuri cibernetice;

f) să se asigure că infrastructurile cibernetice sunt auditate anual pe linia securităţii cibernetice, potrivit standardelor şi specificaţiilor europene sau internaţionale aplicabile;

g) să constituie, în condiţiile legii, structuri sau să desemneze persoane responsabile privind coordonarea activităţilor de securitate cibernetică;

h) să pună la dispoziţia autorităţii competente, la solicitarea motivată a acesteia, rezultatele auditului de securitate cibernetică;

i) 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;

j) să transmită autorităţilor competente date referitoare la rezultatele măsurilor aplicate pentru contracararea incidentelor de securitate cibernetică;

k) să respecte cerinţele minime de securitate stabilite de autorităţile competente.

Art. 18. – (1) Furnizorii de servicii de securitate cibernetică ce desfăşoară activităţi pe teritoriul României au obligaţia să notifice autorităţile competente de îndată, dar nu mai târziu de 24 de ore, cu privire la identificarea unor ameninţări sau vulnerabilităţi critice a căror manifestare poate afecta o infrastructură 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.

Art. 19. – (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 actelor de autorizare a restrângerii temporare a exerciţiului drepturilor şi libertăţilor persoanelor, emise de judecător pentru îndeplinirea scopului prezentei legi.

(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 sprijin 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 III
Asigurarea securităţii cibernetice

Art. 20. – (1) Sistemul Naţional de Alertă Cibernetică, denumit în continuare SNAC, este un ansamblu de măsuri tehnice şi procedurale destinate evaluării şi optimizării componentelor şi funcţiilor SNSC în vederea prevenirii descurajării şi combaterii acţiunilor sau inacţiunilor ce se pot constitui în vulnerabilităţi sau ameninţări la adresa securităţii cibernetice a României.

(2) În cadrul SNAC, ameninţările, incidentele sau atacurile 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, precum şi trecerea de la un nivel la altul se decide de către autorităţile competente prevăzute la art. 8 alin. (2) pentru infrastructurile din aria de

competenţă, activitate sau responsabilitate, cu informarea Consiliului Operativ de Securitate Cibernetică.

(4) Instituirea sau modificarea nivelurilor de alertă cibernetică 1 – verde – SCĂZUT sau 2 – galben – MODERAT, la nivel naţional, se aprobă de către Consiliul Operativ de Securitate Cibernetică, la propunerea membrilor acestuia şi se comunică de către autorităţile prevăzute de art. 8 alin. (2).

(5) Instituirea sau modificarea nivelurilor de alertă cibernetică 3 – portocaliu – RIDICAT sau 4 – roşu – CRITIC, la nivel naţional, se aprobă de către Consiliul Suprem de Apărare a Ţării, la propunerea Consiliului Operativ de Securitate Cibernetică.

Art. 21. – (1) Persoanele juridice de drept public sau privat care deţin, organizează, administrează sau utilizează infrastructurile cibernetice prevăzute la art. 2 alin. (1) au următoarele obligaţii:

a) să elaboreze planuri de acţiune proprii, corespunzătoare fiecărui nivel de alertă cibernetică;

b) să pună în aplicare, la instituirea unui nivel de alertă cibernetică, planurile de acţiune prevăzute la lit. a).

(2) Persoanele juridice de drept public sau privat care deţin, organizează, administrează sau utilizează infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. b) şi c) au următoarele obligaţii:

a) să sprijine autorităţile competente pentru implementarea măsurilor corespunzătoare fiecărui nivel de alertă cibernetică;

b) să informeze autorităţile competente, la modificarea nivelului de alertă cibernetică, cu privire la gradul de afectare a infrastructurii cibernetice şi îndeplinirea măsurilor din planul de acţiune.

(3) În funcţie de impactul asupra securităţii cibernetice, nivelurile de alertă cibernetică sunt ierarhizate după cum urmează:

a) Verde – SCĂZUT – se aplică dacă informaţiile disponibile şi evenimentele recente indică probabilitatea scăzută ca un incident de securitate cibernetică să aibă loc.

b) Galben – MODERAT – se aplică dacă informaţiile disponibile şi evenimentele recente indică o probabilitate medie de producere a unui incident de securitate cibernetică.

c) Portocaliu – RIDICAT – se aplică dacă informaţiile disponibile şi evenimentele recente indică probabilitatea ridicată de producere a unui incident de securitate cibernetică.

d) Roşu – CRITIC – se aplică dacă informaţiile disponibile şi evenimentele recente indică un risc iminent de producere a unui incident de securitate cibernetică, fără a fi cunoscut un remediu imediat şi care poate fi fatal pentru una sau mai multe infrastructuri, sau producerea efectivă a acestuia.

(4) Pentru nivelul de alertă cibernetică SCĂZUT se aplică măsuri de securitate de rutină, menţinute pe termenul de valabilitate a nivelului de alertă şi fără impact asupra desfăşurării activităţii curente.

(5) Pentru nivelul de alertă cibernetică MODERAT se aplică măsuri de securitate suplimentare, menţinute pe termenul de valabilitate a nivelului de alertă chiar dacă ar putea avea impact asupra desfăşurării activităţii curente.

(6) Pentru nivelul de alertă cibernetică RIDICAT se aplică măsuri de securitate suplimentare, menţinute pe termenul de valabilitate a nivelului de alertă chiar dacă pot avea impact asupra desfăşurării activităţii curente.

(7) Pentru nivelul de alertă cibernetică CRITIC se aplică măsuri de securitate suplimentare, menţinute pe termenul de valabilitate a nivelului de alerta chiar dacă au impact asupra desfăşurării activităţii curente.

CAPITOLUL IV
Gestionarea incidentelor de securitate cibernetică

Art. 22. – (1) Notificarea incidentelor de securitate cibernetică se transmite în modalitatea stabilită de autoritatea competentă şi trebuie să conţină, în mod obligatoriu, următoarele:

a) elementele de identificare ale infrastructurii cibernetice afectate;

b) descrierea incidentului;

c) perioada de desfăşurare a incidentului;

d) impactul estimat al incidentului;

e) măsuri preliminare adoptate;

f) lista de autorităţi ale statului afectate de incident;

g) întinderea geografică potenţială a incidentului;

h) date despre efecte potenţial transfrontaliere ale incidentului.

(2) Notificarea prevăzută la alin. (1) nu va conţine:

a) informaţii clasificate;

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

Art. 23. – Autorităţile competente au obligaţia de a stoca şi de a păstra pe un termen de 5 ani notificările primite cu privire la incidentele de securitate cibernetică şi rezultatele măsurilor de contracarare a acestora.

Art. 24. – La primirea unei notificări sau în cazul identificării unui incident de securitate cibernetică, autoritatea competentă are obligaţia să:

a) coordoneze activitatea de management al incidentelor de securitate cibernetică şi să acorde sprijin deţinătorilor de infrastructuri cibernetice aflate în domeniul său de competenţă, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgenţă pentru asigurarea integrităţii datelor necesare asigurării securităţii cibernetice şi remedierea efectelor incidentelor de securitate cibernetică;

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

CAPITOLUL V
Apărarea cibernetică

Art. 25. – În domeniul apărării cibernetice, Ministerul Apărării Naţionale are următoarele responsabilităţi:

a) apără/protejează sistemele şi infrastructurile cibernetice aparţinând Ministerului Apărării Naţionale;

b) planifică, conduce şi execută operaţii în spaţiul cibernetic, prin Statul Major al Apărării;

c) asigură cooperarea şi schimbul de informaţii cu entităţile militare ale NATO, cu parteneri de alianţă şi alte organisme militare, în domeniul apărării cibernetice;

d) asigură punct unic de contact cu NATO în domeniul operaţiilor în spaţiul cibernetic.

Art. 26. – Conducerea acţiunilor de apărare cibernetică se realizează prin Centrul Naţional Militar de Comandă, potrivit legii.

Art. 27. – (1) Ministerul Apărării Naţionale implementează politici şi standarde în domeniul apărării cibernetice, în acord cu standardele şi cerinţele elaborate la nivelul NATO şi UE.

(2) Autorităţile şi instituţiile publice din domeniul apărării, ordinii publice şi securităţii naţionale implementează măsuri proprii în domeniul apărării cibernetice, armonizate cu standardele de interoperabilitate şi cerinţele minime adoptate şi puse la dispoziţie de către Ministerul Apărării Naţionale.

(3) Infrastructurile cibernetice de interes pentru apărarea naţională ale autorităţilor şi instituţiilor publice din domeniul apărării, ordinii publice şi securităţii naţionale se stabilesc prin hotărâre a Consiliului Suprem de Apărare a Ţării şi se actualizează anual sau ori de câte ori este nevoie.

CAPITOLUL VI
Control şi sancţiuni

Art. 28. – Nerespectarea prevederilor prezentei legi poate atrage răspunderea administrativă, civilă, contravenţională sau penală, după caz, în condiţiile legii.

Art. 29. – Constituie contravenţii următoarele fapte dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate infracţiuni, potrivit legii:

a) nerespectarea obligaţiilor prevăzute la art. 13 alin. (2), alin. (3) şi alin. (8);

b) nerespectarea obligaţiilor prevăzute la art. 17;

c) nerespectarea obligaţiilor prevăzute la art. 18 alin. (1);

d) nerespectarea de către persoanele juridice de drept public sau privat care deţin, organizează, administrează sau utilizează infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. b) şi c) a obligaţiilor prevăzute la art. 21.

Art. 30. – (1) Contravenţiile prevăzute la art. 29 se sancţionează cu amendă de la 3.000 lei la 50.000 lei, iar în cazul unor încălcări repetate, cu amendă în cuantum de până la 100.000 lei;

(2) În vederea individualizării sancţiunii, autorităţile prevăzute la art. 8 alin. (2) vor lua în considerare gradul de pericol social concret al faptei, perioada de timp în care obligaţia legală a fost încălcată, precum şi, dacă este cazul, consecinţele încălcării.

(3) În măsura în care prezenta lege nu prevede altfel, contravenţiilor prevăzute la art. 29 li se aplică dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

Art. 31. – Controlul respectării prevederilor prezentei legi la nivelul infrastructurilor cibernetice de la art. 2 alin. (1) revine autorităţilor competente prevăzute la art. 8 alin. (2) lit. a)-c), care acţionează prin personal de specialitate împuternicit în acest scop.

CAPITOLUL VII
Dispoziţii finale

Art. 32. – (1) În termen de 6 luni de la intrarea în vigoare a prezentei legi, Ministerul Apărării Naţionale, cu sprijinul autorităţilor prevăzute la art. 8 alin. (1) si (2), elaborează normele metodologice de aplicare a prezentei legi şi le supune aprobării Guvernului.

(2) Cerinţele minime de securitate prevăzute la art. 9 alin. (1) se emit, în termen de 180 de zile de intrarea în vigoare a normelor prevăzute la alin. (1), de către:

a) ANCOM, pentru infrastructurile cibernetice proprii, precum şi pentru cele prevăzute la art. 2 alin. (1) lit. b);

b) CERT-RO pentru infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. c);

c) autorităţile prevăzute la art. 8 alin. (2) lit. c) pentru infrastructurile cibernetice prevăzute la art. 2 alin. (1) lit. a).