MINISTERUL COMUNICAȚIILOR
ȘI PENTRU
SOCIETATEA INFORMAȚIONALĂ

CONSILIUL ECONOMIC ȘI SOCIAL
Înregistrat nr. 1460
Data 8.04.2016

Nesecret

Cabinet Ministru

Ministerul Comunicațiilor și pentru Societatea Informațională
CABINET MINISTRU
INTRARE/IEȘIRE Nr 1347
Ziua 07 Luna 04 Anul 2016

Către: Consiliul Economic și Social (CES)
În atenția: Domnului Președinte Florian Costache

Stimate Domnule Președinte,

Vă transmitem anexat, în copie, în vederea formulării de observații și propuneri, proiectul de Lege privind securitatea cibernetică a României.

Cu deosebită considerație,

MINISTRU
MARIUS-RAUL BOSTAN

Bulevardul Libertatii nr.14, Sector 5, București Cod Postal 050706
Tel.: +4 021 400 11 90 Fax: +021 311 41 31 email: cabinetministru@msinf.ro
www.comunicatii.gov.ro

1560
8.04.2016

EXPUNERE DE MOTIVE

Secţiunea 1: Titlul proiectului de act normativ LEGE PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI	
Secţiunea a 2-a: Motivul emiterii actului normativ	
1. Descrierea situaţiei actuale	Evoluția recentă a atacurilor cibernetice din țara noastră situează amenințarea cibernetică printre cele mai dinamice amenințări actuale la adresa securității naționale. România este cu certitudine vizată de entități ostile active în mediul virtual, fiind necesară adoptarea unor măsuri organizatorice și de reglementare în vederea creșterii nivelului securității cibernetice și a capabilităților de a face față unor atacuri caracterizate de un nivel foarte ridicat al impactului și al probabilității de manifestare, care vizează domenii de importanţă strategică pentru un stat, respectiv afaceri externe şi interne, apărare şi securitate naţională, resurse energetice, cercetare şi mass-media, prin exfiltrarea de informaţii confidenţiale. Agresiunile cibernetice sunt caracterizate de un nivel ridicat de risc, cu tendințe de evoluție în creștere a impactului și probabilității de materializare, vizând cu predilecție infrastructurile cibernetice ale instituțiilor publice sau care susțin furnizarea de servicii publice ori de interes public, domeniul economiei digitale, prin compromiterea confidenţialităţii datelor gestionate de platforme de comerț electronic și fraudarea clienților acestora. În aceste condiții, asigurarea securității cibernetice trebuie să constituie, o preocupare majoră a tuturor actorilor implicați, atât la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării unor politici coerente în domeniu, cât și la nivelul entităților private interesate de protejarea propriului patrimoniu și a proprietății private. O prioritate națională din acest punct de vedere o reprezintă adoptarea unui act normativ în domeniul *Securității Cibernetice a României*, care să permită: —stabilirea cadrului general de reglementare a activităților în domeniul securității cibernetice; —definirea obligațiilor ce revin autorităților și instituțiilor publice, persoanelor juridice deținătoare de infrastructuri cibernetice și furnizorilor de servicii prevăzuți de lege, în scopul protejării infrastructurilor cibernetice; —asigurarea cadrului general de cooperare pentru realizarea securității cibernetice, prin constituirea Sistemului Național de Securitate Cibernetică, drept mecanism de cooperare interinstituțională. Problematica securității cibernetice, ca parte a securității naționale, a devenit prioritară, astfel ca sunt necesare demersuri de reglementare pentru dezvoltarea mecanismelor de apărare cibernetică. La nivel global, frecvența, amploarea, complexitatea și gravitatea atacurilor cibernetice au crescut concomitent cu diversificarea țintelor

	acestora. Riscul de atacuri cibernetice este, în continuare, dificil de estimat, iar tot mai mulți actori internaționali dezvoltă instrumente puternice în spațiul cibernetic, pe care le folosesc ofensiv pentru a-și apăra interesele economice, politice și ideologice. În situația neadoptării prezentului act normativ, estimăm că țara noastră nu-și va putea armoniza demersurile pe dimensiunea securității cibernetice cu cele ale partenerilor săi din UE și NATO, demersuri necesare unei abordări coerente și eficiente a provocărilor și oportunităților spațiului cibernetic. În lipsa acestei legi, statul român nu va dispune de pârghiile necesare diminuării vulnerabilităților de securitate cibernetică și asigurării apărării cibernetice, în scopul reducerii la un nivel acceptabil a riscurilor la adresa securității infrastructurilor cibernetice. Prezentul proiect a fost întocmit cu luarea în considerare a criticilor aduse prin Decizia nr.17/2015 a Curții Constituționale asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României.
2. Schimbări preconizate	România a conștientizat necesitatea creșterii nivelului de securitate cibernetică națională și de racordare la inițiativele organismelor internaționale din care face parte. Relevantă este aprobarea prin Hotărârea de Guvern nr. 271/2013 a Strategiei de Securitate Cibernetică a României, care stabilește obiectivele și direcțiile de acțiune, fiind necesară adoptarea acestui proiect pentru stabilirea cadrului conceptual, organizatoric și acțional necesar asigurării securității cibernetice. România se va racorda la realitățile internaționale, prin adoptarea prezentei legi, armonizându-și cadrul legislativ cu demersurile similare ale statelor europene, pentru abordarea eficientă a oportunităților spațiului cibernetic și a provocărilor distructive la adresa acestuia, cu consecințe majore inclusiv prin crearea de prejudicii materiale consistente în domenii vitale de activitate la nivel național. În esență, proiectul vizează adoptarea de măsuri necesare pentru asigurarea securității infrastructurilor cibernetice. Obiectul de reglementare îl reprezintă creșterea nivelui de protecție a infrastructurilor cibernetice în raport cu evoluțiile tehnologice și aplicațiile IT&C pentru a putea contracara folosirea acestor tehnologii de ultimă generație în atacurile cibernetice. Prezentul act normativ contribuie la asigurarea protejării, în spațiul cibernetic, a dreptului cetățenilor la viață intimă, familială și privată. Legea privind securitatea cibernetică a României nu vizează protecția datelor cu caracter personal, această problematică fiind reglementată prin Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare, însă proiectul de act normativ va contribui,prin măsurile tehnice și organizatorice

	reglementate, la protejarea infrastructurilor cibernetice care prelucreaza acest date cu caracter personal. În vederea asigurării unor garanții ale dreptului la viață intimă, familială și privată al cetățenilor, prezenta lege prevede obligația deținătorilor de infrastructuri cibernetice de a nu permite accesul la datele de conținut din infrastructurile cibernetice deținute sau aflate în competență, în lipsa unei înștiințări scrise din partea autorităților abilitate, privind existența unei autorizații emise de judecător. Totodată, persoana care se consideră vătămată într-un drept al său prin aplicarea acestei legi poate contesta măsurile dispuse de autoritatea de control. Actul normativ contribuie și la creșterea capacității de reacție la incidentele cibernetice, prin impunerea de cerințe minime de securitate cibernetică și prin stabilirea principiilor de acțiune pentru gestionarea incidentelor de securitate cibernetică. În vederea identificării disfuncțiilor și vulnerabilităților, precum și a furnizării unor soluții de remediere a acestora, legea instituie auditul 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. Furnizorii de servicii de securitate care realizează audit de securitate pentru infrastructurile cibernetice de interes național (ICIN) au obligația de a se înregistra la MCSI, potrivit normelor aprobate prin ordin al ministrului. Legea definește ICIN-urile ca fiind infrastructuri cibernetice deținute fie de persoane juridice de drept privat - care susțin servicii publice sau de interes public, ori servicii ale societății informaționale, fie de autorități și instituții publice, a căror afectare aduce atingere securității naționale, sau prejudicii grave statului român ori cetățenilor acestuia. În calitatea sa de autoritate de reglementare, potrivit legii, MCSI întocmește Catalogul ICIN, având în vedere informațiile transmise de către autoritățile competente referitoare la: - descrierea generală a ICIN; - rolul și funcționalitățile asigurate de ICIN; - arhitectura ICIN; - tipuri și număr de utilizatori; - fluxuri informaționale susținute, precum și dinamica datelor stocate/ prelucrate, capacitatea de stocare/ prelucrare. Legea instituie un ansamblu organizat de măsuri tehnice și procedurale destinate prevenirii și contracarării activităților de natură să afecteze securitatea cibernetică la nivel național, denumit Sistem Național de Alertă Cibernetică. Instituirea nivelurilor de alertă cibernetică, precum și trecerea de la un nivel la altul se aprobă de către CSAT, la propunerea COSC. Deținătorii de infrastructuri cibernetice au obligația să sprijine autoritățile competente pentru implementarea măsurilor corespunzătoare fiecărui nivel de alertă cibernetică.

	Adoptarea acestei legi stabileşte definirea unei terminologii unitare în domeniul securităţii cibernetice şi a unui cadru armonizat de acţiune a autorităţilor şi instituţiilor publice cu responsabilităţi şi capabilităţi în domeniul securităţii cibernetice. Prin definiţiile utilizate, s-a urmărit o configurare explicită a conceptelor şi noţiunilor din domeniul securităţii cibernetice, ţinând cont de noutatea reglementării, în vederea unei înţelegeri corecte a acestora, pentru evitarea interpretărilor eronate, inclusiv în cadrul actelor normative subsecvente şi pentru proiectarea unui cadru acţional coerent din partea deţinătorilor de infrastructuri cibernetice. Evoluţia ultimilor ani a făcut ca problematica securităţii cibernetice, ca parte a securităţii naţionale, să devină prioritară, demersul actual de reglementare fiind necesar pentru dezvoltarea mecanismelor naţionale de apărărare cibernetică. Actul normativ stabileşte cadrul juridic privind organizarea şi desfăşurarea activităţilor din domeniul securităţii cibernetice a României şi asigurarea protejării drepturilor şi libertăţilor fundamentale ale cetăţenilor în spaţiul cibernetic. Proiectul urmăreşte totodată educarea societăţii civile în domeniu, precum şi crearea unui cadru de cooperare optim între autorităţile statului şi societatea civilă, aceste deziderate reprezentând puncte esenţiale în obţinerea unui climat de securitate şi încredere în spaţiul cibernetic.
3. Alte informaţii	Dat fiind ritmul rapid de evoluţie a problematicii, legea va fi analizată şi revizuită permanent, în vederea adaptării continue la provocările şi oportunităţile generate de un mediu de securitate în permanentă schimbare şi la evoluţiile înregistrate în dezvoltarea tehnologiilor informaţionale pe plan mondial.
Secţiunea a 3-a: Impactul socio-economic al proiectului de act normativ	
1. Impactul macro-economic	Prezentul act normativ va contribui la preîntâmpinarea unor potenţiale prejudicii aduse statului român prin stabilirea unor linii de acţiune necesare prevenirii şi combaterii atacurilor cibernetice.
1^1 Impactul asupra mediului concurenţial şi domeniului ajutoarelor de stat	Proiectul de act normativ nu se referă la acest subiect.
2.Impactul asupra mediului de afaceri	Prezentul act normativ va contribui la consolidarea securităţii cibernetice şi la creşterea nivelului de securitate cibernetică, va duce la dezvoltarea comerţului electronic şi, în general, la utilizarea Internetului în condiţii de siguranţă sporită.
2^1. Impactul asupra sarcinilor administrative	Proiectul de act normativ nu se referă la acest subiect.
2^2. Impactul asupra întreprinderilor mici şi mijlocii	Proiectul de act normativ nu se referă la acest subiect.
3. Impactul social	Prezentul act normativ va contribui la conştientizarea publicului cu privire la natura multivalentă a spaţiului cibernetic şi la creşterea

	încrederii populației în utilizarea Internetului.
4. Impactul asupra mediului	Prezentul act normativ nu are impact asupra mediului.
5. Alte informații	Nu au fost identificate.

Secțiunea a 4-a: Impactul financiar asupra bugetului general consolidat, atât pe termen scurt, pentru anul curent, cât și pe termen lung (pe 5 ani)

-mii lei -

Indicatori	Anul curent	Următorii 4 ani				Media pe 5 ani
	2016	2017	2018	2019	2020	
1	2	3	4	5	6	7
1. Modificări ale veniturilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) impozit pe profit						
(ii) impozit pe venit						
b) bugete locale:						
(i) impozit pe profit						
c) bugetul asigurărilor sociale de stat:						
(i) contribuții de asigurări						
2. Modificări ale cheltuielilor bugetare, plus/minus, din care:						
a) buget de stat, din acesta:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
b) bugete locale:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
c) bugetul asigurărilor sociale de stat:						
(i) cheltuieli de personal						
(ii) bunuri și servicii						
3. Impact financiar, plus/minus, din care:						
a) buget de stat						
b) bugete locale						
4. Propuneri pentru acoperirea creșterii cheltuielilor bugetare						
5. Propuneri pentru a compensa reducerea veniturilor bugetare						
6. Calcule detaliate privind fundamentarea modificărilor veniturilor și/sau cheltuielilor bugetare						
7. Alte informații	Proiectul de act normativ nu are impact pe termen scurt și mediu asupra bugetului autorităților și instituțiilor publice cu competențe legale în domeniul securității cibernetice. Centrul Național de Securitate Cibernetică (CNSC) va prelua atribuțiile Centrului Național Cyberint, entitate constituită și					

	organizată în cadrul Serviciului Român de Informații, potrivit unor Hotărâri CSAT. Astfel, funcționarea CNSC nu implică alocări bugetare suplimentare, posturile fiind deja prevăzute și încadrate cu personal specializat.
Secțiunea a 5-a: Efectele proiectului de act normativ asupra legislației în vigoare	
1. Măsuri normative necesare pentru aplicarea prevederilor proiectului de act normativ: a) acte normative în vigoare ce vor fi modificate sau abrogate, ca urmare a intrării în vigoare a proiectului de act normativ; b) acte normative ce urmează a fi elaborate în vederea implementării noilor dispoziții.	Urmează să fie elaborate norme metodologice de aplicare și acte subsecvente prezentei legi.
1¹. Compatibilitatea proiectului de act normativ cu legislația în domeniul achizițiilor publice	Proiectul de act normativ nu se referă la acest subiect.
2. Conformitatea proiectului de act normativ cu legislația comunitară în cazul proiectelor ce transpun prevederi comunitare.	Proiectul de act normativ nu se referă la acest subiect.
3. Măsuri normative necesare aplicării directe a actelor normative comunitare	Proiectul de act normativ nu se referă la acest subiect.
4. Hotărâri ale Curții de Justiție a Uniunii Europene	Proiectul de act normativ nu se referă la acest subiect.
5. Alte acte normative și/sau documente internaționale din care decurg angajamente	Proiectul de act normativ nu se referă la acest subiect.
6. Alte informații	Nu au fost identificate.
Secțiunea a 6-a: Consultările efectuate în vederea elaborării proiectului de act normativ	
1. Informații privind procesul de consultare cu organizații non-guvernamentale, institute de cercetare și alte organisme implicate	Elaborarea proiectului de act normativ nu a necesitat astfel de consultări.
2. Fundamentarea alegerii organizațiilor cu care a avut loc consultarea, precum și a modului în care activitatea acestor organizații este legată de obiectul proiectului de act normativ	Elaborarea proiectului de act normativ nu a necesitat astfel de consultări.
3. Consultările organizate cu autoritățile administrației publice locale, în situația în care proiectul de act normativ are ca obiect activități ale acestor autorități, în condițiile Hotărârii Guvernului nr. 521/2005 privind procedura de consultare a	Elaborarea proiectului de act normativ nu a necesitat astfel de colaborări.

structurilor asociative ale autorităţilor administraţiei publice locale la elaborarea proiectelor de acte normative.	
4. Consultările desfăşurate în cadrul consiliilor interministeriale, în conformitate cu prevederile Hotărârii Guvernului nr. 750/2005 privind constituirea consiliilor interministeriale permanente	Elaborarea proiectului de act normativ nu a necesitat astfel de consultări.
5. Informaţii privind avizarea de către:	
a) Consiliul Legislativ	Proiectul de act normativ necesită avizul CSAT precum şi avizul Consiliului Legislativ.
b) Consiliul Suprem de Apărare a Ţării	
c) Consiliul Economic şi Social	
d) Consiliul Concurenţei	
e) Curtea de Conturi	
6. Alte informaţii	Nu au fost identificate.
Secţiunea a 7-a: Activităţi de informare publică privind elaborarea şi implementarea proiectului de act normativ	
1. Informarea societăţii civile cu privire la necesitatea elaborării proiectului de act normativ	În conformitate cu prevederile Legii nr. 52/2003 privind transparenţa decizională în administraţia publică, cu modificările şi completările ulterioare, proiectul de act normativ a fost afişat pe pagina de internet a Ministerului Comunicaţiilor şi pentru Societatea Informaţională, în vederea acordării posibilităţii cetăţenilor şi reprezentanţilor societăţii civile de a formula propuneri şi observaţii.
2. Informarea societăţii civile cu privire la eventualul impact asupra mediului în urma implementării proiectului de act normativ, precum şi efectele asupra sănătăţii şi securităţii cetăţenilor sau diversităţii biologice.	Proiectul de act normativ nu se referă la acest subiect.
3. Alte informaţii	Nu au fost identificate.
Secţiunea a 8-a: Măsuri de implementare	
1. Măsurile de punere în aplicare a proiectului de act normativ de către autorităţile administraţiei publice centrale şi/sau locale - înfiinţarea unor noi organisme sau extinderea competen-ţelor instituţiilor existente	Proiectul de act normativ nu se referă la acest subiect.
2. Alte informaţii	Nu au fost identificate.

Față de cele prezentate, a fost promovată prezenta Lege privind securitatea cibernetică a României, pe care o supunem spre aprobare.

MINISTRUL COMUNICAŢIILOR ŞI PENTRU SOCIETATEA INFORMAŢIONALĂ,
MARIUS-RAUL BOSTAN

AVIZĂM FAVORABIL,

VICEPRIM-MINISTRU, MINISTRUL ECONOMIEI, COMERȚULUI ȘI RELAȚIILOR CU MEDIUL DE AFACERI
COSTIN BORC

VICEPRIM-MINISTRU, MINISTRUL DEZVOLTĂRII REGIONALE ȘI ADMINISTRAȚIEI PUBLICE
VASILE DÎNCU

MINISTRUL AFACERILOR INTERNE,
PETRE TOBĂ

MINISTRUL APĂRĂRII NAŢIONALE,
MIHNEA IOAN MOTOC

MINISTRUL AFACERILOR EXTERNE,
LAZĂR COMĂNESCU

MINISTRUL FINANŢELOR PUBLICE,
ANCA DANA DRAGU

DIRECTORUL
SERVICIULUI ROMÂN DE INFORMAŢII,
EDUARD HELLVIG

DIRECTORUL
SERVICIULUI DE INFORMAŢII EXTERNE,
MIHAI RĂZVAN UNGUREANU

DIRECTORUL
SERVICIULUI DE TELECOMUNICAŢII SPECIALE,
MARCEL OPRIŞ

DIRECTORUL
SERVICIULUI DE PROTECŢIE ŞI PAZĂ,
LUCIAN-SILVAN PAHONŢU

PREŞEDINTELE AUTORITĂŢII NAŢIONALE PENTRU ADMINISTRARE ŞI REGLEMENTARE ÎN COMUNICAŢII,
CĂTĂLIN MARINESCU

DIRECTORUL GENERAL AL OFICIULUI REGISTRULUI NAŢIONAL AL INFORMAŢIILOR SECRETE DE STAT,
MARIUS PETRESCU

MINISTRUL SĂNĂTĂȚII
PATRICHIU ACHIMAȘ CADARIU

MINISTRUL TRANSPORTURILOR
DAN MARIAN COSTESCU

MINISTRUL EDUCAȚIEI NAȚIONALE ȘI CERCETĂRII ȘTIINȚIFICE
ADRIAN CURAJ

MINISTRUL ENERGIEI
VICTOR VLAD GRIGORESCU

PREȘEDINTELE AUTORITĂȚII NAȚIONALE DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL
ANCUȚA GIANINA OPRE

MINISTRUL JUSTIȚIEI,
RALUCA ALEXANDRA PRUNĂ

LEGE PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI

CAPITOLUL I - DISPOZIŢII GENERALE

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

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

Art. 2 - Prezenta lege se aplică:

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

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

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

δ) furnizorilor de servicii de găzduire internet;

ε) furnizorilor de servicii de securitate cibernetică.

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

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

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

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

d) atac cibernetic - acţiune desfăşurată în spaţiul cibernetic cu intenţia de a afecta securitatea cibernetică;

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

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

g) cerințe minime de securitate cibernetică - măsuri de natură organizatorică, tehnică sau procedurală destinate asigurării confidențialității, integrității, disponibilității, autenticității și nonrepudierii datelor stocate și prelucrate în cadrul unei infrastructuri cibernetice.

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 care perturbă funcționarea uneia sau mai multor infrastructuri cibernetice și ale cărui consecințe sunt de natură a afecta securitatea cibernetică;

n) infrastructuri cibernetice - infrastructuri de tehnologia informației, constând în sisteme informatice sau 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 cibernetice, incluzând conținutul informațional, procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta;

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

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

a) asigurarea, prin introducerea unor măsuri de securitate cibernetică, a unui nivel crescut de protecție a infrastructurilor cibernetice și, implicit, a datelor cu caracter personal gestionate de către deținătorii de infrastructuri cibernetice;

b) garantarea dreptului la viață intimă, familială și privată al cetățenilor în relația deținătorilor de infrastructuri cibernetice cu autoritățile în domeniu prevăzute la art. 9;

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

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

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

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

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

CAPITOLUL II - SISTEMUL NAȚIONAL DE SECURITATE CIBERNETICĂ

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

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

(3) În exercitarea 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 cibernetice 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 organismele de coordonare sau de conducere constituite, la nivel național, pentru managementul situațiilor de urgență, a acțiunilor in situații de criză în domeniul ordinii publice, pentru prevenirea și combaterea terorismului și pentru apărarea națională.

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

a) Ministerul Comunicațiilor și pentru Societatea Informațională, cu rol de autoritate de reglementare și control al implementării măsurilor tehnice și organizatorice privind securitatea infrastructurilor cibernetice, cu excepția celor aflate în domeniul de competență, activitate și responsabilitate al instituțiilor prevăzute la lit. d) și e);

b) Centrul Național de Răspuns la Incidente de Securitate Cibernetică, denumit în continuare CERT-RO, 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 rețelelor publice de comunicații electronice și a serviciilor 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 tehnice și organizatorice 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).

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) Pentru infrastructurile cibernetice de interes național, cerințele minime de securitate cibernetică au în vedere următoarele categorii de activități vizând securitatea cibernetică:

a) managementul drepturilor de acces;
b) conștientizarea și instruirea utilizatorilor;
c) jurnalizarea și asigurarea trasabilității activităților în cadrul infrastructurii cibernetice;
d) testarea și evaluarea securității cibernetice;
e) managementul configurațiilor infrastructurii cibernetice;
f) asigurarea disponibilității infrastructurii cibernetice și a continuității funcționării resurselor critice ale acesteia;
g) managementul identificării și autentificării utilizatorilor;
h) răspunsul la incidente de securitate cibernetică;
i) mentenanța infrastructurii cibernetice;
j) managementul suporturilor de memorie externă;
k) asigurarea protecției fizice a infrastructurii cibernetice;
l) realizarea planurilor de securitate;
m) asigurarea securității personalului;
n) analizarea și evaluarea riscurilor de securitate cibernetică;
o) procedurarea activităților de achiziție a sistemelor și serviciilor;
p) asigurarea protecției produselor și serviciilor aferente infrastructurii cibernetice;
q) managementul vulnerabilităților și alertelor de securitate cibernetică.

(2) Cerințele minime de securitate cibernetică pentru infrastructurile cibernetice, altele decât infrastructurile cibernetice de interes național, sunt stabilite de către autoritățile prevăzute la art. 11 în baza următoarelor categorii de activități de asigurare a securității cibernetice:

a) managementul accesului la infrastructura cibernetică;
b) conștientizarea și instruirea utilizatorilor;
c) asigurarea protecției la nivel software și hardware a infrastructurii cibernetice;
d) analiza si evaluarea riscurilor de securitate cibernetică;
e) protecția sistemelor de comunicații aferente infrastructurii cibernetice.

Art. 13- (1) Autoritățile prevăzute de art. 9 lit. b) - e) au următoarele obligații:

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

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

c) să asigure colectarea notificărilor cu privire la incidente de securitate cibernetică provenite de la deţinătorii infrastructurilor cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate;

d) să asigure evaluarea datelor şi informaţiilor cu privire la incidente şi atacuri cibernetice la adresa infrastructurilor cibernetice, aflate în domeniul lor de competenţă, activitate sau responsabilitate;

e) să informeze deţinătorii de infrastructuri cibernetice aflate în domeniul 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;

g) să acorde sprijin deţinătorilor de infrastructuri cibernetice din zona 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, pentru îmbunătăţirea capacităţilor deţinătorilor de infrastructuri cibernetice;

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

k) să coopereze şi să-şi comunice reciproc date 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 propriilor competenţe, inclusiv pentru ridicarea nivelului de alertă cibernetică.

(2) Autorităţile prevăzute la alin. (1) pot constitui structuri specializate în realizarea de audit de securitate cibernetică şi pot constitui şi operaţionaliza structuri specializate de securitate cibernetică de tip CERT.

Art. 14 - Autorităţile prevăzute la art. 9 lit. e), pentru infrastructurile cibernetice aflate în domeniul lor de activitate şi responsabilitate, 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. 15 - (1) În procesul identificării infrastructurilor cibernetice de interes naţional în vederea întocmirii Catalogului ICIN, deţinătorii de infrastructuri cibernetice au obligaţia de a furniza autorităţilor de la art. 9 datele tehnice necesare.

(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 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 arhitectura acestora.

(6) Datele tehnice 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.

(7) Datele tehnice necesare pentru întocmirea Catalogului ICIN, prevăzute la alin. (1), nu vor conține date care pot aduce atingere drepturilor și libertăților cetățenești ori intereselor legitime ale unor terțe entități implicate.

Art. 16 - 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 administrației publice;

b) infrastructuri cibernetice destinate susținerii serviciilor publice;

c) infrastructuri cibernetice din sectoarele energetic, alimentare cu apă, alimentație, sănătate, transporturi, industrie chimică și nucleară, spațiu și cercetare;

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 şi alertă;

i) infrastructuri cibernetice care asigură servicii de securitate cibernetică;

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

k) infrastructuri cibernetice pentru navigaţie, radiolocaţie şi identificare;

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

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

Art. 17- (1) Evaluarea potenţialului impact asupra securităţii infrastructurilor cibernetice prin compromiterea confidenţialităţii, integrităţii, disponibilităţii, autenticităţii sau a non-repudierii datelor, resurselor şi serviciilor se realizează pe baza următoarelor criterii:

a) prejudiciul adus intereselor statului român;

b) prejudiciul produs în planul securităţii naţionale;

c) afectarea vieţii şi siguranţei cetăţeanului;

d) afectarea încrederii utilizatorilor în serviciile oferite;

e) prejudiciul material sau financiar;

f) întreruperea furnizării serviciului afectat;

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

h) afectarea relaţiilor internaţionale în care România este angrenată;

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

j) interdependenţa cu alte infrastructuri cibernetice.

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

CAPITOLUL III - ASIGURAREA SECURITĂŢII CIBERNETICE

Art. 18- (1) Sistemul Naţional de Alertă Cibernetică, denumit în continuare SNAC, este un ansamblu organizat de măsuri tehnice şi procedurale destinate prevenirii şi contracarării activităţilor de natură să afecteze securitatea cibernetică la nivel naţional.

(2) În cadrul SNAC, stările de ameninţare reflectă gradul de risc pentru securitatea cibernetică şi sunt identificate prin niveluri de alertă cibernetică. Acestea pot fi instituite pentru întreg teritoriul naţional, pentru o zonă geografică delimitată,

pentru un anumit domeniu de activitate sau pentru una sau mai multe persoane juridice de drept public sau privat.

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

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

(5) Persoanele juridice de drept public sau privat deţinători de infrastructuri cibernetice de interes naţional elaborează planuri de acţiune proprii, corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligaţia să le pună în aplicare la instituirea unui nivel de alertă cibernetică, conform normelor cu privire la organizarea şi funcţionarea SNAC, aprobate prin Hotărâre a Guvernului.

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

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

a) nivel de alertă 1 - verde-scăzut;

b) nivel de alertă 2 - galben-moderat;

c) nivel de alertă 3 - portocaliu-ridicat;

d) nivel de alertă 4 - roşu-critic.

Art. 19 - (1) Deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) adoptă măsuri organizatorice şi tehnice pentru:

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

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

c) managementul incidentelor de securitate cibernetică;

d) prevenirea accesului neautorizat la infrastructurile cibernetice;

e) prevenirea diseminării datelor deţinute la nivelul infrastructurilor cibernetice către alte persoane decât cele autorizate să cunoască conţinutul acestora.

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

a) implementarea unui sistem de management al riscului;

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

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

Art. 20 - Deţinătorii de infrastructuri cibernetice prevăzuţi 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 informări din partea autorităților competente cu privire la identificarea unor incidente de securitate cibernetică sau vulnerabilități și atacuri cibernetice identificate la nivelul infrastructurilor cibernetice deținute;

c) să solicite asistență de specialitate autorităților competente potrivit prezentei legi, pentru asigurarea securității cibernetice 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 realizeze managementul incidentelor de securitate cibernetică, prin utilizarea resurselor proprii, prin contractarea unor servicii de securitate cibernetică sau solicitarea sprijinului autorităților competente.

Art. 21- (1) Deținătorii de infrastructuri cibernetice prevăzuți la art. 2 lit. a) - c) au următoarele obligații:

a) să asigure implementarea cerințelor minime de securitate cibernetică;

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

c) să se asigure că datele tehnice referitoare la configurarea și protecția infrastructurilor cibernetice sunt diseminate exclusiv persoanelor autorizate să le cunoască;

d) să nu permită accesul la datele de conținut din infrastructurile cibernetice 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 cibernetice.

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

a) să efectueze auditări de securitate cibernetică, potrivit standardelor și specificațiilor europene sau internaționale, aplicabile în domeniul securității cibernetice;

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;

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

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

Art. 22 - (1) Furnizorii de servicii de comunicaţii electronice destinate publicului au obligaţia de a-şi informa utilizatorii şi abonaţii de îndată ce au fost sesizaţi de autoritatea competentă, dar nu mai târziu de 24 de ore din momentul în care au fost sesizaţi de autorităţile competente potrivit prezentei legi, cu privire la situaţiile în care sistemele informatice utilizate de aceştia au fost implicate în atacuri cibernetice şi de a recomanda măsurile necesare în vederea restabilirii condiţiilor normale de funcţionare.

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

Art. 23 - (1) Furnizorii de servicii de securitate cibernetică ce desfăşoară activităţi pe teritoriul României au obligaţia să notifice autorităţile competente, deîndată dar nu mai târziu de 24 de ore, cu privire la identificarea unor ameninţări sau vulnerabilităţi critice a căror manifestare poate afecta infrastructura cibernetică a deţinătorului sau a unor terţi.

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

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

Art. 24- (1) Furnizorii de servicii de găzduire internet care desfăşoară activităţi pe teritoriul României au obligaţia să acorde sprijin autorităţilor competente, respectiv organelor de urmărire penală, pentru punerea în aplicare, potrivit legii, a oricărui act de autorizare a restrângerii temporare a exerciţiului drepturilor şi libertăţilor persoanelor, emis de judecător.

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

(3) Persoanele care sunt chemate să acorde 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 IV - GESTIONAREA INCIDENTELOR DE SECURITATE CIBERNETICĂ

Art. 25- (1) Notificarea incidentelor de securitate cibernetică se transmite în modalitatea stabilită de autoritatea competentă şi trebuie să conţină, în mod obligatoriu, următoarele elemente:

a) elementele de identificare ale infrastructurii cibernetice afectate;

b) descrierea incidentului;

c) perioada de desfăşurare a incidentului;

d) impactul incidentului.

(2) Pentru gestionarea incidentelor de securitate cibernetică, 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 incidentele și atacurile cibernetice pe care le gestionează, cu asigurarea anonimizării datelor cu caracter personal deținute.

(3) Notificarea prevăzută la alin. (1) și datele tehnice transmise în condițiile 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. 26 - 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. 27- 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. 28 - (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. 29 - 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. 30- (1) Apărarea cibernetică cuprinde ansamblul de măsuri şi activităţi adoptate şi desfăşurate de autorităţile cu atribuţii în domeniul apărării ţării şi securităţii naţionale pentru protejarea infrastructurilor cibernetice destinate apărării naţionale şi a infrastructurilor cibernetice naţionale care susţin activităţile NATO şi UE.

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

Art. 31 - (1) Activităţile prevăzute la art. 30 alin. (1) se planifică şi se desfăşoară de autorităţile cu atribuţii în domeniul apărării ţării şi securităţii naţionale în strânsă legătură cu activităţile privind apărarea naţională şi planificarea apărării, conform legii şi potrivit obligaţiilor asumate de România la nivel internaţional.

(2) Autorităţile şi instituţiile publice au obligaţia de a identifica şi implementa, în condiţiile legii şi în termen de 180 de zile de la intrarea în vigoare a prezentei legi măsuri de apărare cibernetică şi răspund de executarea acestora, fiecare în domeniul său de activitate.

Art. 32 - (1) Ministerul Apărării Naţionale împreună cu celelalte autorităţi şi instituţii publice cu atribuţii în domeniul apărării ţării şi securităţii naţionale asigură, din timp de pace, integrarea într-o concepţie unitară a activităţilor privind apărarea cibernetică desfăşurate de forţele armate participante la acţiunile de apărare a ţării în caz de agresiune armată, la instituirea stării de asediu, declararea stării de mobilizare sau a stării de război.

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

CAPITOLUL VI - CONTROL ŞI SANCŢIUNI

Art. 33 - (1) Autorităţile prevăzute la art. 9, lit. a), d) şi e) au atribuţii de control asupra aplicării prevederilor prezentei legi de către deţinătorii infrastructurilor cibernetice aflate în domeniul lor de competenţă, activitate sau responsabilitate.

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

Art. 34 - (1) Nerespectarea prevederilor prezentei legi atrage răspunderea contravenţională, potrivit dispoziţiilor legale în vigoare.

(2) Constatarea contravenţiilor şi aplicarea sancţiunilor se realizează potrivit prevederilor Cap. II din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al

contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

(3) Procesul-verbal de contravenţie poate fi contestat în termen de 30 de zile de la data înmânării sau comunicării acestuia, conform Cap. IV din Ordonanţa Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.

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

Art. 35 - (1) La nivelul instituţiilor publice, aşa cum sunt definite în Legea nr. 500/2002 privind finanţele publice, cu modificările şi completările ulterioare, fondurile necesare organizării şi desfăşurării activităţii în condiţiile prezentei legi se asigură de la bugetul de stat, din venituri proprii sau din alte surse legal constituite, anual, potrivit legii.

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

Art. 36 - Constituie contravenţii următoarele fapte dacă nu au fost săvârşite în astfel de condiţii încât să fie considerate, potrivit legii, infracţiuni:

a) nerespectarea de către deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) a obligaţiilor prevăzute la art. 21 alin. (1), lit. a) şi c);

b) încălcarea de către deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) a obligaţiilor prevăzute la art. 21 alin.(1), lit. d), e) şi f);

c) nerespectarea de către deţinătorii de infrastructuri cibernetice de interes naţional a obligaţiei prevăzute la art. 19 alin. (2), precum şi a obligaţiilor prevăzute la art. 21, alin.(2), lit. a) - e);

d) nerespectarea de către furnizorii de servicii de comunicaţii electronice destinate publicului a obligaţiei prevăzute la art. 22;

e) încălcarea de către furnizorii de servicii de securitate cibernetică ce îşi desfăşoară activitatea pe teritoriul României a obligaţiei prevăzute la art. 23, alin. (1);

f) nerespectarea de către deţinătorii de infrastructuri cibernetice a obligaţiei de notificare prevăzute la art. 21 alin. (1) lit. b) în condiţiile stabilite de art. 25 alin. (1).

Art. 37 - Contravenţiile prevăzute la art. **36** se sancţionează astfel:

a) cu amendă de la 1.000 lei la 10.000 lei, pentru săvârşirea contravenţiilor prevăzute la art. 36 lit. a), e) şi f);

b) cu amendă de la 2.000 lei la 20.000 lei, pentru săvârşirea contravenţiilor prevăzute la art. 36, lit. b) - d).

CAPITOLUL VII - DISPOZIŢII FINALE

Art. 38 - (1) Prezenta lege nu aduce atingere prevederilor Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, cu modificările și completările ulterioare precum și celor ale Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare.

(2) În termen de 90 zile de la intrarea în vigoare a prezentei legi, Ministerul Comunicațiilor și pentru Societatea Informațională cu sprijinul autorităților prevăzute la art. 9 lit. b) - e) inițiază și supune aprobării Guvernului organizarea și funcționarea Sistemului Național de Alertă Cibernetică.

(3) În termen de 90 zile de la intrarea în vigoare a prezentei legi, Ministerul Comunicațiilor și pentru Societatea Informațională supune aprobării Guvernului Programul național destinat managementului riscului în domeniul securității cibernetice.

(4) Catalogul infrastructurilor cibernetice de interes național prevăzut la art.15 alin. (2) se aprobă prin hotărâre a Guvernului în termen de 180 de zile de la intrarea în vigoare a prezentei legi și se va revizui periodic.

(5) Cerințele minime de securitate prevăzute la art. 11, alin.1 se aprobă prin decizia președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații, în termen de 90 de zile de intrarea în vigoare a prezentei legi.

(6) Cerințele minime de securitate prevăzute la art. 10 și 11 alin.(2) se aprobă prin hotărâre a Guvernului, în termen de 90 zile de la intrarea în vigoare a prezentei legi.

(7) Implementarea de către deținătorii de infrastructuri cibernetice a cerințelor minime de securitate cibernetică se realizează în termen de maximum un an de la publicarea acestora de către autoritățile prevăzute la art. 10 și art. 11 alin. (1) și (2) din prezenta lege.