PARLAMENTUL ROMÂNIEI

SENAT

Comisia pentru apărare, ordine publică şi siguranţă naţională

Nr. XXV/155/09.12.2014

RAPORT
asupra PROIECTULUI DE LEGE PRIVIND SECURITATEA CIBERNETICĂ A ROMÂNIEI

În conformitate cu prevederile art. 68 din Regulamentul Senatului, cu modificările ulterioare, Comisia pentru apărare, ordine publică şi siguranţă naţională a fost sesizată, de către Biroul Permanent al Senatului, prin **L 580/2014**, în vederea dezbaterii şi elaborării Raportului asupra ***Proiectului de lege privind securitatea cibernetică a României,*** iniţiat de Guvernul României.

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.**

Consiliul Legislativ, a avizat favorabil proiectul de lege, cu observaţii şi propuneri.

La dezbateri au participat, în conformitate cu prevederile art.61 din Regulamentul Senatului, reprezentanţi ai Ministerului .pentru Societatea Informaţională, ai Serviciului Român de Informaţii, precum şi ai Ministerului Afacerilor Interne.

În urma dezbaterilor, în şedinţa din 09 decembrie 2014, membrii Comisiei, cu majoritate de voturi, au hotărât să adopte **Raport de admitere, cu amendamentele cuprinse în Anexa, care face parte integrantă din prezentul Raport.**

Comisia pentru apărare, ordine publică şi siguranţă naţională supune spre dezbatere şi adoptare plenului Senatului, **Raportul de admitere, cu amendamente şi Proiectul de lege.**

În raport cu obiectul de reglementare, proiectul de lege face parte din categoria **legilor organice** şi urmează a fi adoptat în conformitate cu prevederile art.76 alin.(1) din Legea fundamentală.

Potrivit art.75 alin.(3) din Constituţia României, republicată, şi ale art.88 alin.(8), pct. 2 din Regulamentul Senatului, cu modificările ulterioare, **Senatul este Cameră Decizională.**

PREŞEDINTE,

Senator
Corneliu DOBRIŢOIU

SECRETAR,

Senator
NICOLAE NASTA

Întocmit Cons. Viorica Popovici

ANEXĂ

la Raportul Proiectului de Lege privind securitatea cibernetică a României (L 580/2014)

Nr. crt.	Text Lege	Amendamente Comisie	Motivații
1.	**Art. 5 –** **(3) atac cibernetic** – acțiune ostilă de natură să afecteze securitatea cibernetică, **desfășurată în spațiul cibernetic**.	**Art. 5 – (3) – modificat.** **(3) atac cibernetic** - acțiune ostilă de natură să afecteze securitatea cibernetică.	
2.	**Art. 5 – (5) incident _____cibernetic** – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică.	**Art. 5 – (5) - completat.** **(5) incident de securitate cibernetică** – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică.	Pentru claritatea textului raportat la domeniul de referință al legii – securitatea cibernetică.
3.		**Art. 5 – pct. 17 . nou introdus** **17. furnizor de servicii de securitate cibernetica – orice persoana juridică, română sau străină, care are ca obiect de activitate prestarea de servicii în domeniul securității cibernetice către terți.**	Se defineşte termenul de furnizor de servicii de securitate cibernetică. Aşa cum se stipulează în Strategia de securitate cibernetică a României un obiectiv al strategiei îl reprezintă *"promovarea şi dezvoltarea cooperării între sectorul public şi cel privat în plan național"*. Furnizorul de servicii de securitate cibernetică joacă astfel rolul unui terț de încredere în ceea ce priveşte securitatea sistemelor informatice.

4.	**Art. 10 – (5)** <u>CERT-RO</u> 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. 10 – (5) - modificat și completat.** (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.	
5.	**Art. 13** –(1) În vederea realizării coerenței activităților din cadrul SNSC, Ministerul pentru Societatea Informațională asigură legătura COSC cu autoritățile și instituțiile publice care nu sunt reprezentate în cadrul acestuia, iar prin <u>**Centrul Național de Răspuns la Incidente de Securitate,**</u> **denumit în continuare CERT-RO**, cu deținătorii de infrastructuri cibernetice, persoane juridice de drept privat.	**Art. 13 – (1) – modificat.** (1) În vederea realizării coerenței activităților din cadrul SNSC, Ministerul pentru Societatea Informațională asigură legătura COSC cu autoritățile și instituțiile publice care nu sunt reprezentate în cadrul acestuia, iar prin <u>**CERT-RO**</u>, cu deținătorii de infrastructuri cibernetice, persoane juridice de drept privat.	În conformitate cu Art.10- (5) – amendament propus de Comisie
6.	**Art. 15** –(2) Organizarea SNAC, măsurile specifice pe care autoritățile și instituțiile publice competente le implementează pentru fiecare nivel de alertă, precum și procedura de instituire a nivelurilor de alertă și cerințele privind elaborarea planurilor de acțiune se aprobă prin norme metodologice, **la propunerea SRI**.	**Art. 15 –(2) – modificat.** **2)** Organizarea SNAC, măsurile specifice pe care autoritățile și instituțiile publice competente le implementează pentru fiecare nivel de alertă, precum și procedura de instituire a nivelurilor de alertă și cerințele privind elaborarea planurilor de acțiune se aprobă prin norme metodologice.	

		Art 16 - aliniat nou **(2) Deținătorii de infrastructuri cibernetice implementează masurile tehnice prevăzute la alin.(1) lit.b prin utilizarea de resurse interne sau prin intermediul unor furnizori de servicii de securitate cibernetică .**	Permite externalizarea, implementarea obligațiilor ce le revin conform Art. 16 – alin 1 către un furnizor de servicii de securitate informatica.
7.	**Art. 18.** - Deținătorii de infrastructuri cibernetice, furnizori de servicii de internet au obligația de a-şi notifica clienții, **persoane de drept public şi privat**, de îndată, **dar nu mai târziu de 24 de ore** din momentul în care au fost sesizați de autoritățile competente potrivit prezentei legi, cu privire la,situațiile în care sistemele informatice utilizate de aceştia au fost implicateîn incidente sau atacuri cibernetice şi de a dispune măsurile necesare în vedereare stabilirii condițiilor normale de funcționare.	**Art.18 – modificat.** - Deținătorii de infrastructuri cibernetice, furnizori de servicii de internet, au obligația de a-şi notifica **clienții, de îndată,** din momentul în care au fost sesizați de autoritățile competente potrivit prezentei legi, cu privire la situațiile în care sistemele informatice utilizate de aceştia au fost implicate în incidente sau atacuri cibernetice şi de a dispune măsurile necesare în vederea restabilirii condițiilor normale de funcționare.	
8.	**Art. 19** – (4) La **elaborarea** catalogului ICIN, Ministerul pentru Societatea Informațională **va colabora** şi cu ANCOM, în situația persoanelor juridice de drept privat care dețin calitatea de furnizori de rețele publice sau servicii de comunicații electronice destinate publicului.	**Art. 19 – (4) - modificat.** (4) La **întocmirea** catalogului ICIN, Ministerul pentru Societatea Informațională **colaborează** şi cu ANCOM, în situația persoanelor juridice de drept privat care dețin calitatea de furnizori de rețele publice sau servicii de comunicații electronice destinate publicului.	

9.	**Art. 19 – (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.	**Art. 19 – (7) – modificat.** **(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 configuraţia acesteia.	
10.	**Art. 20, alin 1 lit c)** **c)** să efectueze **periodic** şi/sau să permită efectuarea unor auditări de securitate cibernetică, la solicitarea motivată a autorităţilor competente potrivit prezentei legi._____	**Art. 20, alin 1 lit c) – modificată şi completată.** **c)** să efectueze **anual** şi/sau să permită efectuarea unor auditări de securitate cibernetică, la solicitarea motivată a autorităţilor competente potrivit prezentei legi. **Auditările de securitate sunt realizate de catre autoritatea nationala în domeniul securităţii cibernetice, prevazuta la art. 10 alin (1) sau de catre furnizori de servicii de securitate cibernetică .**	Stabilirea frecvenţei realizării auditurilor este necesară pentru un cadru comun de verificare a nivelului de securitate pentru toate persoanele juridice de drept public sau privat care deţin sau au în responsabilitate ICIN. Stabilirea entităţii care poate realiza auditul elimină ambiguităţile care pot să apară la momentul aplicării legii.
11.		**Art 20 (3) aliniat nou** **(3) Persoanele juridice de drept public sau privat care deţin sau au în responsabilitate ICIN îndeplinesc obligaţiile prevăzute la alin (1) lit. a, b, d, e, f, g, h şi i prin utilizarea de resurse interne sau prin intermediul unor furnizori de servicii de securitate cibernetică.**	Permite externalizarea implementarea obligaţiilor ce le revin conform Art. 16 – alin 1 către un furnizor de servicii de securitate informatica.

12.	**Art. 23** – (1) Securitatea infrastructurilor cibernetice deținute sau administrate de furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului se realizează în condițiile Ordonanței de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice, aprobată, cu modificări și completări, prin Legea nr. 140/2012_____, precum și în conformitate cu dispozițiile prezentei legi.	**Art. 23 – (1) - completat.** **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.	
13.	**Art. 25** – (2) Autoritățile și instituțiile publice au obligația de a identifica și implementa, în condițiile legii și în termenul prevăzut de normele metodologice_____ la prezenta lege, măsuri de apărare cibernetică și răspund de executarea acestora, fiecare în domeniul său de activitate.	**Art. 25 – (2) – completat și modificat.** **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.	
14.	**a)** Camera Deputaților și Senat, Administrația Prezidențială____, **Guvern, CSAT**, precum și instituțiile și autoritățile publice prevăzute la art. 10 alin. (1) și (2), pentru infrastructurile cibernetice proprii sau aflate în responsabilitate;	**Art.27 – lit.a – modificată.** **a)** Camera Deputaților și Senat, Administrația Prezidențială **inclusiv Consiliul Suprem de Apărare a Țării, 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;	- aparatul de lucru al Guvernului este alcătuit din aparatul de lucru al primului-ministru, Secretariatul General al Guvernului, departamente și alte asemenea structuri organizatorice cu atribuții specifice stabilite prin hotărâre a Guvernului - CSAT este o autoritatea administrativă autonomă fără personalitate juridica, sub conducerea Președintelui României

15.	**Art. 28** – (1) Constituie contravenții următoarele fapte: a) nerespectarea de către deținătorii de infrastructuri cibernetice a obligației **privind adoptarea și punerea în aplicare a politicii de securitate cibernetică care să respecte cerințele minime de securitate stabilite potrivit prezentei legi**, prevăzute la art. 16 lit. a); b) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației **de notificare cu privire la modificările de regim juridic, respectiv de configurație a ICIN,** prevăzute la art.19 alin.(7); c) **încălcarea** de către deținătorii de sau cei care au în responsabilitate ICIN obligațiilor prevăzute la art. 20 alin. (1), lit. c)-e) privind efectuarea de auditări de securitate cibernetică, constituirea de structuri sau desemnarea de persoane responsabile cu prevenirea, identificarea și reacția la incidente cibernetice, respectiv implementarea de soluții pentru gestionarea evenimentelor din spațiul cibernetic și generarea de alerte cu privire la acestea; d) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a obligației privind aplicarea politicilor de securitate, prevăzută la art. 20 alin.(1) lit.h); e) **nerespectarea** de către deținătorii de sau cei care au în responsabilitate ICIN a	**Art. 28 – (1), lit. a), b), c), d), h), g) – modificate.** **– (1)** 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),**	

	cerințelor obligației de notificare impuse potrivit art.20 alin. (1) lit. h);	**lit. b)-e) privind efectuarea de auditări de securitate cibernetică, constituirea de structuri sau desemnarea de persoane responsabile cu prevenirea, identificarea şi reacția la incidente cibernetice, respectiv implementarea de soluții pentru gestionarea evenimentelor din spațiul cibernetic şi generarea de alerte cu privire la acestea;**	
	f)) nerespectarea de către deținătorii de sau cei care au în responsabilitate ICIN a **cerințelor minime de securitate cibernetică, a modalității de notificare, precum şi datele şi informațiile care însoțesc în mod obligatoriu notificarea obligației prevăzută la art. 20 alin. (1) lit. i);**	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 **care au transmis notificarea în condițiile 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 şi a obligației de a reține şi asigura integritatea datelor referitoare la incidentele cibernetice , prevăzute la art.21 alin. (2) lit. c) şi lit. d);**	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) **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 şi cu privire la modul în care acesta este**	h) **nerespectarea** de către deținătorii de sau cei care au în responsabilitate ICIN a **cerințelor minime de securitate cibernetică, a modalității de notificare, precum şi informațiile care însoțesc în mod obligatoriu notificarea obligației**	

	gestionat, stabilită de prevederile prevăzute la art.21 alin. (2) lit.b); i) nerespectarea de către furnizorii de rețele 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) li.a) precum și refuzul de a se supune controlului potrivit art.23 alin. (3) lit. b);** j) **nerespectarea** obligației de notificare a clienților de către deținătorii de infrastructuri cibernetice, furnizori de servicii de internet, prevăzută la art.18.	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 prevăzută 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 lit. 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 prevedeile prevăzute la art.21 alin.(2) lit. b); **k) – nou introdus** **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) – nou introdus.** **l) nerespectarea obligației de notificare a clienților de către deținătorii de infrastructuri cibernetice, furnizori de servicii de internet, prevăzută la art.18.**	
16.	**Art. 29 –** (1)Contravențiile prevăzute la art. 28 se sancționează, astfel: a) cu amendă de la 500 lei la 5.000 ____, pentru săvârșirea contravențiilor prevăzute la art. 28 lit. a) și h)- j);	**Art. 29 – a) – completat.** **(1)** Contravențiile prevăzute la art. 28 se sancționează, astfel: a) cu amendă de la 500 lei la 5.000 **lei**, pentru săvârșirea contravențiilor prevăzute la art. 28 lit. a) și h)- j);	
17.	**Art.30** **d) <u>Serviciul Român de Informații</u>**, pentru contravențiile prevăzute la art.28 lit. b) – h)	**Art.30 - lit.d) - modificată** **d) <u>Ministerul pentru Societatea Informațională desemnează prin ordin al ministrului pentru societatea</u>**	- pentru consecvența reglementării (vezi lit.a) și pentru implicarea MSI (acolo unde este cazul prin structura

		<u>informațională persoane calificate sau instituții competente din cadrul sau subordinea ministerului</u>, pentru contravențiile prevăzute la art.28 lit. b) – h)	aflată în coordonare) în actul de constatare a contravențiilor și aplicare a sancțiunilor, activități care nu erau specifice Serviciului Român de Informații