

PARLAMENTUL ROMÂNIEI

SENATUL

CAMERA DEPUTAȚILOR

LEGE

privind securitatea cibernetică a României

Parlamentul României adoptă prezenta lege.

CAPITOLUL I

Dispoziții generale

Art.1. - Prezenta lege stabilește cadrul general de reglementare a activităților în domeniul securității cibernetică și obligațiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetică.

Art.2. - Dispozițiile prezentei legi se aplică persoanelor juridice de drept public sau privat, care au calitatea de proprietari, administratori, operatori sau utilizatori de infrastructuri cibernetică, denumite în continuare deținători de infrastructuri cibernetică.

Art.3. - (1) Securitatea cibernetică este componentă a securității naționale a României și se realizează prin:

a) cunoașterea, prevenirea și contracararea amenințărilor și atacurilor, precum și prin diminuarea vulnerabilităților infrastructurilor cibernetică, în scopul gestionării riscurilor la adresa securității acestora;

b) prevenirea și combaterea criminalității informatice;

c) apărarea cibernetică.

(2) Prevenirea criminalității informatice se realizează în condițiile Legii nr.161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu modificările și completările ulterioare. Combaterea criminalității informatice se efectuează de organele judiciare în condițiile legislației penale și procesual penale.

Art.4. -Securitatea cibernetică vizează:

- a) realizarea rezilienței infrastructurilor cibernetic;
- b) creșterea capacității de reacție la incidentele cibernetic și diminuarea impactului acestora asupra resurselor și serviciilor infrastructurilor cibernetic;
- c) asigurarea protecției datelor gestionate prin intermediul infrastructurilor cibernetic;
- d) asigurarea nivelului de încredere necesar pentru dezvoltarea societății informaționale și a mediului de afaceri în spațiul cibernetic;
- e) realizarea accesului egal și nediscriminatoriu al persoanelor la informații și servicii publice oferite prin intermediul infrastructurilor cibernetic;
- f) guvernanta participativă, democratică și eficientă a spațiului cibernetic;
- g) responsabilizarea deținătorilor de infrastructuri cibernetic pentru asigurarea securității cibernetic;
- h) asigurarea climatului de exercitare neîngrădită a drepturilor și libertăților fundamentale ale persoanelor în spațiul cibernetic.

Art.5. - În sensul prezentei legi, termenii și expresiile de mai jos au următorul înțeles:

1. amenințare cibernetică - circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetic;

2. apărare cibernetică – acțiuni desfășurate în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun

împotriva amenințărilor asupra infrastructurilor cibernetice destinate apărării naționale;

3. atac cibernetic - acțiune ostilă de natură să afecteze securitatea cibernetică, desfășurată în spațiul cibernetic;

4. audit de securitate cibernetică – evaluare sistematică, detaliată, măsurabilă și tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, precum și emiterea de recomandări pentru minimizarea riscurilor identificate;

5. incident cibernetic - eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică;

6. eveniment survenit în spațiul cibernetic – acțiune desfășurată în spațiul cibernetic care are drept consecință modificarea stării infrastructurilor cibernetice;

7. infrastructuri cibernetice - infrastructuri din domeniul tehnologiei informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice;

8. infrastructuri cibernetice de interes național (ICIN) - infrastructurile cibernetice care susțin servicii publice sau de interes public, ori servicii ale societății informaționale, a căror afectare poate aduce atingere securității naționale, sau prejudicii grave statului român ori cetățenilor acestuia, denumite în continuare ICIN ;

9. managementul identității - metode de validare a identității persoanelor când acestea accesează anumite infrastructuri cibernetice;

10. managementul riscului - un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetice, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură;

11. operații în rețele de calculatoare - procesul complex de planificare, coordonare, sincronizare, armonizare și desfășurare a acțiunilor în spațiul cibernetic pentru protecția, controlul și utilizarea rețelelor de calculatoare, în scopul obținerii superiorității informaționale, concomitent cu neutralizarea capabilităților adversarului;

12. reziliența infrastructurilor cibernetice - capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate;

13. risc de securitate în spațiul cibernetic - probabilitatea ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice;

14. securitate cibernetică - starea 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, a resurselor și serviciilor publice sau private, din spațiul cibernetic. Măsurile proactive și reactive pot include politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protejare a infrastructurilor cibernetice, managementul identității, managementul consecințelor;

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

16. 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.

CAPITOLUL II

Sistemul Național de Securitate Cibernetică

Art.6. - (1) În vederea asigurării cadrului general de cooperare pentru realizarea securității cibernetice se constituie Sistemul Național de Securitate Cibernetică, denumit în continuare SNSC, care reunește autoritățile și instituțiile publice cu responsabilități și capacități în domeniu.

(2) Autoritățile și instituțiile publice din SNSC colaborează cu deținătorii de infrastructuri cibernetice, mediul academic, mediul de afaceri, asociațiile profesionale și organizațiile neguvernamentale.

(3) Activitatea SNSC este coordonată la nivel strategic de Consiliul Suprem de Apărare a Țării, denumit în continuare CSAT.

Art.7. - (1) SNSC îndeplinește următoarele funcții:

a) funcția de cunoaștere, prin care furnizează suportul informațional necesar elaborării măsurilor proactive și reactive, în vederea asigurării securității cibernetice;

b) funcția de prevenire, prin care asigură în principal, securitatea cibernetică a României, prin crearea și dezvoltarea capacităților necesare analizei și prognozei evoluției stării acesteia;

c) funcția de cooperare și coordonare, prin care asigură mecanismul unitar și eficient de relaționare a autorităților și instituțiilor componente ale SNSC;

d) funcția de contracarare, prin care asigură reacția eficientă la amenințările sau atacurile cibernetice, prin identificarea și blocarea manifestării acestora. Aceasta se realizează în scopul menținerii sau restabilirii securității infrastructurilor cibernetice vizate, precum și pentru identificarea și sancționarea autorilor, potrivit legii.

(2) Funcțiile SNSC se realizează prin adoptarea de măsuri proactive și reactive privind informarea, monitorizarea, diseminarea, analizarea, avertizarea, coordonarea, decizia, reacția, refacerea și conștientizarea.

Art.8. - (1) Coordonarea unitară a activităților SNSC se realizează de către Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC.

(2) COSC este format din reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază,

Oficiului Registrului Național al Informațiilor Secrete de Stat, precum și Secretarul Consiliului Suprem de Apărare a Țării.

(3) Conducerea COSC este asigurată de Consilierul Prezidențial pentru apărare și securitate națională, în calitate de președinte și de Consilierul Primului Ministru pe probleme de securitate națională – în calitate de vicepreședinte.

(4) COSC își desfășoară activitatea în conformitate cu propriul Regulament de organizare și funcționare, care se aprobă prin hotărâre a CSAT, la propunerea Consilierului Prezidențial pentru apărare și securitate națională, în termen de 60 de zile de la intrarea în vigoare a prezentei legi.

(5) La activitățile COSC pot participa, în calitate de invitați, reprezentanți ai altor instituții sau autorități publice.

Art.9. - (1) În exercitarea atribuțiilor sale, COSC analizează și evaluează starea securității cibernetice, formulează și înaintează CSAT 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 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;

f) cerințe minime de securitate cibernetică și politici de securitate cibernetică pentru autoritățile și instituțiile publice prevăzute la art.10 alin.(1) și (2).

(2) COSC cooperează pentru realizarea securității cibernetice cu organismele de coordonare sau conducere constituite, potrivit legii, 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, așa cum sunt acestea prevăzute de legislația în domeniu.

Art.10. - (1) Serviciul Român de Informații este desemnat autoritate națională în domeniul securității cibernetice, calitate în care asigură coordonarea tehnică a COSC, precum și organizarea și executarea activităților care privesc securitatea cibernetică a României. În acest scop, în structura SRI funcționează Centrul Național de Securitate Cibernetică, denumit în continuare CNSC.

(2) Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază sunt desemnate autorități în domeniul securității cibernetice pentru domeniile lor de activitate, asigurând securitatea infrastructurilor cibernetice proprii sau aflate în responsabilitate potrivit legii și au obligația să constituie și să operaționalizeze structuri specializate de securitate cibernetică.

(3) CNSC cooperează cu autoritățile și instituțiile publice componente ale SNSC, precum și cu deținătorii de infrastructuri cibernetice.

(4) În caz de atac cibernetic care poate afecta securitatea cibernetică a României, CNSC este punct de contact pentru relaționarea cu organismele similare din străinătate.

(5) CERT-RO reprezintă un punct național de contact cu structurile de tip CERT care funcționează în cadrul instituțiilor sau autorităților publice ori al altor persoane juridice de drept public sau privat, naționale ori internaționale, cu respectarea competențelor ce revin celorlalte autorități și instituții publice cu atribuții în domeniu, potrivit legii.

Art.11. - (1) CNSC are următoarele atribuții principale:

a) acționează în scopul cunoașterii, prevenirii, protecției, reacției și managementului consecințelor amenințărilor și atacurilor cibernetice;

b) asigură schimbul de date și informații între autoritățile și instituțiile publice

componente ale SNSC;

c) analizează și integrează date și informații obținute de autoritățile și instituțiile publice componente ale SNSC, în scopul stabilirii, întreprinderii sau propunerii măsurilor ce se impun pentru asigurarea securității cibernetice;

d) asigură colectarea și identificarea evenimentelor survenite în spațiul cibernetic;

e) generează avertizări pentru deținătorii de infrastructuri cibernetice și ICIN cu privire la posibile incidente de securitate cibernetică și emite recomandări cu privire la modalitatea de acțiune;

f) primește notificările făcute de persoanele juridice de drept public care dețin sau administrează ICIN, potrivit art. 20 alin. (1) lit. h);

g) transmite autorităților și instituțiilor publice competente din cadrul SNSC datele și informațiile necesare punerii în aplicare a măsurilor specifice de acțiune corespunzătoare fiecărui nivel de alertă cibernetică;

h) elaborează propuneri cu privire la nivelul de alertă cibernetică pe care le înaintează COSC, în baza analizelor și evaluărilor efectuate cu privire la starea de securitate cibernetică la nivel național;

i) înaintează propuneri către COSC cu privire la declararea nivelurilor de alertă cibernetică;

j) în caz de atac cibernetic, asigură colectarea și evaluarea datelor și informațiilor cu privire la incident, propune deținătorilor de ICIN sau, după caz, ia măsuri reactive de primă urgență pentru asigurarea integrității datelor și remedierea situației de fapt, informează potrivit legii, organele competente pentru investigare și cercetare, sau, după caz, sesizează organele de urmărire penală.

(2) Autoritățile și instituțiile publice din componența COSC deleagă un reprezentant în cadrul CNSC.

(3) Cadrul general de organizare și funcționare a CNSC se aprobă prin hotărâre a CSAT, la propunerea SRI, în termen de 60 de zile de la intrarea în vigoare a prezentei legi.

Art.12. - Autoritățile și instituțiile publice prevăzute la art. 10 alin. (1) și (2) asigură securitatea infrastructurilor cibernetice proprii sau aflate în responsabilitate potrivit legii și în acest sens exercită următoarele atribuții generale:

a) elaborează și implementează politici de securitate și programe destinate managementului riscurilor de securitate cibernetică;

b) asigură managementul incidentelor de securitate cibernetică;

c) controlează modul în care se asigură securitatea cibernetică;

d) elaborează și aprobă cadrul specific de reglementare destinat asigurării securității cibernetice, cu respectarea cerințelor stabilite la nivel național;

e) contribuie conform competențelor legale la asigurarea securității cibernetice în cadrul SNSC;

f) cooperează și schimbă date și informații referitoare la securitatea cibernetică cu CNSC și cu celelalte autorități și instituții publice sau deținători de infrastructuri cibernetice;

g) sesizează sau solicită convocarea COSC, potrivit propriilor competențe și ori de câte ori se impune, inclusiv pentru ridicarea nivelului de alertă;

h) asigură colectarea și evaluarea datelor și informațiilor cu privire la incidente și atacuri cibernetice, ia măsuri reactive de primă urgență pentru asigurarea integrității datelor și remediarea situației de fapt.

Art.13. - (1) În vederea realizării coerenței activităților din cadrul SNSC, Ministerul pentru Societatea Informațională asigură legătura COSC cu autoritățile și instituțiile publice care nu sunt reprezentate în cadrul acestuia, iar prin Centrul Național de Răspuns la Incidente de Securitate, denumit în continuare CERT-RO, cu deținătorii de infrastructuri cibernetice, persoane juridice de drept privat.

(2) În cazul persoanelor prevăzute la art. 23 alin. (1), pentru realizarea dispozițiilor alin. (1), Ministerul pentru Societatea Informațională va colabora cu Autoritatea Națională pentru Administrare și Reglementare în Comunicații, denumită în continuare ANCOM.

Art.14. - În cadrul SNSC autoritățile și instituțiile publice desfășoară, potrivit competențelor legale, activități pentru asigurarea securității cibernetice a României, inclusiv activități de informare și comunicare publică, relații publice și de cooperare internațională.

Art.15. - (1) La nivel național se constituie Sistemul Național de Alertă Cibernetică denumit în continuare SNAC, reprezentând un ansamblu organizat de măsuri tehnice și proceduri și principalul mijloc al SNSC destinat prevenirii și contracarării activităților de natură să afecteze securitatea cibernetică.

(2) Organizarea SNAC, măsurile specifice pe care autoritățile și instituțiile publice competente le implementează pentru fiecare nivel de alertă, precum și procedura de instituire a nivelurilor de alertă și cerințele privind elaborarea planurilor de acțiune se aprobă prin norme metodologice, la propunerea SRI.

(3) În cadrul SNAC, 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.

(4) Instituirea nivelurilor de alertă cibernetică, precum și trecerea de la un nivel la altul se aprobă de către CSAT, la propunerea COSC.

(5) Pentru punerea în aplicare a măsurilor specifice prevăzute la alin. (2) persoanele juridice de drept public sau privat deținători de ICIN elaborează planuri de acțiune proprii, corespunzătoare fiecărui nivel de alertă cibernetică.

(6) La instituirea unui nivel de alertă cibernetică, persoanele juridice de drept public sau privat deținători de ICIN au obligația să pună în aplicare măsurile specifice prevăzute prin planurile prevăzute la alin.(5).

(7) Deținătorii de infrastructuri cibernetice au obligația să sprijine autoritățile și instituțiile publice competente pentru implementarea măsurilor corespunzătoare fiecărui nivel de alertă cibernetică, potrivit solicitărilor acestora, adresate în condițiile art.17 alin.(1) lit.a).

(8) Persoanele juridice de drept public sau privat deținători de ICIN au obligația transmiterii cu celeritate a datelor privind starea de securitate cibernetică la nivelul acestora către CNSC conform competențelor prevăzute de lege.

CAPITOLUL III

Asigurarea securității cibernetică

Art.16. - Deținătorii de infrastructuri cibernetică au următoarele obligații:

a) să aplice politici de securitate cibernetică, cu respectarea cerințelor minime de securitate stabilite la nivel național de Ministerul pentru Societatea Informațională, ANCOM sau de către alte autorități publice competente potrivit legii;

b) să identifice și să implementeze măsurile tehnice și organizatorice adecvate pentru a gestiona eficient riscurile de securitate în infrastructurile cibernetică proprii sau aflate în responsabilitate;

c) să prevină și să reducă la minimum impactul incidentelor care afectează infrastructurile cibernetică proprii sau aflate în responsabilitate;

d) să nu afecteze, prin acțiunile proprii, securitatea altor infrastructuri cibernetică;

e) să prevină accesul neautorizat al persoanelor la resursele infrastructurilor cibernetică proprii sau aflate în responsabilitate;

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

Art.17. (1) Pentru realizarea securității cibernetică, deținătorii de infrastructuri cibernetică au următoarele responsabilități:

a) să acorde sprijinul necesar, la solicitarea motivată a Serviciului Român de Informații, Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Oficiului Registrului Național al Informațiilor Secrete de Stat, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază,

CERT-RO și ANCOM, în îndeplinirea atribuțiilor ce le revin acestora și să permită accesul reprezentanților desemnați în acest scop la datele deținute, relevante în contextul solicitării;

b) să informeze, de îndată, autoritățile și instituțiile publice prevăzute la lit.a) cu privire la incidentele cibernetice identificate, conform procedurilor stabilite prin normele metodologice la prezenta lege.

(2) Deținătorii de infrastructuri cibernetice pot solicita asistență de specialitate autorităților și instituțiilor publice cu atribuții în domeniul securității cibernetice, pentru asigurarea securității cibernetice în domeniul lor de activitate.

Art.18. - Deținătorii de infrastructuri cibernetice, furnizorii de servicii de internet au obligația de a-și notifica clienții, persoane de drept public și privat, de îndată, 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 incidente sau atacuri cibernetice și de a dispune măsurile necesare în vederea restabilirii condițiilor normale de funcționare.

Art.19. - (1) La nivel național se constituie Catalogul ICIN, care se aprobă în termen de 90 de zile de la intrarea în vigoare a prezentei legi, prin hotărâre a Guvernului .

(2) Catalogul ICIN se întocmește de către Ministerul pentru Societatea Informațională, cu consultarea COSC, la propunerea CNSC sau după caz, a CERT-RO, potrivit competențelor legale.

(3) Identificarea ICIN se realizează pe baza criteriilor de selecție cuprinse în metodologia elaborată de Serviciul Român de Informații și Ministerul pentru Societatea Informațională și aprobată, în termen de 60 de zile de la intrarea în vigoare a prezentei legi, prin hotărâre de Guvern.

(4) La elaborarea catalogului ICIN, Ministerul pentru Societatea Informațională va colabora și cu ANCOM, în situația persoanelor juridice de drept

privat care dețin calitatea de furnizori de rețele publice sau servicii de comunicații electronice destinate publicului.

(5) Se exceptează de la prevederile alin. (1) ICIN 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, denumit în continuare ORNISS.

(6) ICIN prevăzute la alin. (5), se comunică CNSC, cu excepția celor constituite la nivelul Autorităților Desemnate de Securitate, care dețin Structuri Interne INFOSEC acreditate potrivit prevederilor legale în vigoare.

(7) Persoanele juridice de drept public și privat deținătoare de ICIN sau care au în responsabilitate ICIN trebuie să notifice CNSC și CERT-RO, în termen de 48 de ore, cu privire la orice modificare intervenită în regimul juridic al ICIN, respectiv în configurația acesteia.

Art.20. - (1) Persoanele juridice de drept public sau privat care dețin sau au în responsabilitate ICIN, cu excepția celor prevăzute la art.10 alin(1) și (2) au următoarele obligații:

a) să stabilească și să aplice măsuri pentru asigurarea rezilienței infrastructurilor cibernetice proprii sau aflate în responsabilitate;

b) să întocmească planul de securitate al ICIN, precum și planuri de acțiune proprii corespunzătoare fiecărui nivel de alertă cibernetică;

c) să efectueze anual auditări de securitate cibernetică sau să permită efectuarea unor astfel de auditări la solicitarea motivată a autorităților competente potrivit prezentei legi;

d) să constituie structuri sau să desemneze persoane responsabile cu prevenirea, identificarea și reacția la incidentele cibernetice;

e) să implementeze soluții pentru gestionarea permanentă a evenimentelor din spațiul cibernetic care pot afecta securitatea infrastructurii cibernetice și să genereze alerte cu privire la acestea;

f) să aplice politicile de securitate prevăzute prin cerințele minime stabilite conform dispozițiilor prezentei legi;

g) să ia măsuri pentru prevenirea incidentelor cibernetice și să reducă, după caz, impactul acestora asupra utilizatorilor sau beneficiarilor ICIN;

h) să notifice imediat, după caz, CNSC, CERT-RO, ANCOM sau autoritățile desemnate, în condițiile legii, în domeniul securității cibernetice cu privire la riscurile și incidentele cibernetice care, prin efectul lor, pot aduce prejudicii de orice natură utilizatorilor sau beneficiarilor serviciilor lor;

i) să respecte modalitatea de notificare, precum și datele și informațiile care însoțesc în mod obligatoriu notificarea, stabilite potrivit alin.(2) .

(2) În vederea îndeplinirii obligațiilor prevăzute la alin. (1) lit. a), f) și g), Ministerul pentru Societatea Informațională, ANCOM sau autoritățile desemnate, în condițiile legii, în domeniul securității cibernetice, stabilesc cerințele minime de securitate cibernetică, modalitatea de notificare, precum și datele și informațiile care însoțesc în mod obligatoriu notificarea, care se aprobă prin ordine sau decizii emise în termen de 90 de zile de la intrarea în vigoare a prezentei legi, de conducătorii autorităților sau instituțiilor publice respective, publicate în Monitorul Oficial al României, Partea I.

Art.21. - (1) În funcție de tipul și natura riscurilor și incidentelor cibernetice, autoritățile competente să recepționeze notificarea prevăzută la art. 20 alin. (1) lit. h), acționează potrivit competențelor stabilite prin lege.

(2) Deținătorii de ICIN, care au transmis notificări conform art. 20 alin. (1) lit. h), au următoarele obligații:

a) să aplice planurile prevăzute la art. 20 alin. (1) lit. b);

b) să mențină legătura cu autoritățile competente, potrivit legii, informând despre evoluția incidentului și modul în care acesta este gestionat;

c) să permită autorităților competente, potrivit legii, să intervină pentru identificarea și analizarea cauzelor incidentelor cibernetice, respectiv pentru înlăturarea sau reducerea efectelor incidentelor cibernetice;

d) să rețină și să asigure integritatea datelor referitoare la incidentele cibernetice pentru o perioadă de 6 luni de la data notificării, cu respectarea principiului confidențialității și să le pună la dispoziția autorităților competente, în condițiile legii.

(3) Obligațiile prevăzute la alin. (2), se aplică tuturor deținătorilor de infrastructuri cibernetice implicate în incidentul notificat.

(4) Dispozițiile prezentului articol nu se aplică în cazul instituțiilor și autorităților publice prevăzute la art. 10 alin.(1) și (2).

Art.22. - (1) CERT-RO asigură colectarea și evaluarea datelor și informațiilor cu privire la incidente și atacuri cibernetice notificate, potrivit art. 20 alin.(1) lit.h), de deținătorii de ICIN, persoanelor juridice de drept privat, ia măsuri reactive de primă urgență pentru asigurarea integrității datelor și remedierea situației de fapt.

(2) CERT-RO informează CNSC cu privire la notificările primite și la situațiile în care a luat măsuri reactive de primă urgență, potrivit alin.(1).

Art.23. - (1) Securitatea infrastructurilor cibernetice deținute sau administrate de furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului se realizează în condițiile Ordonanței de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012, precum și în conformitate cu dispozițiile prezentei legi.

(2) Pentru îndeplinirea obiectivelor prezentei legi, ANCOM poate emite decizii.

(3) În vederea realizării scopului prezentei legi, ANCOM îi revin următoarele atribuții:

a) verifică respectarea de către furnizorii de rețele publice sau servicii de comunicații electronice destinate publicului care dețin și/sau administrează ICIN a dispozițiilor art. 20 alin.(1) lit. a)- g);

b) exercită controlul respectării dispozițiilor art. 20 de către furnizorii de rețele publice sau servicii de comunicații electronice destinate publicului care dețin și/sau administrează ICIN.

(4) În cazul furnizorilor de rețele publice sau servicii de comunicații electronice destinate publicului care dețin și/sau administrează ICIN, notificarea prevăzută la art. 20 alin. (1) lit. h) se transmite către ANCOM.

(5) ANCOM va transmite CNSC, conform unor proceduri convenite de comun acord, în cel mult 24 de ore, informațiile relevante privind atacurile, amenințările și incidentele, care prin efectul lor, pot compromite sau aduce atingere securității naționale și apărării țării sau care afectează serviciile de interes public ori serviciile societății informaționale determinând producerea unor prejudicii grave statului român ori cetățenilor acestuia.

(6) În implementarea prevederilor prezentei legi, ANCOM va constitui și va operaționaliza o structură specializată de securitate cibernetică, de tip CERT.

CAPITOLUL IV

Apărarea cibernetică

Art.24. - (1) Apărarea cibernetică cuprinde ansamblul de măsuri și activități adoptate și desfășurate de autoritățile competente pentru protejarea infrastructurilor cibernetice destinate apărării naționale și a infrastructurilor cibernetice naționale care sunt critice pentru misiunile NATO și UE.

(2) Infrastructurile cibernetice destinate apărării naționale și măsurile privind apărarea cibernetică a acestora se stabilesc în termen de 60 de zile de la intrarea în vigoare a prezentei legi și se actualizează periodic prin hotărâre a CSAT.

Art.25. - (1) Activitățile prevăzute la art.24 alin.(1) se planifică și se desfășoară de autoritățile competente 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 la prezenta lege, măsuri de apărare cibernetică și răspund de executarea acestora, fiecare în domeniul său de activitate.

Art.26. - (1) Ministerul Apărării Naționale împreună cu celelalte autorități și instituții publice din Sistemul Național de Apărare, Ordine Publică și Securitate Națională 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 COSC.

CAPITOLUL V

Regimul sancționator și dispoziții procedurale

Art.27. - (1) Monitorizarea și controlul aplicării prevederilor prezentei legi se asigură, potrivit competențelor stabilite prin lege, de către:

a) Camera Deputaților și Senat, Administrația Prezidențială, Guvern, CSAT, precum și instituțiile și autoritățile publice prevăzute la art. 10 alin. (1) și (2), pentru infrastructurile cibernetice proprii sau aflate în responsabilitate;

b) Serviciul Român de Informații pentru infrastructurile cibernetice proprii sau aflate în responsabilitate, precum și pentru deținătorii de ICIN persoane juridice de drept public;

c) Ministerul pentru Societatea Informațională, respectiv ANCOM, după caz, pentru deținătorii de ICIN, persoane juridice de drept privat.

(2) În vederea exercitării atribuțiilor prevăzute la alin.(1), conducătorii autorităților desemnează persoanele abilitate să desfășoare activități de control care, în baza și în limitele împuternicirii aprobate au dreptul:

a) să solicite declarații sau orice documente necesare pentru efectuarea controlului;

b) să facă inspecții, inclusiv inopinate, la orice instalație, incintă sau infrastructură, destinate ICIN, cu respectarea prevederilor legale în vigoare;

c) să primească, la cerere sau la fața locului, informații sau justificări.

Art.28. - Constituie contravenții următoarele fapte:

a) nerespectarea de către deținătorii de infrastructuri cibernetice a obligației privind adoptarea și punerea în aplicare a politicii de securitate cibernetică care să respecte cerințele minime de securitate stabilite potrivit prezentei legi, prevăzute la art. 16 lit. a);

b) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației de notificare cu privire la modificările de regim juridic, respectiv de configurație a ICIN, prevăzute la art.19 alin.(7);

c) încălcarea de către deținătorii de sau cei care au în responsabilitate ICIN obligațiilor prevăzute la art. 20 alin. (1), lit. c)-e) privind efectuarea de auditări de securitate cibernetică, constituirea de structuri sau desemnarea de persoane responsabile cu prevenirea, identificarea și reacția la incidente cibernetice, respectiv implementarea de soluții pentru gestionarea evenimentelor din spațiul cibernetic și generarea de alerte cu privire la acestea;

d) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației privind aplicarea politicilor de securitate, prevăzută la art.20 alin.(1) lit.f);

e) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației de notificare impuse potrivit art. 20 alin. (1) lit. h);

f) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a cerințelor minime de securitate cibernetică, a modalității de notificare, precum și

datele și informațiile care însoțesc în mod obligatoriu notificarea obligației prevăzută la art. 20 alin. (1) lit. i);

g) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN care au transmis notificarea în condițiile prevăzute la art. 20 alin. (2) a obligațiilor de aplicare a planurilor de securitate sau de acțiune, respectiv de a permite autorităților competente să intervină, precum și a obligației de a reține și asigura integritatea datelor referitoare la incidentele cibernetice, prevăzute la art. 21 alin. (2) lit. c) și lit. d);

h) încălcarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației de a informa autoritățile competente potrivit legii despre evoluția incidentului cibernetic notificat și cu privire la modul în care acesta este gestionat, stabilită de prevederile prevăzută la art. 21 alin. (2) lit. b);

i) nerespectarea de către furnizorii de rețele publice sau servicii de comunicații electronice destinate publicului, deținători de ICIN sau care au în administrare infrastructuri cibernetice a cerințelor minime stabilite de ANCOM, a modalității de notificare, precum și a datelor și informațiilor care însoțesc în mod obligatoriu notificarea, în temeiul obligației prevăzute art. 23 alin. (3) lit.a) precum și refuzul de a se supune controlului potrivit art.23 alin.(3) lit.b);

j) nerespectarea obligației de notificare a clientilor de către deținătorii de infrastructuri cibernetice, furnizori de servicii de internet, prevăzută la art. 18.

Art.29. - Contravențiile prevăzute la art. 28 se sancționează, astfel:

a) cu amendă de la 500 lei la 5.000, pentru săvârșirea contravențiilor prevăzute la art. 28 lit. a) și h)- j);

b) cu amendă de la 1.000 la 10.000 lei, pentru săvârșirea contravențiilor prevăzute la art. 28 lit. b) – g).

Art.30. - Constatarea contravențiilor și aplicarea sancțiunilor se realizează, potrivit competențelor legale, de către persoane împuternicite din cadrul :

a) Ministerul pentru Societatea Informațională, în cazul persoanelor juridice de drept privat, pentru contravențiile prevăzute la art. 28 lit. a) – h);

b) ANCOM în situația în care contravențiile prevăzute la art. 28 lit. a) sunt săvârșite de persoanele juridice prevăzute la art. 23 alin. (1), precum și pentru contravențiile prevăzute la art. 28 lit. i) și j);

c) autoritățile și instituțiile publice prevăzute la art.27 alin.(1) lit. a) pentru contravențiile prevăzute la art.28 lit.b) – h) ce vizează infrastructurile cibernetice proprii sau aflate în responsabilitate.d) Serviciul Român de Informații, pentru contravențiile prevăzute la art.28 lit. b) – h).

Art.31. Contravențiilor prevăzute la art.28 le sunt aplicabile dispozițiile Ordonanței Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.

CAPITOLUL VII

Dispoziții finale

Art.32. - (1) La nivelul persoanelor juridice de drept public, fondurile necesare organizării și desfășurării activității în condițiile prezentei legi se asigură de la bugetul de stat, din venituri proprii și 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.33. - (1) Prezenta lege intră în vigoare la 30 de zile de la publicarea în Monitorul Oficial al României, Partea I.

(2) În termen de 90 de zile de la data publicării în Monitorul Oficial al României, Partea I, Guvernul aprobă:

a) la propunerea Serviciului Român de Informații, normele metodologice prevăzute la art.15 alin.(2);

b) la propunerea Ministerului pentru Societatea Informațională, normele metodologice prevăzute la art.17 alin.(1) lit.b).