CONFORM CU ORIGINALUL

Parlamentul României
Camera Deputaţilor

Comisia pentru tehnologia informaţiei şi comunicaţiilor

Comisia pentru apărare, ordine publică și siguranță națională

Către,

BIROUL PERMANENT AL CAMEREI DEPUTAŢILOR

Vă înaintăm, alăturat, **RAPORTUL COMUN** asupra **proiectului de Lege privind securitatea cibernetică a României** trimis Comisiei pentru tehnologia informaţiei şi comunicaţii şi Comisiei pentru apărare, ordine publică și siguranță națională, pentru dezbatere şi avizare în fond, cu adresa nr. PLx 263 din 27 mai 2014 şi înregistrat la Comisia pentru tehnologia informaţiei şi comunicaţiilor cu nr.4c-16/16/28.05.2014, iar la Comisia pentru apărare, ordine publică și siguranță națională cu nr.4c-12/151 din 28.05.2014.

În raport cu obiectul şi conţinutul său, proiectul de lege face parte din categoria **legilor organice.**

PREŞEDINTE,
Daniel Vasile Oajdea

PREŞEDINTE,
Ion Mocioalcă

Parlamentul României
Camera Deputaţilor

Comisia pentru tehnologia informaţiei şi comunicaţiilor

Comisia pentru apărare, ordine publică și siguranță națională

RAPORT COMUN
asupra proiectul de Lege privind securitatea cibernetică a României

În conformitate cu prevederile art.95 din Regulamentul Camerei Deputaţilor, republicat, Comisia pentru tehnologia informaţiei şi comunicaţii şi Comisia pentru apărare, ordine publică și siguranță națională au fost sesizate spre dezbatere în fond, prin adresa nr. **PL.x nr.263** din 27 mai 2014, cu **proiectul de Lege privind securitatea cibernetică a României** și înregistrat la Comisia pentru tehnologia informației și comunicațiilor cu nr.4c-16/16/28.05.2014, iar la Comisia pentru apărare, ordine publică și siguranță națională cu nr.4c-12/151 din 28.05.2014.

La întocmirea prezentului raport Comisia a avut în vedere **avizul favorabil** al **Consiliului Legislativ** (nr.513/5.05.2014) și al Comisiei juridice, de disciplină și imunități (nr.PLx nr.263/2014 din 05.06.2014).

Proiectul de lege are ca obiect reglementarea activităţilor în domeniul securităţii cibernetice, componentă a securităţii naţionale a României, precum şi obligaţiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice.

Potrivit prevederilor art. 75 alin. (1) din Constituţia României, republicată, şi ale art. 92 alin. (8) pct.2 din Regulamentul Camerei Deputaţilor, republicat, Camera Deputaţilor este **Prima Cameră sesizată.**

În conformitate cu prevederile art. 61 și 63 din Regulamentul Camerei Deputaţilor, republicat, cu modificările ulterioare, membrii Comisiei pentru tehnologia informaţiei şi comunicaţiilor au examinat proiectul de lege şi documentele conexe, în şedinţele din 11, 24 iunie 2014 și 2 iulie 2014, la dezbateri participând, în conformitate cu prevederile art. 54 şi 55 din Regulamentul Camerei Deputaţilor, republicat, în calitate de invitați următorii: din partea Serviciului Român de Informații, domnul Surugiu Romulus, domnul Milea Constantin și domnul General Dumitru Dumbravă, din partea Ministerului Afacerilor Interne doamna Chestor de poliție Irina Alexe și domnul Crișan Silviu George, din partea MSI doamna Dobrică Ionela și doamna Carmen Elian, din partea ANCOM domnul Lovin Eduard, domnul Marius Săceanu și doamna Alina Șumudică, din partea ApTI domnul Vasile Matei Eugen, domnul Alecu Bogdan și Domnul Bogdan Manolea, din partea AOMR domnul Liviu Popescu, domnul Mihai Tărniceanu – Vodafone, domnul Dorin Odiațiu – Orange, doamna Andreea Modovanu – Orange și domnul Adrian Ionescu – Romtelecom-Cosmote. Comisia pentru apărare, ordine publică şi siguranţă naţională a examinat proiectul de lege în şedinţa din data de 3 mai 2014, la dezbateri participând, în calitate de invitați, domnul Cosmoiu Florin şi doamna Iordache Luiza din partea Serviciului Român de Informaţii.

Totodată, în **data de 8 septembrie 2014,** Comisia pentru tehnologia informaţiei şi comunicaţiilor și Comisia pentru apărare, ordine publică şi siguranţă naţională s-au reunit în ședință comună pentru dezbaterea proiectul de privind securitatea cibernetică a României (Plx 263/2014).

Din numărul total de **18 membri** ai Comisiei pentru tehnologia informaţiei şi comunicaţiilor au participat la dezbateri **11 deputaţi.**

Din numărul total de **26 membri** ai Comisiei pentru apărare, ordine publică şi siguranţă naţională au participat la dezbateri **16 deputaţi.**

În urma dezbaterilor membrii celor două comisii au hotărât, cu **unanimitate de voturi pentru, să se supună dezbaterii plenului Camerei Deputaţilor, raportul comun de adoptare asupra proiectului de Lege privind securitatea cibernetică a României,** cu **amendamentele admise redactate în Anexa nr.1 și amendamentele respinse redactate în Anexa nr.2, care fac parte integrantă din prezentul raport.**

În raport cu obiectul şi conţinutul său proiectul de lege face parte din categoria **legilor organice**.

PREŞEDINTE,

DANIEL VASILE OAJDEA

SECRETAR,

SORIN AVRAM IACOBAN

PREŞEDINTE,

ION MOCIOALCĂ

SECRETAR,

IOAN BENGA

Anexa nr.1

Amendamente admise la Proiectul de Lege privind securitatea cibernetică a României – Plx nr.263/2014

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
1.	Titlul legii Lege privind securitatea cibernetică a României	**Nemodificat**	
2.	CAPITOLUL I Dispoziţii generale	**Nemodificat**	
3.	**Art.l.** - Prezenta lege stabileşte cadrul general de reglementare a activităţilor în domeniul securităţii cibernetice şi obligaţiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice.	**Nemodificat**	
4.	**Art.2.** - Dispoziţiile 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 deţinători de infrastructuri cibernetice.	**Nemodificat**	
5.	**Art.3.** - (1) Securitatea cibernetică este componentă a securităţii naţionale a României şi se realizează prin: a) cunoaşterea, prevenirea şi contracararea ameninţărilor şi atacurilor, precum şi prin diminuarea vulnerabilităţilor infrastructurilor	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	cibernetice, în scopul gestionării riscurilor la adresa securităţii 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.		
6.	**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	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	în spaţiul cibernetic; e) realizarea accesului egal şi nediscriminatoriu al persoanelor la informaţii şi servicii publice oferite prin intermediul infrastructurilor cibernetice; f) guvemanţa 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.		
7.	**Art.5. -** În sensul prezentei legi, termenii şi expresiile de mai jos au următorul înţeles: **1. ameninţare cibernetică** - circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii cibernetice; **2. apărare cibernetică** - acţiuni desfăşurate în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun împotriva ameninţărilor asupra infrastructurilor cibernetice destinate apărării naţionale;	Nemodificat Nemodificat Nemodificat	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	3. **atac cibernetic** - acţiune ostilă de natură să afecteze securitatea cibernetică, desfăşurată în spaţiul cibernetic;	3.atac cibernetic - acţiune ostilă de natură să afecteze securitatea cibernetică. (Autor: Varujan Pambuccian – deputat Grupupul parlamentar al minorităţilor naţionale)	
	4. **audit de securitate cibernetică** - evaluare 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;	Nemodificat	
	5. **incident cibernetic** - eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;	Nemodificat	
	6. **eveniment survenit în spaţiul cibernetic** - acţiune desfăşurată în spaţiul cibernetic care are drept consecinţă modificarea stării infrastructurilor cibernetice;	Nemodificat	
	7. **infrastructuri cibernetice** - infrastructuri din domeniul tehnologiei informaţiei şi comunicaţii, constând în sisteme	Nemodificat	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice; **8. infrastructuri cibernetice de interes naţional (ICIN)** - infrastructurile cibernetice care susţin servicii publice sau de interes public, ori servicii ale societăţii informaţionale, a căror afectare poate aduce atingere securităţii naţionale, sau prejudicii grave statului român ori cetăţenilor acestuia, denumite în continuare ICIN; **9. managementul identităţii** - metode de validare a identităţii persoanelor când acestea accesează anumite infrastructuri cibernetice; **10. managementul riscului** - un proces complex, continuu şi flexibil de identificare, evaluare şi contracarare a riscurilor la adresa securităţii cibernetice, bazat pe utilizarea unor tehnici şi instrumente complexe, pentru prevenirea pierderilor de orice natură; **11. operaţii în reţele de calculatoare** - procesul complex de planificare, coordonare,	Nemodificat Nemodificat Nemodificat	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	sincronizare, armonizare şi desfăşurare a acţiunilor în spaţiul cibernetic pentru protecţia, controlul şi utilizarea reţelelor de calculatoare, în scopul obţinerii superiorităţii informaţionale, concomitent cu neutralizarea capabilităţilor adversarului; **12. rezilienţa infrastructurilor cibernetice** - capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate; **13. risc de securitate în spaţiul cibernetic** - probabilitatea ca o ameninţare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice; **14. securitate cibernetică** - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive pot	Nemodificat	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor; **15. spaţiu cibernetic** - mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta; **16. vulnerabilitate în spaţiul cibernetic** - slăbiciune în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatată de către o ameninţare.		
8.	CAPITOLUL II Sistemul Naţional de Securitate Cibernetică	**Nemodificat**	
9.	**Art.6.** - (1) În vederea asigurării cadrului general de cooperare pentru realizarea securităţii cibernetice se constituie Sistemul Naţional de Securitate Cibernetică, denumit în continuare SNSC, care reunește	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	autorităţile şi instituţiile publice cu responsabilităţi şi capacităţi în domeniu. (2) Autorităţile şi instituţiile publice din SNSC colaborează cu deţinătorii de infrastructuri cibernetice, mediul academic, mediul de afaceri, asociaţiile profesionale şi organizaţiile neguvemamentale. (3) Activitatea SNSC este coordonată la nivel strategic de Consiliul Suprem de Apărare a Ţării, denumit în continuare CSAT.		
10.	**Art.7**. - (1) SNSC îndeplineşte următoarele funcţii: a)funcţia de cunoaştere, prin care furnizează suportul informaţional necesar elaborării măsurilor proactive şi reactive, în vederea asigurării securităţii cibernetice; b) funcţia de prevenire, prin care asigură în principal, securitatea cibernetică a României, prin crearea şi dezvoltarea capacităţilor necesare analizei şi prognozei evoluţiei stării acesteia; c) funcţia de cooperare şi coordonare, prin care asigură mecanismul unitar şi eficient de relaţionare a autorităţilor şi instituţiilor componente ale SNSC;	**Nemodificat**	.

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	d) funcţia de contracarare, prin care asigură reacţia eficientă la ameninţările sau atacurile cibernetice, prin identificarea şi blocarea manifestării acestora. Aceasta se realizează în scopul menţinerii sau restabilirii securităţii infrastructurilor cibernetice vizate, precum şi pentru identificarea şi sancţionarea autorilor, potrivit legii. (2) Funcţiile SNSC se realizează prin adoptarea de măsuri proactive şi reactive privind informarea, monitorizarea, diseminarea, analizarea, avertizarea, coordonarea, decizia, reacţia, refacerea şi conştientizarea.		
11.	**Art. 8.** - (1) Coordonarea unitară a activităţilor SNSC se realizează de către Consiliul Operativ de Securitate Cibernetică, denumit în continuare COSC. (2) COSC este format din reprezentanţi ai Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societate Informaţională, Serviciului Român de Informaţii, Serviciului de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază, Oficiului	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	Registrului Naţional al Informaţiilor Secrete de Stat, precum şi Secretarul Consiliului Suprem de Apărare a Ţării. (3) Conducerea COSC este asigurată de Consilierul Prezidenţial pentru apărare şi securitate naţională, în calitate de preşedinte şi de Consilierul Primului Ministru pe probleme de securitate naţională - în calitate de vicepreşedinte. (4) COSC îşi desfăşoară activitatea în conformitate cu propriul Regulament de organizare şi funcţionare, care se aprobă prin hotărâre a CSAT, la propunerea Consilierului Prezidenţial pentru apărare şi securitate naţională, în termen de 60 de zile de la intrarea în vigoare a prezentei legi. (5) La activităţile COSC pot participa, în calitate de invitaţi, reprezentanţi ai altor instituţii sau autorităţi publice.		
12.	**Art.9. -** (1) În exercitarea atribuţiilor sale, COSC analizează şi evaluează starea securităţii cibernetice, formulează şi înaintează CSAT propuneri privind: a)măsuri de armonizare a reacţiei autorităţilor competente ale statului în situaţii generate de ameninţări şi atacuri cibernetice, care necesită	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	schimbarea nivelului de alertă cibernetică; b) solicitarea de asistenţă din partea altor state sau organizaţii şi organisme internaţionale; c) modalitatea de răspuns la solicitările de asistenţă adresate României din partea altor state sau organizaţii şi organisme internaţionale; d) planuri sau direcţii de acţiune, în funcţie de concluziile rezultate şi evoluţia spaţiului cibernetic; e) direcţii de dezvoltare sau programe de investiţii în domeniul securităţii cibernetice; f) cerinţe minime de securitate cibernetică şi politici de securitate cibernetică pentru autorităţile şi instituţiile publice prevăzute la art.10 alin. (l) şi (2). (2) COSC cooperează pentru realizarea securităţii cibernetice cu organismele de coordonare sau conducere constituite, potrivit legii, la nivel naţional, pentru managementul situaţiilor de urgenţă, a acţiunilor în situaţii de criză în domeniul ordinii publice, pentru prevenirea şi combaterea terorismului şi pentru apărarea naţională, aşa cum sunt acestea prevăzute de legislaţia în		

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	domeniu.		
12.	**Art.10.** - (1) **Serviciul Român de Informaţii** este desemnat autoritate naţională în domeniul securităţii cibernetice, calitate în care asigură coordonarea tehnică a COSC, precum şi organizarea şi executarea activităţilor care privesc securitatea cibernetică a României. În acest scop, în structura SRI funcţionează Centrul Naţional de Securitate Cibernetică, denumit în continuare CNSC. (2) Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale şi Serviciul de Protecţie şi Pază sunt desemnate autorităţi în domeniul securităţii cibernetice pentru domeniile lor de activitate, asigurând securitatea infrastructurilor cibernetice proprii sau aflate în responsabilitate potrivit legii şi au obligaţia să constituie şi să operaţionalizeze structuri specializate de securitate cibernetică. (3) CNSC cooperează cu autorităţile şi instituţiile publice componente ale SNSC, precum şi cu deţinătorii de infrastructuri cibernetice.	**Nemodificat** **Nemodificat** **Nemodificat** **Nemodificat** **Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	(4) În caz de atac cibernetic care poate afecta securitatea cibernetică a României, CNSC este punct de contact pentru relaţionarea cu organismele similare din străinătate. (5) CERT-RO reprezintă un punct naţional de contact cu structurile de tip CERT care funcţionează în cadrul instituţiilor sau autorităţilor publice ori al altor persoane juridice de drept public sau privat, naţionale ori internaţionale, cu respectarea competenţelor ce revin celorlalte autorităţi şi instituţii publice cu atribuţii în domeniu, potrivit legii.	(5) **Centrul Naţional de Rrăspuns la Incidente de Securitate, denumit în continuare** *CERT-RO,* reprezintă un punct naţional de contact cu structurile de tip CERT care funcţionează în cadrul instituţiilor sau autorităţilor publice ori al altor persoane juridice de drept public sau privat, naţionale ori internaţionale, cu respectarea competenţelor ce revin celorlalte autorităţi şi instituţii publice cu atribuţii în domeniu, potrivit legii. ***(Autor: Comisia pentru apărare, ordine publică și siguranță națională)***	Pentru claritate textului şi respectarea normelor de tehnică legislativă.
13.	**Art.11.** - (1) CNSC are următoarele atribuţii principale: a) acţionează în scopul cunoaşterii, prevenirii, protecţiei, reacţiei şi managementului consecinţelor ameninţărilor şi atacurilor cibernetice; b) asigură schimbul de date şi informaţii între autorităţile şi instituţiile 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	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	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) în caz de atac cibernetic, asigură colectarea şi evaluarea datelor şi		

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	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. (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 SRI, în termen de 60 de zile de la intrarea în vigoare a prezentei legi.		
14.	**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	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	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.		
15.	**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 **Centrul Naţional de Răspuns la Incidente de Securitate**,	**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.	Pentru corelarea textului cu art. 10 alin. (5)

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	denumit în continuare 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.	**(Autor: Comisia pentru apărare, ordine publică și siguranță națională şi Comisia pentru tehnologia informaţiei şi comunicaţiilor)** **Nemodificat**	
16.	**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.	**Nemodificat**	
17.	**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.	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	(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, **la propunerea SRI.**	(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 normele metodologice de aplicare a prezentei legi. **(Autor:Comisia pentru apărare, ordine publică și siguranță națională)**	Pentru acurateţea textului.
	(3) 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.	**Nemodificat**	
	(4) Instituirea nivelurilor de alertă cibernetică, precum şi trecerea de la un nivel la altul se aprobă de către CSAT, la propunerea COSC.	**Nemodificat**	
	(5) Pentru punerea în aplicare a măsurilor specifice prevăzute la alin. (2) persoanele juridice de drept public sau privat deţinători de ICIN elaborează planuri de acţiune proprii,	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	corespunzătoare fiecărui nivel de alertă cibernetică. (6) La instituirea unui nivel de alertă cibernetică, persoanele juridice de drept public sau privat deţinători de ICIN au obligaţia să pună în aplicare măsurile specifice prevăzute prin planurile prevăzute la alin. (5). (7) Deţinătorii de infrastructuri cibernetice au obligaţia să sprijine autorităţile şi instituţiile publice competente pentru implementarea măsurilor corespunzătoare fiecărui nivel de alertă cibernetică, potrivit solicitărilor acestora, adresate în condiţiile art.17 alin. (l) lit.a). (8) Persoanele juridice de drept public sau privat deţinători de ICIN au obligaţia transmiterii cu celeritate a datelor privind starea de securitate cibernetică la nivelul acestora către CNSC conform competenţelor prevăzute de lege.	**Nemodificat** **Nemodificat** **Nemodificat**	
18.	CAPITOLUL III Asigurarea securităţii cibernetice	**Nemodificat**	
19.	**Art.16.** - Deţinătorii de infrastructuri cibernetice au următoarele obligaţii: a) să aplice politici de securitate cibernetică, cu respectarea cerinţelor minime de securitate	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	stabilite la nivel naţional de Ministerul pentru Societatea Informaţională, ANCOM sau de către alte autorităţi 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 acţiunile 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.		
20.	**Art. 17.** (1) Pentru realizarea securităţii cibernetice, deţinătorii de	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	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	**Nemodificat** b)să informeze, de îndată, autorităţile şi instituţiile publice prevazute la lit. a) cu privire la incidentele cibernetice identificate, conform procedurilor stabilite prin normele motodologice **de aplicare a prezentei legi.** **(Autor: Sorin-Avram Iacoban – deputat PSD şi Comisia pentru apărare, ordine publică şi siguranţă naţională)** **Nemodificat**	Pentru conformitate cu normele de tehnică legislativă

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	publice cu atribuţii în domeniul securităţii cibernetice, pentru asigurarea securităţii cibernetice în domeniul lor de activitate.		
21.	**Art. 18.** - Deţinătorii de infrastructuri cibernetice, furnizori de servicii de internet au obligaţia de a-şi notifica clienţii**, persoane de drept public şi privat**, de îndată, 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 incidente sau atacuri cibernetice şi de a dispune măsurile necesare în vederea restabilirii condiţiilor normale de funcţionare.	**Art.18** - Deţinătorii de infrastructuri cibernetice, furnizori de servicii de internet, au obligaţia de a-şi notifica **clienţii**, de îndată, 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 incidente sau atacuri cibernetice şi de a dispune măsurile necesare în vederea restabilirii condiţiilor normale de funcţionare**.** **(Autor: Sorin-Avram Iacoban – deputat PSD şi Comisia pentru apărare, ordine publică şi siguranţă naţională)**	Trebuie notificați toți clienții atât persoane fizice, cât și persoane juridice de drept public și privat.
22.	**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	**Nemodificat** **Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	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 selecţie cuprinse în metodologia elaborată de Serviciul Român de Informaţii şi Ministerul pentru Societatea Informaţională şi aprobată, în termen de 60 de zile de la intrarea în vigoare a prezentei legi, prin hotărâre de Guvern.		
	(4) La **elaborarea** catalogului ICIN, Ministerul pentru Societatea Informaţională **va colabora** şi cu ANCOM, în situaţia persoanelor juridice de drept privat care deţin calitatea de furnizori de reţele publice sau servicii de comunicaţii electronice destinate publicului.	(4) **La întocmirea** catalogului ICIN, Ministerul pentru Societatea Informaţională **colaborează** şi cu ANCOM, în situaţia persoanelor juridice de drept privat care deţin calitatea de furnizori de reţele publice sau servicii de comunicaţii electronice destinate publicului. **(Autor: Comisia pentru apărare, ordine publică și siguranță națională)**	Pentru uniformitatea normei
	(5) Se exceptează de la prevederile alin. (1) ICIN care stochează, procesează sau transmit informaţii clasificate, deţinute, administrate sau utilizate de persoanele juridice de drept public sau privat, care se centralizează la nivelul Oficiului Registrului Naţional al Informaţiilor Secrete de	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	Stat, denumit în continuare ORNISS. (6) ICIN prevăzute la alin. (5), se comunică CNSC, cu excepţia celor constituite la nivelul Autorităţilor Desemnate de Securitate, care deţin Structuri Interne INFOSEC acreditate potrivit prevederilor legale în vigoare. (7) Persoanele juridice de drept public şi privat deţinătoare de ICIN sau care au în responsabilitate ICIN trebuie să notifice CNSC şi CERT-RO, în termen **de 48 de ore**, cu privire la orice modificare intervenită în regimul juridic al ICIN, respectiv în configuraţia acesteia.	**Nemodificat** (7) Persoanele juridice de drept public şi privat deţinătoare de ICIN sau care au în responsabilitate ICIN trebuie să notifice CNSC şi CERT-RO, în termen de **72 de ore**, cu privire la orice modificare intervenită în regimul juridic al ICIN, respectiv în **(Autor: Comisia pentru tehnologia informației și comunicațiilor și Comisia pentru apărare,ordine public şi siguranţă naţională)**	In cadrul elaborarii reglmentarilor mentionate va trebui tinut cont si de faptul că furnizorii de rețele publice sau servicii de comunicații electronice destinate publicului pot efectua activități de mentenanță, upgrade de infrastructură, implementare servicii noi, modificări aduse în parametrajul diferitelor sisteme tehnice, modificarea topologiei de rețea etc.
23.	**Art.20.** - (1) Persoanele juridice de drept public sau privat care deţin sau au în responsabilitate ICIN, cu excepţia celor prevăzute la art.10 alin. (l) şi (2) au următoarele obligaţii: a) să stabilească şi să aplice măsuri pentru asigurarea rezilienţei infrastructurilor cibernetice proprii sau aflate în responsabilitate; b) să întocmească planul de securitate al ICIN, precum şi planuri de	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	acţiune proprii corespunzătoare fiecărui nivel de alertă cibernetică; c)să efectueze anual auditări de securitate cibernetică sau să permită efectuarea unor astfel de auditări la solicitarea motivată a autorităţilor competente potrivit prezentei legi; d) să constituie structuri sau să desemneze persoane responsabile cu prevenirea, identificarea şi reacţia la incidentele cibernetice; e) să implementeze soluţii pentru gestionarea permanentă a evenimentelor din spaţiul cibernetic care pot afecta securitatea infrastructurii cibernetice şi să genereze alerte cu privire la acestea; f) să aplice politicile de securitate prevăzute prin cerinţele minime stabilite conform dispoziţiilor prezentei legi; g) să ia măsuri pentru prevenirea incidentelor cibernetice şi să reducă, după caz, impactul acestora asupra utilizatorilor sau beneficiarilor ICIN; h) să notifice imediat, după caz, CNSC, CERT-RO, ANCOM sau autorităţile desemnate, în condiţiile legii, în domeniul securităţii cibernetice cu privire la riscurile şi incidentele cibernetice care, prin efectul lor, pot		

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	aduce prejudicii de orice natură utilizatorilor sau beneficiarilor serviciilor lor; i) să respecte modalitatea de notificare, precum şi datele şi informaţiile care însoţesc în mod obligatoriu notificarea, stabilite potrivit alin. (2) . (2) În vederea îndeplinirii obligaţiilor prevăzute la alin. (1) lit. a), f) şi g), Ministerul pentru Societatea Informaţională, ANCOM sau autorităţile desemnate, în condiţiile legii, în domeniul securităţii cibernetice, stabilesc cerinţele minime de securitate cibernetică, modalitatea de notificare, precum şi datele şi informaţiile care însoţesc 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 autorităţilor sau instituţiilor publice respective, publicate în Monitorul Oficial al României, Partea I.		
24.	**Art.21**. - (1) În funcţie de tipul şi natura riscurilor şi incidentelor cibernetice, autorităţile competente să recepţioneze notificarea prevăzută la art 20 alin. (1) lit. h), acţionează potrivit competenţelor stabilite prin	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	lege. (2) Deţinătorii de ICIN, care au transmis notificări conform art. 20 alin. (1) lit. h, au următoarele obligaţii: a) să aplice planurile prevăzute la art. 20 alin. (1) lit. b); b) să menţină legătura cu autorităţile competente, potrivit legii, informând despre evoluţia incidentului şi modul în care acesta este gestionat; c)să permită autorităţilor competente, potrivit legii, să intervină pentru identificarea şi analizarea cauzelor incidentelor cibernetice, respectiv pentru înlăturarea sau reducerea efectelor incidentelor cibernetice; d)să reţină şi să asigure integritatea datelor referitoare la incidentele cibernetice pentru o perioadă de 6 luni de la data notificării, cu respectarea principiului confidenţialităţii şi să le pună la dispoziţia autorităţilor competente, în condiţiile legii. (3) Obligaţiile prevăzute la alin. (2), se aplică tuturor deţinătorilor de infrastructuri cibernetice implicate în incidentul notificat. (4) Dispoziţiile prezentului articol nu se aplică în cazul instituţiilor şi autorităţilor publice prevăzute la art. 10 alin. (l) şi (2).		

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
24.	**Art.22.** - (1) CERT-RO asigură colectarea şi evaluarea datelor şi informaţiilor cu privire la incidente şi atacuri cibernetice notificate, potrivit art. 20 alin. (l) lit.h), de deţinătorii de ICIN, persoanelor juridice de drept privat, ia măsuri reactive de primă urgenţă pentru asigurarea integrităţii datelor şi remedierea situaţiei de fapt. (2) CERT-RO informează CNSC cu privire la notificările primite şi la situaţiile în care a luat măsuri reactive de primă urgenţă, potrivit alin. (l).	**Nemodificat**	
25.	**Art.23.** - (1) Securitatea infrastructurilor cibernetice deţinute sau administrate de furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului se realizează în condiţiile Ordonanţei de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată, cu modificări şi completări, prin Legea nr. 140/2012, precum şi în conformitate cu dispoziţiile prezentei legi. (2) Pentru îndeplinirea obiectivelor prezentei legi, ANCOM poate emite decizii. (3) În vederea realizării scopului	Art. 23. - (1) Securitatea infrastructurilor cibernetice deţinute sau administrate de furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului se realizează în condiţiile Ordonanţei de urgenţă a Guvernului nr. 111/2011 privind comunicaţiile electronice, aprobată cu modificări şi completări prin Legea nr. 140/2012**, cu modificările şi competările ulterioare,** precum şi în conformitate cu dispoziţiile prezentei legi. **(Autor:Comisia pentru apărare, ordine public şi siguranţă naţională)** **Nemodificat** **Nemodificat**	Pentru acurateţea textului şi pentru respectarea normelor de tehnică legislativă

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	prezentei legi, ANCOM îi revin următoarele atribuţii: a)verifică respectarea de către furnizorii de reţele publice sau servicii de comunicaţii electronice destinate publicului care deţin şi/sau administrează ICIN a dispoziţiilor art. 20 alin.(l) lit. a)- g) b)exercită controlul respectării dispoziţiilor art. 20 de către furnizorii de reţele publice sau servicii de comunicaţii electronice destinate publicului care deţin şi/sau administrează ICIN. (4) În cazul furnizorilor de reţele publice sau servicii de comunicaţii electronice destinate publicului care deţin şi/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, informaţiile relevante privind atacurile, ameninţările şi incidentele, care prin efectul lor, pot compromite sau aduce atingere securităţii naţionale şi apărării ţării sau care afectează serviciile de interes public ori serviciile societăţii informaţionale determinând producerea	**Nemodificat** **Nemodificat** **Nemodificat** **Nemodificat** **Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	unor prejudicii grave statului român ori cetăţenilor acestuia. (6) În implementarea prevederilor prezentei legi, ANCOM va constitui şi va operaţionaliza o structură specializată de securitate cibernetică, de tip CERT.		
26.	CAPITOLUL IV Apărarea cibernetică	**Nemodificat**	
27.	**Art.24.** - (1) Apărarea cibernetică cuprinde ansamblul de măsuri şi activităţi adoptate şi desfăşurate de autorităţile competente pentru protejarea infrastructurilor cibernetice destinate apărării naţionale şi a infrastructurilor cibernetice naţionale care sunt critice pentru misiunile NATO şi UE. (2) Infrastructurile cibernetice destinate apărării naţionale şi măsurile privind apărarea cibernetică a acestora se stabilesc în termen de 60 de zile de la intrarea în vigoare a prezentei legi şi se actualizează periodic prin hotărâre a CSAT.	**Nemodificat**	
28.	**Art.25.** - (1) Activităţile prevăzute la art.24 alin.(l) se planifică şi se desfăşoară de autorităţile competente în strânsă legătură cu activităţile	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	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 termenul prevăzut de normele metodologice la prezenta lege, măsuri de apărare cibernetică şi răspund de executarea acestora, fiecare în domeniul său de activitate.	(2) Autorităţile şi instituţiile publice au obligaţia de a identifica şi implementa, în condiţiile legii şi în termenul prevăzut de normele metodologice **de aplicare a prezentei legi,** măsuri de apărare cibernetică şi răspund de executarea acestora, fiecare în domeniul său de activitate. **(Autor:Comisia pentru apărare,ordine publică şi siguranţă naţională şi Comisia pentu tehnologia informaţiei)**	Conform normelor de tehnică legislativă
29.	**Art.26.** - (1) Ministerul Apărării Naţionale împreună cu celelalte autorităţi şi instituţii publice din Sistemul Naţional de Apărare, Ordine Publică şi Securitate Naţională 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,	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	declararea stării de mobilizare sau a stării de război se realizează de către Centrul naţional militar de comandă în cooperare cu COSC.		
30.	CAPITOLUL V Regimul sancţionator şi dispoziţii procedurale	**Nemodificat**	
31.	**Art.27.** - (1) Monitorizarea şi controlul aplicării prevederilor prezentei legi se asigură, potrivit competenţelor stabilite prin lege, de către: a)Camera Deputaţilor şi Senat, Administraţia Prezidenţială, Guvern, CSAT, precum şi instituţiile şi autorităţile publice prevăzute la art. 10 alin. (1) şi (2), pentru infrastructurile cibernetice proprii sau aflate în responsabilitate; b)Serviciul Român de Informaţii pentru infrastructurile cibernetice proprii sau aflate în responsabilitate, precum şi pentru deţinătorii de ICIN persoane juridice de drept public; c) Ministerul pentru Societatea Informaţională, respectiv ANCOM, după caz, pentru deţinătorii de ICIN, persoane juridice de drept privat. (2) În vederea exercitării atribuţiilor prevăzute la alin.(l), conducătorii	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	autorităţilor desemnează persoanele abilitate să desfăşoare activităţi de control care, în baza şi în limitele împuternicirii aprobate au dreptul: a) să solicite declaraţii sau orice documente necesare pentru efectuarea controlului; b) să facă inspecţii, inclusiv inopinate, la orice instalaţie, incintă sau infrastructură, destinate ICIN, cu respectarea prevederilor legale în vigoare; c) să primească, la cerere sau la faţa locului, informaţii sau justificări.		
32.	**Art.28.** - Constituie contravenţii următoarele fapte: a) nerespectarea de către deţinătorii de infrastructuri cibernetice a obligaţiei privind adoptarea şi punerea în aplicare a politicii de securitate cibernetică care să respecte cerinţele minime de securitate stabilite potrivit prezentei legi, prevăzute la art. 16 lit. a); b) nerespectarea de către deţinătorii de sau cei care au în responsabilitate ICIN a obligaţiei de notificare cu privire la modificările de regim juridic, respectiv de configuraţie a ICIN, prevăzute la art. 19 alin.(7); c) încălcarea de către	**Nemodificat** a) **nerespectarea de către deţinătorii de infrastructuri cibernetice a obligaţiei prevăzute la art. 16 lit. a);** b) **nerespectarea de către deţinătorii de sau de către cei care au în responsabilitate ICIN a obligaţiei prevăzute la art. 19 alin. (7);** **Nemodificat**	Conform normelor de tehnică legislativă

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	deţinătorii de sau cei care au în responsabilitate ICIN obligaţiilor prevăzute la art. 20 alin. (1), lit. c)-e) privind efectuarea de auditări de securitate cibernetică, constituirea de structuri sau desemnarea de persoane responsabile cu prevenirea, identificarea şi reacţia la incidente cibernetice, respectiv implementarea de soluţii pentru gestionarea evenimentelor din spaţiul cibernetic şi generarea de alerte cu privire la acestea; d) nerespectarea de către deţinătorii de sau cei care au în responsabilitate ICIN a obligaţiei privind aplicarea politicilor de securitate, prevăzută la art.20 alin.(1) lit.f); e) nerespectarea de către deţinătorii de sau cei care au în responsabilitate ICIN a obligaţiei de notificare impuse potrivit art. 20 alin. (1) lit. h); f) nerespectarea de către deţinătorii de sau cei care au în responsabilitate ICIN a cerinţelor minime de securitate cibernetică, a modalităţii de notificare, precum şi datele şi informaţiile care însoţesc în mod obligatoriu notificarea obligaţiei prevăzută la art. 20 alin. (1) lit. i); g) nerespectarea de către deţinătorii de	**Nemodificat** **Nemodificat** **Nemodificat** **Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	sau cei care au în responsabilitate ICIN care au transmis notificarea în condiţiile prevăzute la art. 20 alin.(2) a obligaţiilor de aplicare a planurilor de securitate sau de acţiune, respectiv de a permite autorităţilor competente să intervină, precum şi a obligaţiei de a reţine şi asigura integritatea datelor referitoare la incidentele cibernetice, prevăzute la art. 21 alin. (2) lit. c) şi lit. d); h) încălcarea de către deţinătorii de sau cei care au în responsabilitate ICIN a obligaţiei de a informa autorităţile competente potrivit legii despre evoluţia incidentului cibernetic notificat şi cu privire la modul în care acesta este gestionat, stabilită de prevederile prevăzută la art. 21 alin. (2) lit. b); i)nerespectarea de către furnizorii de reţele publice sau servicii de comunicaţii electronice destinate publicului, deţinători de ICIN sau care au în administrare infrastructuri cibernetice a cerinţelor minime stabilite de ANCOM, a modalităţii de notificare, precum şi a datelor şi informaţiilor care însoţesc în mod obligatoriu notificarea, în temeiul obligaţiei prevăzute art. 23 alin. (3)	**Nemodificat** **Nemodificat** **j) nerespectarea de către deţinătorii de infrastructuri cibernetice, furnizori de servicii de internet, a obligaţiei prevăzută la art. 18.** **(Autor:Comisia pentru apărare, ordine publică și siguranță națională)**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	lit.a) precum şi refuzul de a se supune controlului potrivit art.23 alin.(3) lit.b); j) nerespectarea obligaţiei de notificare a clienţilor de către deţinătorii de infrastructuri cibernetice, furnizori de servicii de internet, prevăzută la art. 18.		Pentru claritatea textului şi respectraea normelor de tehnică legislativă.
33.	**Art. 29**. - Contravenţiile prevăzute la art. 28 se sancţionează, astfel: a) cu amendă de la 500 lei la 5.000, pentru săvârşirea contravenţiilor prevăzute la art. 28 lit. a) şi h)- j); b) cu amendă de la 1.000 la 10.000 lei, pentru săvârşirea contravenţiilor prevăzute la art. 28 lit. b) - g).	**Art. 29**. - Contravenţiile prevăzute la art. 28 se sancţionează, astfel: a) cu amendă de la 500 lei la 5.000 **lei**, pentru săvârşirea contravenţiilor prevăzute la art. 28 lit. a) şi h)- j); b) cu amendă de la 1.000 **lei** la 10.000 lei, pentru săvârşirea contravenţiilor prevăzute la art. 28 lit. b) - g). **(Autor:Comisia pentru apărare, ordine publică și siguranță națională)**	Pentru respectarea normelor de tehnică legislativă.
34.	**Art.30.** - Constatarea contravenţiilor şi aplicarea sancţiunilor se realizează, potrivit competenţelor legale, de către persoane împuternicite din cadrul: a) Ministerul pentru Societatea Informaţională, în cazul persoanelor juridice de drept privat, pentru contravenţiile prevăzute la art. 28 lit. a) - h);	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	b) ANCOM în situaţia în care contravenţiile prevăzute la art. 28 lit. a) sunt săvârşite de persoanele juridice prevăzute la art. 23 alin. (1), precum şi pentru contravenţiile prevăzute la art. 28 lit. i) şi j); c) autorităţile şi instituţiile publice prevăzute la art.27 alin.(l) lit. a) pentru contravenţiile prevăzute la art.28 lit.b) - h) ce vizeaza infrastructurile cibernetice proprii sau aflate în responsabilitate. d) Serviciul Român de Informaţii, pentru contravenţiile prevăzute la art.28 lit. b) - h).		
35.	**Art.31.-** Contravenţiilor prevăzute la art.28 le sunt aplicabile dispoziţiile Ordonanţei Guvernului nr. 2/2001 privind regimul juridic al contravenţiilor, aprobată cu modificări şi completări prin Legea nr. 180/2002, cu modificările şi completările ulterioare.	**Nemodificat**	
36.	Capitolul VII Dispoziţii finale	**Nemodificat**	
37.	**Art.32.** - (1) La nivelul persoanelor juridice de drept public, fondurile necesare organizării şi desfăşurării activităţii în condiţiile prezentei legi se	**Nemodificat**	

Nr. crt.	Text Lege	Text propus de Comisii	Motivarea Amendamentului
	asigură de la bugetul de stat, din venituri proprii şi 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.		
38.	**Art.33.** - (1) Prezenta lege intră în vigoare la 30 de zile de la publicarea în Monitorul Oficial al României, Partea I. (2) În termen de 90 de zile de la data publicării în Monitorul Oficial al României, Partea I, Guvernul aprobă: a) la propunerea Serviciului Român de Informaţii, normele metodologice prevăzute la art. 15 alin.(2); b)la propunerea Ministerului pentru Societatea Informaţională, normele metodologice prevăzute la art. 17 alin.(l) lit.b).	**Nemodificat**	

Anexa nr.2

Amendamente respinse la Proiectul de Lege privind securitatea cibernetică a României – Plx nr.263/2014

Nr. crt.	Text Lege	Text propus de Comisie (autorul amendamentului)	Motivarea Amendamentului
1.	**Art.10.** - (1) **Serviciul Român de Informaţii** este desemnat autoritate naţională în domeniul securităţii cibernetice, calitate în care asigură coordonarea tehnică a COSC, precum şi organizarea şi executarea activităţilor care privesc securitatea cibernetică a României. În acest scop, în structura SRI funcţionează Centrul Naţional de Securitate Cibernetică, denumit în continuare CNSC.	**Art.10 – (1) CERT-RO** este desemnat autoritate naţională în domeniul securităţii cibernetice, precum şi organizarea şi executarea activităţilor care privesc securitatea cibernetică a României. **(Autor: Daniel Iane, deputat PNL)**	Autoritatea națională trebuie să fie ***un organism civil***, ***„sub completă supraveghere democratică și nu ar trebui să îndeplinească nici un fel de rol de serviciu de informații, de aplicare a legii sau de apărare sau să aibă legături organizaționale de orice fel cu organizații active în aceste domenii” în conformitate cu propunerea de Directivă NIS.”.*** Singura instituție cu expertiză in domeniul securității informatice care îndeplinește cerințele de mai sus și ar putea îndeplini acest rol este, în acest moment, CERT RO.