PARLAMENTUL ROMÂNIEI
Nr. L580 29.12.2014

ROMÂNIA
CURTEA CONSTITUŢIONALĂ
CABINETUL PREŞEDINTELUI

Palatul Parlamentului
Calea 13 Septembrie nr. 2, Intrarea B1, Sectorul 5, 050725 Bucureşti, România
Telefon: (+40-21) 313 25 31 *Fax: (+40-21) 312 54 80*
Internet : http://www.ccr.ro *E-mail: pres@ccr.ro*

Dosar nr.1419A/2014

CURTEA CONSTITUŢIONALĂ
REGISTRATURA JURISDICŢIONALĂ
6195 23 DEC 2014
Nr...../.....

SENAT
PREŞEDINTE
Nr. I 1915
Data 23 XII 2014

Domnului
Călin Constantin Anton POPESCU-TĂRICEANU
Preşedintele Senatului

L580/2014

În conformitate cu dispoziţiile art.16 alin.(2) din Legea nr.47/1992 privind organizarea şi funcţionarea Curţii Constituţionale, vă trimitem, alăturat, în copie, sesizarea formulată de un număr de 69 de deputaţi aparţinând Grupului parlamentar al Partidului Naţional Liberal din Camera Deputaţilor cu privire la neconstituţionalitatea prevederilor Legii privind securitatea cibernetică a României.

Vă adresăm rugămintea de a ne comunica punctul dumneavoastră de vedere până la data de 7 ianuarie 2015, ţinând seama de faptul că dezbaterile Curţii Constituţionale vor avea loc la data de 21 ianuarie 2015.

Vă asigurăm de deplina noastră consideraţie.

p. Preşedinte,

judecător Petre LĂZĂROIU

CURTEA CONSTITUȚIONALĂ

Dosar nr. 1419A/2014

CURTEA CONSTITUȚIONALĂ
REGISTRATURA JURISDICȚIONALĂ
6188 23 DEC 2014
Nr...../.....

PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR

Cabinet Secretar General

București, 23.12.2014
Nr.2/6103

Domnului

AUGUSTIN ZEGREAN
Președintele Curții Constituționale

Stimate domnule Președinte,

În temeiul dispozițiilor art.15, alin.(4) din Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale, republicată, vă trimitem alăturat sesizarea formulată de 69 deputați aparținând Grupului Parlamentar al PNL din Camera Deputaților, referitoare la neconstituționalitatea Legii privind securitatea cibernetică a României.

Cu deosebita considerație,

SECRETAR GENERAL

Adrian Cristian PĂUCIU

PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR
2/6103/23.12.2014

GRUP PARLAMENTAR
PARTIDUL NAȚIONAL LIBERAL
Nr. 3c-15/511
14 12 23

ROMANIA

Parlamentul României
Camera Deputaţilor

Grupul Parlamentar al Partidului Național Liberal

telefon: (021) 414 10 70 **fax: (021) 414 10 72** **email:pnl@cdep.ro**

Bucureşti, 23 decembrie 2014

C ă t r e,

Secretariatul General al Camerei Deputaților

Domnului Adrian PANCIU

Domnule Secretar General,

În temeiul prevederilor art. 146 lit. a) din Constituție, şi în baza art. 15, alin (1) din Legea 47/1992 privind organizarea şi funcționarea Curții Constituționale, vă înaintăm ***Sesizarea*** la Curtea Constituțională cu privire la ***Legea privind securitatea cibernetică a României,*** adoptată de Senat, în calitate de Cameră decizională, la data de 19.12.2014.

Lider Grup PNL Camera Deputaților,

Deputat Ludovic ORBAN

PARLAMENTUL ROMÂNIEI Grupul Parlamentar - NAȚIONAL LIBERAL - CAMERA DEPUTAȚILOR

PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR
SECRETAR GENERAL
Nr. ____ / ____

ROMANIA

Parlamentul României
Camera Deputaților

Grupul Parlamentar al Partidului Național Liberal

telefon: (021) 414 10 70 **fax: (021) 414 10 72** **email:pnl@cdep.ro**

Domnului Augustin ZEGREAN
Președintele Curții Constituționale

Stimate domnule Președinte,

În temeiul art. 146 lit. a) din Constituția României, al art. 11 lit. a) raportat la art. 15 alin. (1) din Legea 47/1992 privind organizarea și funcționarea Curții Constituționale, republicată, deputații Partidului Național Liberal, înscriși pe lista anexată, formulează prezenta

SESIZARE DE NECONSTITUȚIONALITATE

prin care vă adresăm solicitarea de a constata neconstituționalitatea ***Legii privind securitatea cibernetică a României,*** adoptată de Senat, în calitate de Cameră decizională, la data de 19.12.2014.

Ne motivăm această sesizare prin următoarele:

1. **Legea privind securitatea cibernetică a României este neconstituțională** deoarece încalcă principiul legalității afirmat de Curtea Constituțională ca fiind fundamental pentru buna funcționare a statului de drept, **cu consecința nerespectării dispozițiilor art. 1 alin.(3) din Constituția României, care afirmă că *„România este stat de drept...”* și ale art.1 alin. (5) din Constituția României, conform căruia *„în România respectarea Constituției, a supremației sale și a legilor este obligatorie”.***

Textul legii nu respectă, în opinia noastră, prevederile art. 6 din *Legea 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative*, astfel încât *„(1)Proiectul de act normativ trebuie să instituie reguli necesare, suficiente și posibile care să conducă la o cât mai mare stabilitate și eficiență legislativă. Soluțiile pe care le cuprinde trebuie să fie temeinic fundamentate, luându-se în considerare interesul social, politica legislativă a statului român și cerințele corelării cu ansamblul reglementărilor interne și ale armonizării legislației naționale cu legislația comunitară și cu tratatele internaționale la care România este parte, precum și cu jurisprudența Curții Europene a Drepturilor Omului. (la data 18-Mar-2011 Art. 6, alin. (1) din capitolul I modificat de Art. I, punctul 1. din* ***Legea 29/2011*** *)”.*

Așadar, sunt încălcate prevederile art.1 alin. (5) din Constituție conform căruia *„în România respectarea Constituției, a supremației sale și a legilor este obligatorie”.*

Prin aceasta lege se introduc foarte multe confuzii și condiționări pentru cei implicați, în special pentru deținătorii de infrastructuri cibernetice care vor trebui să se supună unor constrângeri generate de unele instituții ale statului, cele mai multe parte ale sistemului național de securitate al țării, aspect care poate genera neplăceri la nivelul relațiilor cu statele democratice europene, în special pe zona de

respectare și apărare a drepturilor și libertăților fundamentale ale cetățeanului protejate prin deciziile Curții Europene a Drepturilor Omului și Constituția României;

La art. 1 al Legii mai sus sesizate se constată că acest act normativ implică doar obligații pentru cei în drept și nu stabilește și drepturile acestora. Deci, se începe cu un dezechilibru fundamental în stabilirea firului logic și teleologic al normei juridice în cauză, prin introducerea de prevederi cu caracter de coerciție pentru persoanele vizate și unele excepții pentru autoritățile implicate în aplicarea acestei legi.

La art. 2 se constată că există o enumerare a entităților/persoanelor cărora li se aplică legea, în esență tuturor deținătorilor de infrastructuri cibernetice, dar fără a se preciza și situațiile în care apar intermediari ce pun la dispoziție astfel de infrastructuri, ce se întamplă în cazul unor infrastructuri inactive neoperaționale, obligațiile pe care le au acționarii unor persoane juridice, fondatorii unor asociații, fundații sau organizații neguvernamentale care dețin astfel de infrastructuri.

2. Legea privind securitatea cibernetică a României are probleme fundamentale de concepție, propunând o serie de măsuri cu efect limitativ asupra dreptului la viață privată în zona digitală și încalcă în mod evident reglementările europene discutate pe subiectul securității informației. Astfel, sunt încălcate prevederile **articolului 26, alin.(1) din Legea fundamentală**: *"Autoritățile publice respectă și ocrotesc viața intimă, familială și privată".*

3. Articolul 23 din Constituție - *(1) Libertatea individuală și siguranța persoanei sunt inviolabile* și **articolul 28** - *Secretul scrisorilor, al telegramelor, al altor trimiteri poștale, al convorbirilor telefonice și al celorlalte mijloace legale de comunicare este inviolabil* sunt încălcate în opinia noastră, prin subminarea gravă

a dreptului la viață privată al cetățenilor și încălcarea secretului corespondenței. Astfel, reținem din textul legii, următoarele articole:

Articolul 17 stipulează că deținătorii de sisteme cibernetice (adică persoanele juridice care au un calculator trebuie să „permită accesul la date" autorităților stipulate în lege (SRI, MApN, MAI, ORNISS, SIE, STS, SPP, CERTRO și ANCOM). Accesul se face la simpla „solicitare motivată", în condițiile în care astăzi, conform Codului de procedură penală, **orice acces la sistemele informatice (unde sunt stocate datele informatice) se poate face doar cu autorizarea unui judecător.** Mai mult, accesul la datele de trafic este momentan imposibil pentru organele legal abilitate tocmai deoarece Curtea Constituțională a considerat, prin decizia 440/2014, că un atare acces **nu respectă principiile respectării vieții private.** Cu acest prilej, Curtea a constat următoarele: *"Legea nr. **82/2012** privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. **506/2004** privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice reprezintă transpunerea în legislația națională a Directivei **2006/24/CE** a Parlamentului European și a Consiliului din 15 martie 2006 privind păstrarea datelor generate sau prelucrate în legătură cu furnizarea serviciilor de comunicații electronice accesibile publicului sau de rețele de comunicații publice și de modificare a Directivei **2002/58/CE**. Însă Directiva **2006/24/CE** a fost declarată nevalidă prin Hotărârea Curții de Justiție a Uniunii Europene din 8 aprilie 2014, pronunțată în cauzele conexate C-293/12 - Digital Rights Ireland Ltd împotriva Minister for Communications, Marine and Natural Resources și alții - și C-594/12 - Karntner Landesregierung și alții. Prin hotărârea menționată instanța europeană a constatat că directiva analizată încalcă dispozițiile art. 7, art. 8 și art. 52 alin. (1)*

din Carta drepturilor fundamentale a Uniunii Europene." Totodată, amintim că în **Decizia nr. 461 din 16 septembrie 2014 asupra obiecției de neconstituționalitate a dispozițiilor Legii pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice** și Curtea a reținut faptul că, *"deși nici Constituția și nici jurisprudența Curții Constituționale nu interzic stocarea preventivă, fără o ocazie anume, a datelor de trafic și de localizare, modalitatea prin care sunt obținute și stocate datele necesare pentru identificarea utilizatorilor serviciilor de comunicații electronice pentru care plata se face în avans, respectiv a utilizatorilor conectați la puncte de acces la internet nu respectă condițiile impuse de principiul proporționalității, nu oferă garanții care să asigure confidențialitatea datelor cu caracter personal, aducând atingere însăși esenței drepturilor fundamentale referitoare la viață intimă, familială și privată si la secretul corespondenței, precum și libertății de exprimare."*

Prin aceasta lege în mod mascat se restrâng drepturi și libertăți ale cetățeanului prin permiterea accesului la infrastructura cibernetică și la datele conținute în baza unei simple motivări comunicate de instituțiile abilitate si nominalizate prin lege fara existenta unei aprobari judecatoresti conform Codului de procedura penala si conform cerintelor adoptate de Curtea Constitutionala prin Deciziile 440/2014 si 461/2014, deci lege nu este armonizata la cerintele Curtii Constitutionale a României.

Articolul 10 stipulează că Serviciul Român de Informații este desemnat autoritate națională în domeniul securității cibernetice, calitate în care asigură coordonarea tehnică, organizarea și executarea activităților ce privesc securitatea cibernetică a României. În vreme ce Uniunea Europeană propune în directiva NIS ca instituțiile care se ocupă de domeniul securității cibernetice să fie „organisme civile, care să funcționeze integral pe baza controlului democratic, și nu ar trebui să

desfășoare activități în domeniul informațiilor", Parlamentul României acordă acces nelimitat și nesupravegheat la toate datele informatice deținute de persoane de drept public și privat unor instituții care nu îndeplinesc niciuna din condițiile de mai sus.

Amintim faptul că, **în 2014, Curtea Constituțională a României** a mai constatat neconstituționalitatea **Legii "Big Brother"** și a **Legii cartelelor prepay și a Wi-Fi-ului** cu buletinul. Acestea erau acte normative în ton cu recent adoptata *Lege a securității cibernetice* și care încălcau grav dreptul la viață privată și protecția datelor personale, instituind un regim de supraveghere informatică total nedemocratic, sub pretextul protejării securității naționale. Mai mult, textul de lege care face obiectul prezentei sesizări nu prevede care sunt modalitățile de control asupra celor care utilizează informațiile obținute, precum și faptul că nu exista garanția că datele nu pot fi folosite și în alte scopuri.

Faptul că în această vară Curtea Constituțională a declarat neconstituționale două legi care, în esență, încălcau aceleași drepturi ca și Legea la care ne referim, constituie un motiv suplimentar, serios pentru o dezbatere reală a implicațiilor Legii securității cibernetice și, într-un cadru mai larg, a echilibrului dintre **drepturile individuale** și securitatea națională pe care România trebuie sa îl asigure prin sistemul său de legi.

4. Legea încalcă dispozițiile art. 148, alin (2) și următoarele, din Constituția României, prin netranspunerea corectă reglementărilor comunitare în materie. Totodată, considerăm că art. 17 alin. 1 lit. a) nu este conform cu jurisprudența Curții Europene de Justiție. În primul rând nu se precizează exact ce date necesită a fi deținute, iar cadrul în care se solicită aceste date nu prezintă suficiente garanții procesuale. A se vedea în acest sens cauzele reunite C-293/12 și C-594/12.

Totodată, considerăm că Legislația românească trebuie să țină seama de legislația europeană în materie și trebuie să fie în concordanță cu următoarele directive europene: 2006/24/EG, 2002/58/EG, sancționate de CJUE C-301/06.

CEDO a invalidat în aprilie 2014 directiva deoarece încălca drepturile fundamentale ale omului.

De asemenea, **Art. 17 alin. 1 lit. b)** nu e conform cu jurisprudența Curții Europene de Justiție. Pentru o astfel de informare este necesară o monitorizare perpetuă a tuturor persoanelor, aspect ce creează o obligație disproporționată pentru subiecții vizați și implică totodată încălcarea drepturilor persoanelor monitorizate fără să existe în legătură cu acestea o suspiciune în legătură cu eventualitatea comiterii vreunei infracțiuni. A se vedea în acest sens cauza **Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL** (C-70/10).

Legea contravine din multe puncte de vedere și propunerii de Directivă NIS (Network &Information Security) care pornește de la scopul protecției datelor personale ale cetățenilor și nu de la crearea de noi atribuții pentru serviciile secrete. În timp ce Directiva NIS are drept scop protejarea sistemelor informatice și a datelor informatice ale cetățenilor, Legea, în forma adoptată, reprezintă un cec în alb care poate fi folosit de serviciile de informații pentru a controla orice persoană de drept privat (SRL, SA, PFA,ONG) care deține un sistem informatic (adică orice calculator sau smart-phone). Potențialul pentru abuzuri este, astfel, enorm. Acesta decurge din nenumăratele ambiguități prezente în lege, începând de la definirea vagă a „deținătorilor de sisteme informatice" și continuând cu obligațiile ce le revin celor care cad sub incidența legii.

Întreaga arhitectura a actului normativ este de natura a permite încalcarea drepturilor fundamentale ale omului, fara a exista un remediu eficient impotriva unor astfel de incalcari.

Asa cum a aratat constant in jurisprudenta sa, Curtea Europeana a Drepturilor Omului consideră că „un sistem de supraveghere secretă destinat apărării siguranței naționale implică riscul de a submina, ba chiar de a distruge, democrația sub pretextul apărării ei "(***Klass şi alţii împotriva Germaniei).***

În cazul nostru, posibilitatea accesării fără mandat a datelor electronice provenind de la orice computer, indiferent de proprietarul său (pentru că datele trec prin serverele societăților ce oferă accesul la internet) este o ingerință nejustificată în dreptul la protecția corespondenței, adică în dreptul la viață privată, drept garantat de art. 26 și 28 din Constituție.

O astfel de ingerință nu numai că nu este necesară într-o societate democratică, dar ea are tocmai efectul contrar: subminează esența societății democratice.

Astfel, sub pretextul protecției împotriva atacurilor cibernetice, orice fel de date pot fi accesate la bunul plac al puterii executive, fără existența vreunui control al societății civile.

Mai mult, așa cum arată CEDO, deși într-o societate democratică limitele protecției drepturilor fundamentale pot fi reduse în cazul unor pericole deosebite (terorism, infracțiuni transfrontaliere) probele obținute prin aceste proceduri nu pot fi folosite în cazurile de drept comun (cele care nu implică protecția siguranței naționale, așa cum este ea definită prin lege), acolo unde garanțiile procedurale trebuie să fie strict respectate. Or, legea atacată nu instituie nicio interdicție de utilizare a datelor în orice alt mod decât cel necesar pentru protecția în fața atacurilor cibernetice, situație ce poate submina garanția unui proces echitabil.

Mai mult, legea nu prevede nicio interdicție cu privire la interceptarea comunicațiilor protejate prin legi speciale. Astfel, dreptul la apărare este încălcat, orice comunicații legale și legitime între avocat și acuzat putând fi interceptate fără

mandat și în secret, situație incompatibilă cu dispozițiile art. 24 alin. 1 din Constituție.

Pe cale de consecință vă rugăm, onorată Curte, să constatați că ***Legea privind securitatea cibernetică a României*** **este neconformă cu prevederile art. 1, alin. (3) și (5), art. 23, 24, 26 și 28 din Constituție, fiind astfel neconstituțională.**

În drept, ne motivăm sesizarea pe dispozițiile art. 55 alin.(1) din *Regulamentul activităților comune ale Camerei Deputaților și Senatului* și ale art. 15 alin.(1) și (2) din *Legea 47/1992 privind organizarea și funcționarea Curții Constituționale.*

Tabel cu deputații PNL pentru susținerea sesizării la Curtea Constituțională cu privire Legea ...PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI.....

.....

Nr.	Nume	SEMNĂTURA
.	ALEXE COSTEL	
2.	ALEXE FLORIN-ALEXANDRU	
3.	ALMĂJANU MARIN	
4.	ANDRONACHE GABRIEL	
5.	ANUŞCA ROXANA-FLORENTINA	
6.	BĂIŞANU ŞTEFAN-ALEXANDRU	
7.	BERCI VASILE	
8.	BUDURESCU DANIEL-STAMATE	
9.	BUICAN CRISTIAN	
10.	CALIMENTE MIHĂIȚĂ	
11.	CAZAN MIRCEA-VASILE	
12.	CHERECHEŞ FLORICA	
13.	CHIRTEŞ IOAN-CRISTIAN	
14.	CIUBOTARU LUCIAN-MANUEL	
15.	CIURARIU FLORIN	
16.	COCEI ERLAND	
17.	COSTIN GHEORGHE	
18.	COZMANCIUC CORNELIU-MUGUREL	

52
17

19.	CRĂCIUNESCU GRIGORE	
20.	CRISTIAN HORIA	
21.	CUPŞA IOAN	
22.	DOBOŞ ANTON	
23.	DOBRE VICTOR-PAUL	
24.	DOBRINESCU TRAIAN	
25.	DOLHA MIRCEA	
26.	DOLHA NECHITA-STELIAN	
27.	DONȚU MIHAI AUREL	
28.	DRAGOMIR GHEORGHE	
29.	GHEORGHE DANIEL	
30.	GIREADĂ DUMITRU-VERGINEL	
31.	GORGHIU ALINA-ŞTEFANIA	
32.	GRECEA MARIA	
33.	HĂRĂU ELEONORA-CARMEN	
34.	HORGA VASILE	
35.	IANE DANIEL	
36.	ISPIR RALUCA-CRISTINA	
37.	LUPU MIHAI	
38.	MANEA VICTOR-GHEORGHE	
39.	MARCU VIORICA	
40.	MIRONESCU RĂZVAN HORIA	

41.	MOTREANU DAN-ŞTEFAN	
42.	NICOARĂ ROMEO	
43.	NICOLĂESCU GHEORGHE-EUGEN	
44.	NICOLESCU THEODOR-CĂTĂLIN	
45.	NISTOR GHEORGHE-VLAD	
46.	ORBAN LUDOVIC	
47.	OROS NECHITA-ADRIAN	
48.	PALĂR IONEL	
49.	PARDĂU DUMITRU	
50.	POCORA CRISTIANA-ANCUȚA	
51.	POPA OCTAVIAN MARIUS	
52.	RAEȚCHI OVIDIU ALEXANDRU	
53.	ROMAN PETRE	
54.	ROŞCA MIRCEA	
55.	RUSU VALENTIN	
56.	SĂPUNARU NINI	
57.	SCARLAT GEORGE	
58.	SIMEDRU DAN-CORIOLAN	
59.	ŞOPTICĂ COSTEL	
60.	ŞTIRBU GIGEL-SORINEL	
61.	STROE IONUȚ MARIAN	
62.	SURDU RALUCA	

63.	SURUGIU IULIAN-RADU	
64.	TĂMÂIAN IOAN	
65.	THUMA HUBERT PETRU ŞTEFAN	
66.	ŢÎMPĂU RADU-BOGDAN	
67.	UIOREANU ELENA-RAMONA	
68.	VARGA LUCIA-ANA	
69.	VARGA VASILE	
70.	VOICU MIHAI-ALEXANDRU	
71.	ZAMFIR DANIEL-CĂTĂLIN	
72.	ZLATI RADU	

PARLAMENTUL ROMÂNIEI

CAMERA DEPUTAȚILOR **SENAT**

L E G E

privind securitatea cibernetică a României

Parlamentul României adoptă prezenta lege

CAPITOLUL I
Dispoziții generale

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

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 cibernetice, denumite în continuare *deținători de infrastructuri cibernetice*.

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

a) cunoaşterea, prevenirea şi contracararea amenințărilor şi atacurilor, precum şi prin diminuarea vulnerabilităților infrastructurilor cibernetice, în scopul gestionării riscurilor la adresa securității acestora;

b) prevenirea şi combaterea criminalităţii informatice;

c) apărarea cibernetică.

(2) Prevenirea criminalităţii informatice se realizează în condiţiile Legii nr.161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificările şi completările ulterioare. Combaterea criminalităţii informatice se efectuează de organele judiciare în condiţiile legislaţiei penale şi procesual penale.

Art.4.- Securitatea cibernetică vizează:

a) realizarea rezilienţei infrastructurilor cibernetice;

b) creşterea capacităţii de reacţie la incidentele cibernetice şi diminuarea impactului acestora asupra resurselor şi serviciilor infrastructurilor cibernetice;

c) asigurarea protecţiei datelor gestionate prin intermediul infrastructurilor cibernetice;

d) asigurarea nivelului de încredere necesar pentru dezvoltarea societăţii informaţionale şi a mediului de afaceri în spaţiul cibernetic;

e) realizarea accesului egal şi nediscriminatoriu al persoanelor la informaţii şi servicii publice oferite prin intermediul infrastructurilor cibernetice;

f) guvernanţa participativă, democratică şi eficientă a spaţiului cibernetic;

g) responsabilizarea deţinătorilor de infrastructuri cibernetice pentru asigurarea securităţii cibernetice;

h) asigurarea climatului de exercitare neîngrădită a drepturilor şi libertăţilor fundamentale ale persoanelor în spaţiul cibernetic.

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

a) *ameninţare cibernetică* - circumstanţa sau evenimentul care constituie un pericol potenţial la adresa securităţii cibernetice;

b) *apărare cibernetică* - acţiunile desfăşurate în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva ameninţărilor asupra infrastructurilor cibernetice destinate apărării naţionale;

c) *atac cibernetic* - acţiunea ostilă de natură să afecteze securitatea cibernetică;

d) *audit de securitate cibernetică* - evaluarea sistematică, detaliată, măsurabilă şi tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, precum şi emiterea de recomandări pentru minimizarea riscurilor identificate;

e) *incident de securitate cibernetică* - evenimentul survenit în spațiul cibernetic, ale cărui consecințe afectează securitatea cibernetică;

f) *eveniment survenit în spațiul cibernetic* - acțiunea desfășurată în spațiul cibernetic, care are drept consecință modificarea stării infrastructurilor cibernetice;

g) *infrastructuri cibernetice* - infrastructurile din domeniul tehnologiei informației și comunicații, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice;

h) *infrastructuri cibernetice de interes național* - 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;

i) *managementul identității* - metodele de validare a identității persoanelor, când acestea accesează anumite infrastructuri cibernetice;

j) *managementul riscului* - procesul 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;

k) *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;

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

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

n) *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;

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

p) *vulnerabilitate în spațiul cibernetic* - slăbiciunea în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare;

r) *furnizor de servicii de securitate cibernetică* - orice persoană juridică, română sau străină, care are ca obiect de activitate prestarea de servicii în domeniul securității cibernetice către terți.

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

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

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

d) 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 Serviciului Român de Informații 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 opereționalizeze 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) Centrul Național de Răspuns la Incidente de Securitate Cibernetică, denumit în continuare 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 şi integrează date şi informaţii obţinute de autorităţile şi instituţiile publice componente ale SNSC în scopul stabilirii, întreprinderii sau propunerii măsurilor ce se impun pentru asigurarea securităţii cibernetice;

d) asigură colectarea şi identificarea evenimentelor survenite în spaţiul cibernetic;

e) generează avertizări pentru deţinătorii de infrastructuri cibernetice şi ICIN cu privire la posibile incidente de securitate cibernetică şi emite recomandări cu privire la modalitatea de acţiune;

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

g) transmite autorităţilor şi instituţiilor publice competente din cadrul SNSC datele şi informaţiile necesare punerii în aplicare a măsurilor specifice de acţiune corespunzătoare fiecărui nivel de alertă cibernetică;

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

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

j) asigură colectarea şi evaluarea datelor şi informaţiilor cu privire la incident, propune deţinătorilor de ICIN sau, după caz, ia măsuri reactive de primă urgenţă pentru asigurarea integrităţii datelor şi remedierea situaţiei de fapt, informează, potrivit legii, organele competente pentru investigare şi cercetare sau, după caz, sesizează organele de urmărire penală în caz de atac cibernetic.

(2) Autorităţile şi instituţiile publice din componenţa COSC deleagă un reprezentant în cadrul CNSC.

(3) Cadrul general de organizare şi funcţionare a CNSC se aprobă prin hotărâre a CSAT, la propunerea Serviciului Român de Informaţii, în termen de 60 de zile de la intrarea în vigoare a prezentei legi.

Art.12.- Autorităţile şi instituţiile publice prevăzute la art. 10 alin. (1) şi (2) asigură securitatea infrastructurilor cibernetice proprii sau aflate în responsabilitate potrivit legii şi, în acest sens, exercită următoarele atribuţii generale:

a) elaborează şi implementează politici de securitate şi 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 şi aprobă cadrul specific de reglementare destinat asigurării securităţii cibernetice, cu respectarea cerinţelor stabilite la nivel naţional;

e) contribuie, conform competenţelor legale, la asigurarea securităţii cibernetice în cadrul SNSC;

f) cooperează şi schimbă date şi informaţii referitoare la securitatea cibernetică cu CNSC şi cu celelalte autorităţi şi instituţii publice sau deţinători de infrastructuri cibernetice;

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

h) asigură colectarea şi evaluarea datelor şi informaţiilor cu privire la incidente şi atacuri cibernetice, ia măsuri reactive de primă urgenţă pentru asigurarea integrităţii datelor şi remedierea situaţiei de fapt.

Art.13.- (1) În vederea realizării coerenţei activităţilor din cadrul SNSC, Ministerul pentru Societatea Informaţională asigură legătura COSC cu autorităţile şi instituţiile publice care nu sunt reprezentate în cadrul acestuia iar, prin CERT-RO, cu deţinătorii de infrastructuri cibernetice, persoane juridice de drept privat.

(2) În cazul persoanelor prevăzute la art.23 alin.(1), pentru realizarea dispoziţiilor alin. (1), Ministerul pentru Societatea Informaţională va colabora cu Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii, denumită în continuare ANCOM.

Art.14.- În cadrul SNSC, autorităţile şi instituţiile publice desfăşoară, potrivit competenţelor legale, activităţi pentru asigurarea securităţii cibernetice a României, inclusiv activităţi de informare şi comunicare publică, relaţii publice şi de cooperare internaţională.

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

(2) Organizarea SNAC, măsurile specifice pe care autorităţile şi instituţiile publice competente le implementează pentru fiecare nivel de alertă, precum şi procedura de instituire a nivelurilor de alertă şi cerinţele privind elaborarea planurilor de acţiune se aprobă prin norme metodologice.

(3) În cadrul SNAC, stările de amenințare reflectă gradul de risc pentru securitatea cibernetică şi 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 şi 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 şi 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 cibernetice

Art.16.- (1) Deținătorii de infrastructuri cibernetice 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 şi să implementeze măsurile tehnice şi organizatorice adecvate pentru a gestiona eficient riscurile de securitate în infrastructurile cibernetice proprii sau aflate în responsabilitate;

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

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

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

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

(2) Deţinătorii de infrastructuri cibernetice implementează măsurile tehnice prevăzute la alin.(1) lit.b) prin utilizarea de resurse interne sau prin intermediul unor furnizori de servicii de securitate cibernetică.

Art.17.- (1) Pentru realizarea securităţii cibernetice, deţinătorii de infrastructuri cibernetice au următoarele responsabilităţi:

a) să acorde sprijinul necesar, la solicitarea motivată a Serviciului Român de Informaţii, Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, Serviciului de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază, CERT-RO şi ANCOM, în îndeplinirea atribuţiilor ce le revin acestora şi să permită accesul reprezentanţilor desemnaţi în acest scop la datele deţinute, relevante în contextul solicitării;

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

(2) Deţinătorii de infrastructuri cibernetice pot solicita asistenţă de specialitate autorităţilor şi instituţiilor publice cu atribuţii în domeniul securităţii cibernetice, pentru asigurarea securităţii cibernetice în domeniul lor de activitate.

Art.18.- Deţinătorii de infrastructuri cibernetice, furnizori de servicii de internet, au obligaţia de a-şi notifica clienţii, de îndată, 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 incidente sau atacuri cibernetice şi de a dispune măsurile necesare în vederea restabilirii condiţiilor normale de funcţionare.

Art.19.- (1) La nivel naţional 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 întocmeşte de către Ministerul pentru Societatea Informaţională, cu consultarea COSC, la propunerea CNSC sau, după caz, a CERT- RO, potrivit competenţelor 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 a Guvernului.

(4) La întocmirea catalogului ICIN, Ministerul pentru Societatea Informațională colaborează 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 72 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 și/sau să permită efectuarea unor auditări de securitate cibernetică, la solicitarea motivată a autorităților competente potrivit prezentei legi. Auditările de securitate sunt realizate de către autoritatea națională în domeniul securității cibernetice prevăzută la art.10 alin.(1) sau de către furnizori de servicii de securitate cibernetică;

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.

(3) Persoanele juridice de drept public sau privat care dețin sau au în responsabilitate ICIN îndeplinesc obligațiile prevăzute la alin.(1) lit.a), b), d), e), f), g), h) și i) prin utilizarea de resurse interne sau prin intermediul unor furnizori de servicii de securitate cibernetică.

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 și 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, cu modificările și completările ulterioare, 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) ANCOM va transmite CERT-RO, conform unor proceduri convenite de comun acord în cel mult 24 de ore, informațiile relevante privind atacurile, amenințările și incidentele cu privire la care a fost notificată potrivit art.20 alin.(1) lit.h) de deținătorii de ICIN persoane juridice de drept privat.

(7) 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 Organizației Tratatului Atlanticului de Nord (N.A.T.O.) și Uniunii Europene.

(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 de aplicare a prezentei legi, 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, inclusiv CSAT, Secretariatul General al Guvernului, 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 prevăzute la art.16 lit.a) și d)-f);

b) nerespectarea de către deținătorii de ICIN a obligației prevăzute la art.15 alin(5), (6) și (8) și art.21 alin.(2) lit.a);

c) nerespectarea de către deținătorii de infrastructuri cibernetice a obligației prevăzute la art.15 alin.(7) și la art.17 alin.(1) lit.a) și b);

d) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației prevăzute la art.19 alin.(7);

e) încălcarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligațiilor prevăzute la art.20 alin.(1) lit.b)-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;

f) 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);

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

h) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a cerințelor minime de securitate cibernetică, a modalității de notificare, precum și informațiile care însoțesc în mod obligatoriu notificarea obligației prevăzute la art.20 alin.(1) lit.i);

i) 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 d);

j) 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 prevăzute la art.21 alin.(2) lit.b);

k) 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 la art.23 alin.(3) lit.b);

l) nerespectarea obligației de notificare a clienților 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 lei, pentru săvârşirea contravențiilor prevăzute la art.28 lit.a) şi lit.j) - l);

b) cu amendă de la 1.000 lei la 10.000 lei, pentru săvârşirea contravențiilor prevăzute la art.28 lit.b) - i).

Art.30.- Constatarea contravențiilor şi 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 săvârşite de persoanele juridice prevăzute la art.23 alin.(1), precum şi pentru contravențiile prevăzute la art.28 lit.k) şi l);

c) autoritățile şi 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) Ministerul pentru Societatea Informațională desemnează, prin ordin al ministrului pentru societatea informațională, persoane calificate sau instituții competente aflate în coordonarea sau în subordinea ministerului, 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 şi completări prin Legea nr.180/2002, cu modificările şi completările ulterioare.

CAPITOLUL VII
Dispoziții finale

Art.32.- (1) La nivelul persoanelor juridice de drept public, fondurile necesare organizării şi desfăşurării activității în condițiile prezentei legi se asigură de la bugetul de stat, din venituri proprii şi din alte surse legal constituite anual, potrivit legii.

(2) Pentru buna desfăşurare a activităților 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.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 prezentei legi 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).

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor articolului 75 şi ale articolului 76 alineatul (1) din Constituţia României, republicată.

PREŞEDINTELE
CAMEREI DEPUTAŢILOR

Valeriu Ştefan Zgonea

PREŞEDINTELE
SENATULUI

Călin Popescu-Tăriceanu

Bucureşti,
Nr.