Comentarii la propunerea de lege privind securitatea cibernetică
Trimise pe data de 25.02.2016

Înainte de comentariile pe textul legii sunt mai multe aspecte esențiale care rezultă din decizia Curții Constituționale nr. 17/2015 (citată în extenso mai jos) și din proiectul de Directivă Network Information Security (NIS) care trebuie rezolvate la nivel fundamental.

Subliniem că textul actual încă suferă de inconsecvență, nerespectând obligațiile de tehnică legislativă (para. 92 – 99 din Decizia Curții Constituționale), iar maniera este neclară și vagă contrazicând în mod flagrant Decizia Curții Constituționale:

> *(59) (…)* ***cadrul normativ într-un domeniu atât de sensibil trebuie să se realizeze într-o manieră clară, previzibilă şi lipsită de confuzie, astfel încât să fie îndepărtată, pe cât posibil, eventualitatea arbitrariului sau a abuzului celor chemaţi să aplice dispoziţiile legale.***

Detaliem în continuare **o listă de 7 chestiuni de neconstituționalitate analizate în Decizia Curții Constituționale nr. 17/2015** și care **nu** au fost corectate de noua propunere de lege privind securitatea cibernetică:

A. Având în vedere faptul că Directiva NIS este aproape adoptată la nivelul UE[1], nu înțelegem „prioritatea națională" prevăzută în expunerea de motive. Chiar dacă România dorește să adopte un act normativ în acest domeniu înainte de publicarea în Jurnalul Oficial al UE a directivei, măcar ar trebui să urmeze pe cât posibil linia directivei pentru a nu face o nouă implementare care să schimbe cadrul legislativ în mai puțin de 2 ani.

B. Conform deciziei CCR, legea trebuie limitată doar la infrastructurile critice:

> *(69) Curtea apreciază că* ***obligaţiile ce decurg din Legea securităţii cibernetice a României trebuie să fie aplicabile în exclusivitate persoanelor juridice de drept public sau privat deţinătoare sau care au în responsabilitate ICIN*** *(care includ, în baza legii, şi administraţiile publice), întrucât numai situaţiile de pericol cu privire la o infrastructură de interes naţional pot avea implicaţii asupra securităţii României, (…) Or, dispoziţiile legale în forma supusă controlului de constituţionalitate prezintă un grad mare de generalitate, obligaţiile vizând totalitatea deţinătorilor de infrastructuri cibernetice, constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice, indiferent de importanţa acestora care poată viza interesul naţional sau doar un interes de grup ori chiar particular. Pentru a evita impunerea unei sarcini disproporţionate asupra micilor operatori, cerinţele trebuie să fie proporţionale cu riscurile la care sunt expuse reţeaua sau sistemul informatic în cauză şi nu trebuie aplicat deţinătorilor de infrastructuri cibernetice cu importanţă nesemnificativă din punctul de vedere al interesului general.*

[1] http://www.europarl.europa.eu/news/en/news-room/20160114IPR09801/First-ever-EU-wide-cyber-security-rules-backed-by-Internal-Market-Committee

C. Definirea ICIN trebuie să fie stabilită în lege și să fie clară și fără echivoc.

(67) ***Curtea apreciază că modalitatea prin care se stabilesc criteriile în funcţie de care se realizează selecţia infrastructurilor cibernetice de interes naţional şi, implicit, a deţinătorilor ICIN nu respectă cerinţele de previzibilitate, certitudine şi transparenţă.*** *(..) Opţiunea pentru o atare modalitate de reglementare apare cu atât mai nejustificată cu cât într-o materie similară, cea a identificării infrastructurilor critice naţionale, Ordonanţa de urgenţă a Guvernului nr. 98/2010 stabileşte în chiar conţinutul său criteriile intersectoriale de identificare a ICN.*

(68) Curtea reţine că atât criteriile în funcţie de care se realizează selecţia infrastructurilor cibernetice de Interes naţional, cât şi modalitatea prin care se stabilesc acestea trebuie prevăzute de lege, iar ***actul normativ de reglementare primară trebuie să conţină o listă cât mai completă a domeniilor în care sunt incidente prevederile legale.***

D. Notificarea incidentelor de securitate trebuie să fie clar restrânsă la acele categorii de incidente și date care sunt relevante pentru securitatea cibernetică națională.

(75) obligaţia de a notifica imediat, (…) în domeniul securităţii cibernetice cu privire la riscurile şi incidentele cibernetice, Curtea consideră că aceasta ***ar trebui să stabilească cu exactitate circumstanţele în care este necesară notificarea, precum şi conţinutul notificării****, inclusiv tipurile de date cu caracter personal care ar trebui notificate, şi, dacă este cazul, în ce măsură notificarea şi documentele sale justificative vor include detalii privind datele cu caracter personal afectate de un incident specific de securitate (precum adresele IP).*

E. Autoritatea competentă NU trebuie să fie o autoritate din domeniul informațiilor.

(48) Curtea apreciază că, pentru asigurarea unui climat de ordine, guvernat de principiile unui stat de drept, democratic, ***înfiinţarea sau identificarea unui organism responsabil cu coordonarea problemelor de securitate a sistemelor şi reţelelor cibernetice,*** *precum şi a informaţiei, care să constituie punctul de contact pentru relaţionarea cu organismele similare din străinătate [aşa cum prevede art. 10 alin. (4) din lege], inclusiv al cooperării transfrontaliere la nivelul Uniunii Europene,* ***trebuie să vizeze un organism civil, care să funcţioneze integral pe baza controlului democratic, iar nu o autoritate care desfăşoară activităţi în domeniul informaţiilor, al aplicării legii sau al apărării ori care să reprezinte o structură a vreunui organism care activează în aceste domenii.***

(51) (...) Or, în condiţiile în care Centrul Naţional de Securitate Cibernetică constituie o structură militară, în cadrul unui serviciu de informaţii, subordonată ierarhic conducerii acestei instituţii, deci sub un control direct militar-administrativ, apare cu evidenţă că o atare entitate nu îndeplineşte condiţiile cu privire la garanţiile necesare respectării drepturilor fundamentale referitoare la viaţă intimă, familială şi privată şi la secretul corespondenţei.

F. Trimiterea aspectelor majore de reglementare către legislație secundară în contextul în care ele pot aduce drepturilor fundamentale este ilegală.

> *(75) (…)* ***Trimiterea la acte administrative, cu o forţă juridică inferioară legii, într-un domeniu critic pentru securitatea naţională, cu impact asupra drepturilor şi libertăţilor fundamentale ale cetăţenilor, încalcă prevederile constituţionale cuprinse în art. 1 alin. (5) referitoare la principiul legalităţii.*** *O dispoziţie legală trebuie să fie precisă, neechivocă, să instituie norme clare, previzibile, a căror aplicare să nu permită arbitrariul sau abuzul. De asemenea, norma trebuie să reglementeze în mod unitar, uniform, să stabilească cerinţe minimale aplicabile tuturor destinatarilor săi.*

G. Pentru persoanele care se consideră vătămate trebuie să existe dreptul real și eficient de a te adresa justiției – vezi detalii în para. 81 – 91 din Decizia Curții Constituționale.

> *(81)* ***Curtea constată că lipsa oricărei prevederi în conţinutul legii prin care să se asigure posibilitatea persoanei ale cărei drepturi, libertăţi sau interese legitime au fost afectate prin acte sau fapte care au ca temei dispoziţiile Legii privind securitatea cibernetică a României de a se adresa unei instanţe judecătoreşti independente şi imparţiale*** *contravine prevederilor art. 1 alin. (3) şi (5), art. 21, precum şi art. 6 din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale.*
>
> *(88) Pentru ca dreptul la un proces echitabil să nu rămână teoretic şi iluzoriu, normele juridice trebuie să fie clare, precise şi explicite, astfel încât să îl poată avertiza în mod neechivoc pe destinatarul acestora asupra gravităţii consecinţelor nerespectării enunţurilor legale pe care le cuprind.*

În ceea ce urmează, vom oferi în tabelul de mai jos comentarii punctuale pe textul propunerii de lege privind securitatea cibernetică. Textele subliniate din partea stângă sunt termenii comentați în coloana din dreapta.

LEGE PRIVIND SECURITATEA <u>CIBERNETICĂ</u> A ROMÂNIEI	Trebuie să avem avenție la terminologie folosită – cibernetic nu înseamnă informatic. Conform DEX98, cibernetică este știința care are ca obiect studiul matematic al legăturilor, comenzilor și controlului în sistemele tehnice și în organismele vii din punctul de vedere al analogiilor lor formale. Termenul de cibernetică – propus prima dată de Stefan Odobleja sub denumirea de „psihologia consonantistă” - nu se ocupa de obiecte, ci de tipuri de comportamente.

Art. 1 - (1) Legea stabileşte cadrul juridic privind organizarea şi desfăşurarea activităţilor din domeniul securităţii cibernetice a României şi ~~asigurarea protejării drepturilor şi libertăţilor fundamentale ale cetăţenilor în spaţiul cibernetic~~.	Nu există nimic în textul legii la protecția drepturilor fundamentale ale cetățenilor în spațiul cibernetic.
(2) Securitatea cibernetică este componentă a securităţii naţionale a României şi se realizează prin adoptarea şi implementarea de politici şi măsuri de securitate la nivelul deţinătorilor de infrastructuri cibernetice în scopul cunoaşterii, prevenirii şi contracarării riscurilor şi ameninţărilor în spaţiul cibernetic.	Conform Deciziei CCR 17/2015, legea ar trebui să se refere doar la infrastructuri cibernetice de interes național.
Art. 2 - Prezenta lege se aplică: a) autorităţilor şi instituţiilor publice, persoanelor juridice deţinătoare de infrastructuri cibernetice care susțin servicii publice sau de interes public, ori servicii ale societăţii informaţionale, a căror afectare aduce atingere securităţii naţionale sau prejudicii grave statului român ori cetăţenilor acestuia;	Serviciile societății informaționale (SSI) sunt definite de Legea 365/2002 – orice site poate intra în această definiție – sunt peste 800 000 domenii .ro înregistrate și probabil în jur de 400 000 active.
b) persoanelor juridice, deţinătoare de infrastructuri cibernetice care prelucrează date cu caracter personal;	Aceasta înseamnă orice persoană juridică care are un calculator. Există în România peste 1.4 milioane de firme înregistrate, probabil cel puțin jumătate au un calculator cu date personale pe el.
c) furnizorilor de rețele publice de comunicații electronice și furnizorilor de servicii de comunicaţii electronice destinate publicului;	
d) furnizorilor de servicii de găzduire internet;	Nu există termenul de „găzduire internet” în legislația română, sunt incluși în SSI – vezi Legea 365/2002 art. 16.
e)furnizorilor de servicii de securitate cibernetică.	
Art. 3 - În sensul prezentei legi, termenii și expresiile de mai jos au următoarea semnificatie: a) ameninţare cibernetică - circumstanţă sau eveniment care constituie un pericol potențial la adresa securității cibernetice;	Comentariu[2]: În Directiva NIS „risc” înseamnă orice circumstanță sau eveniment care are un efect negativ potențial asupra securității. Definiția din propunere nu este clară și corespunde în fapt definiției riscurilor din directiva NIS. Introducerea termenilor „circumstanță” și „eveniment”, termeni care nu

[2]O parte din opiniile tehnice asupra definițiilor și principiilor sunt preluate, cu acordul autorului, de la prof. Adrian Munteanu, care este auditor certificate de sisteme informatice, expert ENISA și predă subiectul "auditul sistemelor informatice" – detalii la https://adimunteanu.wordpress.com/2016/02/11/legea-privind-securitatea-cibernetica-a-romaniei-observtii-punctuale/

	sunt definiți, în cazul amenințării nu este corectă. Evenimentul care are ca rezultat întreruperea funcționării SIUI din cadrul CNAS este amenințare cibernetică? În cadrul literaturii academice de specialitate specifică serviciilor IT, bunelor practici (ITIL – IT Infrastructure Library), cadrelor de referință (COBIT5 - poate cel mai cuprinzător cadru de referință pentru guvernarea și managementul IT), standardelor (seria ISO 27001) - există o distincție clară între „eveniment” și „incident”. Amenințarea este cu siguranță o „acțiune” așa cum și „eveniment” este rezultatul unor acțiuni (cu excepția evenimentelor naturale).
b) alertă cibernetică - semnalare referitoare la un posibil incident de securitate cibernetică;	
c) apărare cibernetică - acţiuni desfăşurate în spațiul cibernetic în scopul protejării, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva ameninţărilor asupra infrastructurilor cibernetice destinate apărării naţionale;	Spațiul cibernetic nu înseamnă nimic – cibernetica este o ramură a psihologiei - chiar dacă se dorește folosirea termenului de “securitate cibernetică”, nu trebuie folosit în alte contexte, unde terminologia este profund eronată. Apărarea nu poate fi limitată doar la „acțiuni”, ci implică și „dispozitive”, „proceduri”, „tehnici” aplicate unui sistem informatic sau/și informațiilor procesate, stocate sau care tranzitează sistemul informatic. Definiția, în forma actuală, omite din scopul apărării informațiile. Ce înseamnă „monitorizare”? Există bază legală pentru „monitorizare”? Dacă în baza „monitorizării”, „contracararea agresiunilor” ar implica atacarea/infectarea „centrului de comandă” al atacatorului, ar fi legal? (avem în vedere botnet)
d) atac cibernetic - acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică;	Cine definește dacă ceva este ostil sau nu?
e) audit de securitate cibernetică - activitate prin care se realizează o evaluare sistematică a tuturor politicilor, procedurilor și măsurilor de protecţie implementate la nivelul unei	Esența auditului o constituie „independența auditorului”. Auditul ar trebui să testeze conformitatea (controalele sunt cele pe care

infrastructuri cibernetice, în vederea identificării disfuncţiilor şi vulnerabilităţilor şi a furnizării unor soluţii de remediere a acestora;	legea le cere) și fondul controalelor minimale/măsurilor de securitate implementate (controalele funcționează așa după cum au fost proiectate). Art. 2 Directiva NIS: Statele membre se asigură că autoritățile competente sunt împuternicite să solicite operatorilor de piață și administrațiilor publice: a să furnizeze informațiile necesare pentru evaluarea securității rețelelor și a sistemelor lor informatice, inclusiv documente privind politicile de securitate; (a) să se supună unui audit de securitate efectuat de un organism calificat independent sau de o autoritate națională și să le pună la dispoziție rezultatele acestuia. Auditorul, în lipsa recunoașterii sale ca profesie, nu va avea răspundere civilă profesională. Nu va putea încheia polițe de asigurare de răspundere profesională dacă nu este recunoscut. O soluție în spiritul Directivei NIS ar putea fi înființarea Corpului/Camerei Auditorilor de Sisteme Informaționale (auditul nu ar trebui limitat doar la aspectele ce țin de securitatea tehnică. Este posibil ca autoritățile să fie interesate la un moment dat dacă bugetul alocat pentru asigurarea securității a fost eficient folosit), pe modelul deja existent în zona financiar-contabilă (CAFR). În acest mod ar fi recunoscută oficial profesia. Pentru a putea fi membri și profesa în România, doritorii ar trebui să fi promovat un examen internațional care le atestă competențele în materie de audit și un examen local care să le ateste cunoaștere legislației aplicabilă diferitelor spețe din domeniul IT și cele conexe IT-ului.
f) Catalog ICIN - registru de evidenţă a infrastructurilor cibernetice de interes;	Un registru este un document public, accesibil tuturor celor care îl cer și în care se va nota, după cum prevede art. 14 alin. (6) lit. c) și e), în mod detaliat arhitectura și fluxurile de date. În alte cuvinte acesta devine un “single point of failure”.

g) cerințe minime de securitate cibernetică - condiţii de natură organizatorică, tehnică sau procedurată, destinate implementării politicilor de securitate;	Politica de securitate nu este tot o cerință minimă? Minimal, nu ar trebui ca managementul să aibă asumate politici de securitate?
h) date de jurnalizare - date generate în mod automat de componente software și hardware care descriu istoricul acţiunilor ce au loc la nivelul acestora;	Există relativ puține componente software sau hardware care generează „automat” date de jurnalizare la nivel de aplicație și/sau dispozitiv. Iar atunci când sunt generate, aceste date sunt minimale. Din punct de vedere tehnic, pentru a putea fi gestionată cantitatea de jurnale, cei vizați vor trebui să achiziționeze și implementeze soluții de tip SIEM și să fie definite tipurile de jurnale ce trebuie activate, ce date trebuie colectate, de la ce tipuri de echipamente și perioada de retenție a jurnalelor. În practică se poate întâmpla să descoperi un incident la momentul t0, iar în urma analizei să rezulte că de fapt incidentul a apărut la momentul t-10.
i) date tehnice - descriere generală a infrastructurii cibernetice, rolul și funcţionalităţile asigurate de aceasta, arhitectura, tipuri și număr de utilizatori, fluxuri informaţionale susținute, descrierea capacităţii de stocare/prelucrare, fişiere de jurnalizare a evenimentelor ce au loc în sistemele de securitate software și hardware, sistemele de operare și aplicațiile software;	
j) deţinători de infrastructuri cibernetice - persoane juridice de drept public sau privat care au calitatea de proprietari, administratori sau operatori de infrastructuri cibernetice;	Care este diferența între proprietar și operator? Care este documentul juridic care stabilește că cineva este operator? Este o definiție absolut uluitoare - ce înseamnă persoană juridică ce desfășoară activități pe teritoriul României? Amzom AWS și Facebook au activități pe teritoriul României prin care pun la dispoziție resurse IT. Și o firmă de închiriat telefoane face acest lucru. Despre ce vorbim de fapt?
k) furnizori de servicii de găzduire internet - orice persoană juridică ce desfășoară activităţi pe teritoriul României, care pune la dispoziţie infrastructuri cibernetice, fizice sau virtuale, pentru derularea de activităţi şi servicii ale societății informaţionale;	Nu există termenul de „găzduire internet” în legislația română, sunt incluși în SSI – vezi Legea 365/2002 art. 16.

l) furnizor de servicii de securitate cibernetică - orice persoană juridică ce realizează, în vederea protejării infrastructuritor cibernetice, cel puţin una dintre următoarele activităţi: implementare de politici, proceduri și măsuri, auditare, evaluare, testare a măsurilor implementate, management al incidentelor de securitate;	Consultantul persoană fizică implicat în dezvoltarea de politici, proceduri dar pe care nu le și implementează, va fi furnizor de servicii? În situația în care angajatul unui astfel de furnizor va fi și auditor. Cum se rezolvă incompatibilitatea? Altfel spus: organizația poate fi furnizor de servicii, iar unul dintre angajați înregistrat ca auditor la MCSI? A se vedea prevederea NIS în legătură cu auditul.
m) incident de securitate cibernetică - eveniment survenit în spaţiul cibernetic ale cărui consecințe afectează securitatea cibernetică;	„incident” înseamnă orice circumstanță sau eveniment care are un efect negativ real asupra securității. Deci conform definiției de aici o scanare de porturi este un incident.
n) infrastructuri cibernetice - infrastructuri de tehnologia informaţiei, constând în sisteme informatice, aplicaţii aferente, reţele de comunicaţii electronice;	De ce este necesar să spunem că A=B ? Dacă există deja infrastructuri de tehnologia informației, de ce trebuie să le redenumim? Pentru că avem un nou termen pe care vrem să îl impunem numit „cibernetic”? De ce nu folosim aceeași terminologie în toată legislația? În Codul Penal e definit în mod clar “sistemul informatic”, care e preluat din Convenția de la Budapesta din 2001 cu privire la criminalitatea informatică. Este necesară o terminologie unitară, atât în lege, cât și în corelare cu restul cadrului normativ.
o) infrastructuri cibernetice de interes naţional - infrastructuri cibernetice deţinute de persoane juridice de drept privat, care susţin servicii publice sau de interes public ori servicii ale societăţii informaţionale, sau infrastructuri cibernetice deţinute de autorităţi și instituţii publice, a căror afectare aduce atingere securităţii naţionale, sau prejudicii grave statului român ori cetăţenilor acestuia;	Avem cel puțin 400 000 de SSI în România. Cum pot să estimeze aceștia dacă afectarea IT-ului aduce atingere securității naționale? Textul este extrem de vag. Cine stabilește dacă s-a adus atingere securității naționale și cum? Care sunt criteriile? Textul este extrem de neclar.
p) politici de securitate cibernetică - principii și reguli generale necesar a fi îndeplinite pentru asigurarea securităţii infrastructurilor cibernetice;	Politica este un control managerial prin care se stabilesc obiective și se alocă responsabilități. Este responsabilitatea directă a managementului. Orice audit de securitate ar trebui să pornească „top-down”: politici-proceduri/standarde/principii-controale tehnice.

q) managementul incidentului de securitate cibernetică - ansamblul proceselor ce prevăd detectarea, raportarea, analiza și răspunsul la incidentul de securitate cibernetică;	Directiva NIS: „administrarea incidentului” înseamnă toate procedurile utilizate pentru analiză, limitare și răspuns în cazul unui incident;
r) risc de securitate în spaţiul cibernetic - probabilitatea ca o ameninţare să se materializeze, exploatând o vulnerabilitate specifică infrastructurii cibernetice;	
s) securitate cibernetică - stare 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, precum și rezilienţa și stabilitatea resurselor și serviciilor publice sau private din spatiul cibernetic;	Directiva NIS: „securitate” înseamnă capacitatea unei rețele sau a unui sistem informatic de a rezista, la un nivel de încredere dat, unei acțiuni accidentale sau răuvoitoare care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise ori a serviciilor conexe oferite de rețeaua sau de sistemul informatic respectiv sau accesibile prin intermediul acestora;
t) Sistem de Control Industrial - infrastructuri și *sisteme informatice* de comandă și control utilizate pentru a automatiza procesele industriale;	Observăm că este totuși folosit sistemul informatic ca termen. Din nou subliniem probleme majore terminologice.
u) spaţiul cibernetic - mediul virtual generat de infrastructurile cibernetice, incluzând conţinutul informaţional, procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta;	Spațiu cibernetic = Internet? Există un motiv bun pentru care Internetul nu este definit în legislația națională sau europeană – pentru respectarea principiului neutralității tehnologice. Cum se generează mediul virtual?
v) vulnerabilitate în spaţiul cibernetic - slăbiciune în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o ameninţare.	Vulnerabilitățile există și în lipsa „slăbiciunilor în proiectare și implemeentare”. Implicit se poate prezuma că orice aplicație conține și vulnerabilități care la momentul lansării în piață a respectivei aplicații nu sunt cunoscute. Definiția ar trebui tradusă corect și complet după NIST 800-100.
Art. 4 - Principiile care stau la baza prezentei legi sunt:	Principiile trebuie revăzute după standardele internaționale – vezi OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

a) asigurarea protejării, în spațiul cibernetic, a dreptului la viaţă intimă, familială și privată al cetățenilor, în special a datelor cu caracter personal gestionate de către detinătorii de infrastructuri cibernetice;	Nimic din acest principiu nu se regăsește în lege. Faptul că este introdus aici nu înseamnă nimic. Nu există nimic specific în lege cu privire la raportarea pierderii de date cu caracter personal care ar fi fost principalul obiectiv în acest sens. Mai mult, în domeniul protecției datelor, există deja o autoritate competentă – ANSPDCP, care are obligații de verificare a securității datelor, conform Ordinul Avocatului Poporului 52/2002 privind aprobarea Cerințelor minime de securitate a prelucrarilor de date cu caracter personal.
b) asigurarea securităţii cibernetice prin responsabilizarea deţinătorilor de infrastructuri cibernetice, astfel încât aceștia să evalueze capabilităţile proprii de securitate cibernetică şi nivelul la care se situează;	
c) creșterea capacităţii de reacție la incidentele cibernetice și diminuarea impactului acestora asupra resurselor şi serviciilor infrastructurilor cibernetice prin impunerea de cerinţe minime de securitate cibernetică și asigurarea rezilienței infrastructurilor cibernetice;	
d) asigurarea nivelului de încredere necesar pentru dezvoltarea societăţii informaţionale și a mediului de afaceri în spaţiul cibernetic și asigurarea accesului egal și nediscriminatoriu al persoanelor la informaţii și servicii publice oferite prin intermediul infrastructurilor cibernetice;	Faptul că ai obligații de raportare nu crește încrederea în Internet! Cum asigură legea accesul egal și nediscriminatoriu? Prin ce dispoziție?
e) asigurarea unei guvernanţe participative, democratice și eficiente a spaţiului cibernetic prin cooperarea autorităţilor competente cu sectorul privat;	Nu există nimic în text care să vorbească de cooperare reală, degeaba punem principii dacă textul legii este contrar lor.
f) cooperarea la nivel naţional, între instituțiile cu competenţe în materie și internaţional, cu persoane juridice de drept public și privat, implicate în asigurarea securitătii cibernetice.	Cooperarea cu persoane juridice de drept privat nu există în lege.
Art.5 (1) La nivel naţional activitatea de realizare a securităţii cibernetice se organizează și se	E o informație gresită. Realizarea securității cibernetice pe calculatorul propriu o face fiecare și este descentralizată. La fel se întâmplă și în

desfașoară în mod unitar, potrivit prezentei legi.	cadrul unei firme sau în cadrul unei asociații. Poate vreți să vă referiți la realizarea securității cibernetice la nivelul ICIN – atunci da, se poate discuta să existe o organizare unitară, dar ca desfășurare e tot descentralizată.
(2) În acest scop, cooperarea în domeniu se organizează ca Sistem Naţional de Securitate Cibernetică, la care participă autorități și instituții publice cu atribuții și responsabilităţi potrivit dispoziţiilor prezentei legi.	Deci cooperarea există doar între autoritățile statului – contrazice principiul de mai sus.
(3) În exercitarea comptetențelor, autoritățile și instituțiile publice cooperează cu sectorul privat şi cu mediul academic, asociaţiile profesionale și organizaţiile neguvernamentale.	Cum? Concret? Ce vrea sa spună acest articol?
Art. 7 (5) În cadrul lucrărilor Consiliului Operativ de Securitate Cibernetică pot prezenta puncte de vedere cu privire la problemele aflate pe agenda de lucru, reprezentanţi ai furnizorilor de servicii de securitate cibernetică, ai mediului academic, ai entităților de tip CERT private și ai altor instituţii publice.	Deci firmele – producători de soluții de securitate nu pot participa.
(6) În exercitarea atribuţiilor sale, Consiliul Operativ de Securitate Cibernetică analizează şi evaluează starea securităţii cibernetice, formulează și înaintează Consiliului Suprem de Apărare a Țării propuneri privind: a) măsuri de armonizare a reacţiei autorităţilor competente ale statului în situațiigenerate de ameninţări și atacuri cibernetice, care necesită schimbarea nivelului de alertă cibernetică; b) solicitarea, în caz de necesitate, de asistenţă din partea altor state sau organizaţii și organisme internaționale;	
c) modalitatea de răspuns la solicitările de asistenţă adresate României din partea altor state sau organizaţii și organisme internaționale;	Este nevoie să clarificați la ce tipuri de solicitări vă referiți. Dacă toate solicitările pe securitate cibernetică a țării merg pe la COSC și CSAT o să fim cea mai lentă țară care răspunde la astfel de solicitări.
d) planuri sau direcţii de acţiune, în funcţie de concluziile rezultate și evoluţia spatiului	

cibernetic; e) direcţii de dezvoltare sau programe de investiţii în domeniul securităţii cibernetice.	Trebuie adăugat la litera e) faptul că se referă la ICIN.
Art.8 - Pentru realizarea securităţii cibernetice, Consiliul Operativ de SecuritateCibernetică cooperează cu organismele de coordonare sau de conducere constituite, la nivel naţional, pentru managementul situaţiilor de urgenţă, a acţiunilor in situaţii de criză în domeniul ordinii publice, pentru prevenirea și combaterea terorismului şi pentru apărarea națională.	Dar niciodată cu sectorul privat?
Art.9 - Pentru asigurarea securităţii cibernetice, instituțiile publice din Românіaau atribuţii după cum urmează: a) Ministerul Comunicaţiilor și pentru Societatea informaţională, cu rol de autoritate de reglementare şi control al implementării măsurilor privitoare la asigurarea securităţii cibernetice, cu excepţia instituţiilor prevăzute la lit. d) şi e); b) Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică, desemnat punct naţional de contact cu entitățile de tip CERT naţionale şi internaţionale și autoritate competentă pentru coordonarea activităţilor în domeniul securității cibernetice a infrastructurilor cibernetice, altele decât cele menționate la lit. c), d) și e); c) Serviciul Român de informaţii, prin Centrul Naţional de Securitate Cibernetică, desemnat autoritate competentă pentru coordonarea activităților în domeniul securităţii cibernetice organizate și desfăşurate la nivelul infrastructurilor cibernetice de interes naţional, cu excepția infrastructurilor cibernetice de interes naţional aflate în administrarea sau responsabilitatea celorlalte autorităţi prevăzute la lit. d) şi e); d) Autoritatea Naţională pentru Administrare și Reglementare în Comunicaţii, desemnată autoritate competentă pentru coordonarea activităților în domeniul securităţii cibernetice a	MCSI nu are suficient personal care să facă acest control și nici nu poate avea – nimeni nu îți face control pe securitate informatică și e plătit cu 1600 de RON pe lună. Dacă vorbim de cooperare ar fi bine ca CERT-ul actual să devină într-adevăr o instituție civilă – vezi detalii în comentariul nostru din iunie 2015 - https://www.apti.ro/sites/default/files/Opinia%20ApTI%20securitate%20cibernetica%20iun%202014.pdf Acest aspect este neconstituțional conform Deciziei CCR 17/2015. Deja reglementat prin OUG 111/2011. Ce aduce în plus această mențiune?

furnizorilor de rețele publice de comunicaţii electronice sau furnizorilor de servicii de comunicaţii electronice destinate publicului; e) Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Autoritatea Naţională pentru Admninistrare și Reglementare în Comunicaţii, Serviciul Român de Informaţii, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale și Serviciul de Protecţie şi Pază sunt autorităţi responsabile de securitate cibernetică cu rol în stabilirea de structuri şi implementarea de măsuri proprii privind coordonarea şi controlul activităţilor referitoare la asigurarea securităţii cibernetice pentru infrastructurile cibernetice, inclusiv infrastructurile cibernetice de interes naţional, aflate în domeniul lor de activitate și responsabilitate.	Observăm că dacă este vorba de instituțiile subordonate sunt suficiente reglementări interne. Mai exact care sunt aceste infrastructuri cibernetice de interes național? Legea este neclară și imprecisă. Mai mult, directiva NIS prevede analiza și identificarea acestora și efectuarea unui studiu (vezi paragrafele legate de articolele 3a(1) și 3a(2) din http://www.consilium.europa.eu/en/press/press-releases/2015/12/pdf/st15229-re02_en15_pdf/
Art. 10 - Cerinţele minime de securitate cibernetică și politicile de securitate cibernetică pentru infrastructurile cibernetice de interes naţional se stabilesc de Ministerul Comunicațiilor și pentru Societatea Informaţională, cu sprijinul autorităţilor prevăzute de art. 9 lit. b) - e), prin normele metodologice de aplicare ale prezentei legi.	Stabilirea acestor aspecte prin norme metodologice este contrară Deciziei CCR 17/2015.
Art.11 (1) Autoritatea Naţionată pentru Administrare și Reglementare în Comunicaţii stabilește cerinţele minime de securitate cibernetică pentru infrastructurile cibernetice, care sunt în competența sa, conform art. 9 litera d). (2) Ministerul Comunicaţiilor și pentru Societatea Informaţională stabileşte cerinţele minime de securitate cibernetică pentru infrastructurile cibernetice, aflate în aria de competență a autorităţilor prevăzute la art. 9 lit. b). (3) Fac excepţie de la prevederile alin. (1) și (2) infrastructurile cibernetice de interes național.	Există deja – decizia ANCOM nr. 512/2013. Are competențele tehnice MCSI să facă acest lucru? Realmente, nu să le primească de la alte autorități.
Art.12 (1) Autorităţile prevăzute de art. 9 lit. b) - e) au următoarele obligaţii: a) să adopte planuri de acţiune	

corespunzătoare fiecărui nivel de alertă cibernetică; b) să asigure, în cazul instituirii unui nivel de alertă cibernetică, sprijinul pentru implementarea măsurilor aferente deţinătorilor de infrastructuri cibernetice; c) să asigure colectarea notificărilor şi evaluarea datelor și informaţiilor cu privire la incidente și atacuri cibernetice la adresa infrastructurilor cibernetice, aflate în domeniul lor de competenţă, activitate sau responsabilitate; d) să notifice deţinătorii de infrastructuri cibernetice aflate în domeniul de competenţă, activitate sau responsabilitate cu privire la incidente de securitate cibernetică sau vulnerabilităţi şi atacuri cibernetice identificate la nivelul acestora; e) să coordoneze managementul incidentelor de securitate cibernetică identificate în cadrul infrastructurilor cibernetice aflate în domeniul lor de competenţă; f) să acorde sprijin deţinătorilor de infrastructuri cibernetice din zona de competenţă, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgenţă pentru remedierea efectelor incidentelor de securitate cibernetică; g) să desfăşoare activităţi de informare și comunicare publică; h) să organizeze sesiuni de formare și instruire în domeniul securităţii cibernetice, pentru îmbunătăţirea capacităţilor deţinătorilor de infrastructuri cibernetice; i) să organizeze sau să participe la exerciţii naționale de securitate cibernetică; j) să coopereze și să-și comunice reciproc date referitoare la securitatea cibernetică, inclusiv către celelalte autorităţi şi instituţii publice sau deţinători de infrastructuri cibernetice; k) să solicite convocarea Consiliului Operativ de Securitate Cibernetică, potrivit propriilor competenţe, inclusiv pentru ridicarea nivelului de alertă cibernetică.	Ce înseamnă măsuri aferente? Pentru o mai bună transparență, ar trebui să existe obligația publicării unui raport anual. ANCOM deja o face. La ce “date referitoare la securitatea cibernetică” ne referim? Că a apărut un ransomware periculos? Sau că site-ul MCSI a fost infectat ? Ambele intră în definiția propusă. Deci date referitoare la securitatea cibernetică sunt trimise de la autorități la orice SRL? Cum? Când? De ce?

(2) Autorităţile prevăzute la alin. (1) pot constitui structuri specializate în realizarea de audit de securitate cibernetică și pot constitui și operaţionaliza structuri specializate de securitate cibernetică de tip CERT.	Este ilegal conform Deciziei CCR 17/2015 – nu poți îndeplini dubla calitate de auditor și autoritate. Dacă nu este auditor, ce înseamnă structuri de tip CERT?
Art.14 (1) În procesul identificării infrastructurilor cibernetice de interes naţional, deţinătorii de infrastructuri cibernetice au obligaţia de a furniza autorităților de la art. 9 datele şi informaţiile necesare pentru întocmirea Catalogului ICIN.	Vorbim probabil de cel puțin jumătate de milion de firme care au un calculator. La asta se referă legea? Și dacă nu vor să furnizeze, ce sancțiune va exista? Răspundere civilă delictuală?
(2) La propunerea autorităţilor prevăzute la art. 9 literele b) - e), Ministerul Comunicațiilor și pentru Societatea Informaţională întocmește Catalogul ICIN.	Responsabilitatea pentru întocmirea registrului va reveni MCSI care trebuie să facă Catalogul ICIN. Acest catalog este în mod logic este un document public, accesibil tuturor celor care îl cer și în care se va nota, după cum prevede art. 14 alin. (6) lit. c) și e), în mod detaliat arhitectura și fluxurile de date. Nu putem decât să concludem încă o dată că este o demostrație genială de “single point of failure”.
(3) Se exceptează de la prevederile alin. (1) şi (2) infrastructurile cibernetice de interes naţional 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 Stat.	
(4) Infrastructurile cibernetice de interes naţional prevăzute la alin. (3) se comunică Centrului Naţional de Securitate Cibernetică, cu excepţia celor constituite la nivelul Autorităţilor Desemnate de Securitate, care deţin Structuri Interne INFOSEC acreditate potrivit prevederilor legate în vigoare.	Ce înseamnă acronimul Autorități Desemnate de Securitate și ce rol are? Ce înseamnă structuri interne INFOSEC? Nu există în lege. Care prevederi legale? Neprecizarea acestor prevederi este împotriva Deciziei CCR 17/2015.
(5) Deţinătorii de infrastructuri cibernetice de interes naţional prevăzuți la art. 9 litera c) trebuie să notifice Centrul Naţional de Securitate Cibernetică, în termen de 10 zile, cu privire la orice modificare intervenită în statutul juridic al infrastructurilor cibernetice de	Care este relevanța modificării statului juridic? Dacă un asociat dobândește 0.001% din capitalul social, de ce este relevant pentru CNSC? Cu ce protejează mai bine securitatea cibernetică? Deci orice modificare în configurația

interes naţional, respectiv în configuraţia acestora. (6) Informaţiile necesare pentru întocmirea Catalogului ICIN trebuie să cuprindă următoarele: a) descrierea generală a infrastructurilor cibernetice de interes naţional; b) rolul și funcţionalităţile asigurate de infrastructurile cibernetice de interesnational; c) arhitectura infrastructurilor cibernetice de interes naţional; d) tipuri și număr de utilizatori; e) fluxuri informaţionale susţinute, precum şi dinamica datelor stocate/prelucrate, capacitatea de stocare/prelucrare.	infrastructurii trebuie notificată? Inclusiv adăugarea unui utilizator este o modificare! În unele cazuri fluxul se schimbă zilnic. Cum dă de exemplu Vodafone SRL spațiul de stocare și prelucrare?
Art. 15 - Pentru derutarea procesului de identificare a infrastructurilor cibernetice de interes naţional, deţinătorii de infrastructuri cibernetice, sub coordonarea autorităţilor competente, vor evalua măsura în care infrastructurile cibernetice proprii se încadrează în cel puţin una dintre următoarele categorii de potențiale infrastructuri cibernetice de interes național: a) infrastructuri cibernetice destinate susţinerii actului de guvernare; b) infrastructuri cibernetice destinate susţinerii administrației publice; c) infrastructuri cibernetice destinate susţinerii serviciilor publice; d) infrastructuri cibernetice prin intermediul cărora se asigură accesul cetăţenilor și a mediului de afaceri la servicii publice; e) infrastructuri cibernetice destinate susţinerii funcţiilor de apărare, ordine publică, justiţie și securitate naţională;	Articolele 15-16 sunt vagi și inutile. Directiva NIS vine cu un exemplu excelent în care identifică în mod clar cine pot fi aceste ICIN. Cum adică sub coordonarea autorităților? Nu e de fapt o autoevaluare? Definițiile sunt extrem de largi. Serviciul public este un concept mai incert decât credeți (vezi Revista Transilvană de Ştiinţe Administrative, VIII, 2002, pp. 51-60). Într-un sens larg cuprinde toate instituțiile de învățământ – publice și private. Aceasta ar trebui să fie ICIN? Orice calculator prin care eu mă conectez la un serviciu public este o astfel de infrastructură. Propunerea de lege se referă și la acest fel de cazuri?

f) infrastructuri cibernetice destinate tranzacţiilor economice și financiar-bancare; g) infrastructuri cibernetice de tip Sistem de Control Industrial; h) infrastructuri cibernetice care asigură supraveghere, sesizare, avertizare și alertă; i) infrastructuri cibernetice care asigură servicii de securitate cibernetică; j) infrastructuri cibernetice care asigură componenta națională destinată cooperării în cadrul NATO, UE sau al organizaţiilor la care România este parte; k) infrastructuri cibernetice pentru navigaţie, radiolocaţie și identificare; l) infrastructuri cibernetice care susţin transmisia sau retransmisia serviciilor de programe de televiziune sau radiodifuziune; m) infrastructuri cibernetice utilizate de către furnizorii de servicii poștale.	
Art.16 (1) Evaluarea potenţialului impact asupra securității infrastructurilor cibernetice prin compromiterea confidenţialităţii, integrităţii, disponibilităţii, autenticității sau a non-repudierii datelor, resurselor și serviciilor se realizează pe baza următoarelor criterii:	Criteriile sunt extrem de subiective – legea nu este deloc predictibilă – vezi Decizia CCR nr. 17/2015.
Art.17 (1) Sistemul Naţional de Alertă Cibernetică este un ansamblu organizat de măsuri tehnice și procedurale destinate prevenirii şi contracarării activităţilor de natură să afecteze securitatea cibernetică la nivel naţional. (2) În cadrul Sistemului Naţional de Alertă Cibernetică, stările de ameninţarereflectă gradul de risc pentru securitatea cibernetică și sunt identificate prin niveluri de alertă cibernetică. Acestea pot fi instituite pentru întreg teritoriul naţional, pentru o zonă geografică delimitată, pentru un anumit domeniu de activitate sau pentru una sau mai multe persoane juridice de drept public sau privat. (3) Instituirea nivelurilor de alertă cibernetică, precum și trecerea de la un nivel la altul se aprobă de către Consiliul Suprem de Apărare a Țării, la propunerea Consiliul Operativ de Securitate Cibernetică. (4) Deţinătorii de infrastructuri cibernetice au obligaţia să sprijine autorităţile competente pentru implementarea măsurilor	Cum se poate stabili unde începe județul Dolj și unde se termină pe Internet? Cum se pot ataca acestea? - vezi decizia CCR Și dacă nu se întâmplă implementarea, ce sancțiuni există?

corespunzătoare fiecărui nivel de alertă cibernetică. (5) Personale juridice de drept public sau privat deţinători de infrastructuri cibernetice de interes naţional elaborează planuri de acţiune proprii, corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligaţia să le pună în aplicare la instituirea unui nivel de alertă cibernetică. (6) La modificarea nivelului de alertă cibernetică deţinătorii de infrastructuri cibernetice de interes național au obligaţia informării deîndată a Centrului Naţional de Securitate Cibernetică cu privire la gradul de afectare a infrastructurii cibernetice și măsurile preconizate.	
Art.18 (1) Deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2, lit. a) - c) adoptă măsuri organizatorice și tehnice pentru: a) evaluarea infrastructurilor cibernetice deţinute în vederea susținerii demersurilor de întocmire a Catalogului ICIN; b) elaborarea și implementarea de politici și planuri de securitate cibernetică, cu respectarea cerinţelor minime de securitate; c) managementul incidentelor de securitate cibernetică; d) prevenirea accesului neautorizat la infrastructurilor cibernetice; e) garantarea diseminării datelor deţinute la nivelul infrastructurilor cibernetice exclusiv persoanelor autorizate să cunoască conţinutul acestora. (2) Faţă de cele prevăzute la alin. (1), deţinătorii de infrastructuri cibernetice de interes naţional adoptă, suplimentar, măsuri organizatorice și tehnice pentru: a) implementarea unui sistem de management al riscului; b) elaborarea de planuri de acţiune pe niveluri de alertă cibernetică; c) auditarea nivelului de securitate cibernetică a infrastructurilor cibernetice de interes național.	Acestea nu se pot face cu costuri 0, cum este prevăzut în expunerea de motive. De asemenea punctele b și c nu asigură scopul legii – faptul că ai o politică de securitate cibernetică nu te ajută cu nimic concret și nu îți garantează ca vei proteja datele cetățenilor. Auditarea se face anual, lunar sau zilnic?
Art.20 (1) Deţinătorii de infrastructuri cibernetice prevăzuţi la art. 2 lit. a) - c) au următoarele obligaţii: a) să asigure implementarea cerinţelor minime	Obligațiile sunt exagerate față de scopul urmărit.

de securitate cibernetică; b) să notifice deîndată autoritatea competentă cu privire la incidentele de securitate cibernetică identificate; c) să se asigure că datele şi/sau informaţiile referitoare la configurarea și protecţia infrastructurilor cibernetice sunt diseminate exclusiv persoanelor autorizate să le Cunoască; d) să nu permită accesul la datele de conţinut din infrastructurile cibernetice deţinute sau aflate în competenţă, în lipsa unei ~~înștiinţări scrise din partea autorităţilor abilitate, privind existenţa unei~~ autorizaţii emise de judecător, în condiţiile legii; e) să gestioneze incidentele de securitate cibernetică; f) să nu afecteze, prin acţiunile proprii, securitatea altor infrastructuri cibernetice. (2) Față de cele prevăzute la alin. (1), deţinătorii de infrastructuri cibernetice de interes naţional au, suplimentar, următoarele obligaţii: a) să efectueze auditări de securitate cibernetică, anual sau când este necesar; b) să constituie structuri sau să desemneze persoane responsabile privind coordonarea activităților de securitate cibernetică; c) să transmită autorităţilor competente copie după rapoartele de audit de securitate cibernetică și <u>date privind evoluţiile în domeniul securităţii cibernetice</u> la nivelul infrastructurilor cibernetice deținute, trimestrial și ori de câte ori li se solicită; d) să elaboreze și să transmită autorităţii competente planuri de acţiune corespunzătoare fiecărui nivel de alertă cibernetică, pe care au obligaţia să le pună în aplicare la instituirea unui nivel de alertă cibernetică; e) <u>să transmită autorităţilor competente date referitoare la rezultatele măsurilor de contracarare a incidentelor de securitate cibernetică aplicate</u>.	Pentru clarificarea textului este nevoie de ștergerea următoarelor cuvinte: „înștiințări scrise din partea autorităților abilitate, privind existența unei”. Este nevoie de mandatul judecătorului. Punct. Nu să existe doar o înștiintare că acesta există. Ce sunt datele privind evoluțiile în domeniul securității cibernetice? Adică numărul de atacuri sau ce? Sunt date statistice? Obligația aceasta presupune angajarea a cel puțin 2-3 oameni care să facă doar asta.
Art.21 (1) Furnizorii de servicii de comunicaţii electronice destinate publicului au obligaţia de a-şi notifica utilizatorii și abonaţii de îndată ce au fost sesizaţi de autoritatea competentă, <u>dar nu mai târziu de 24 de ore</u> din momentul în care au fost sesizaţi de autorităţile competente potrivit prezentei legi, cu privire la situaţiile în	Din sintagma „dar nu mai târziu de 24 de ore” rezultă că autoritățile competente au cunoștință că sistemul a fost compromis înaintea deținătorului sistemului.

care sistemele informatice utilizate de aceştia au fost implicate în atacuri cibernetice şi de a recomanda măsurile necesare în vederea restabilirii condiţiilor normale de funcţionare. (2) Notificarea prevăzută la alin. (1) se realizează în scris, prin mijloaceelectronice, sau prin orice altă modalitate stabilită prin contractul de furnizare de Servicii.	
Art.22 (1) Furnizorii de servicii de securitate cibernetică ce desfăşoară activităţi pe teritoriul României au obligaţia să notifice autorităţile competente, deîndată dar nu mai târziu de 24 de ore, cu privire la identificarea unor ameninţări sau vulnerabilităţi critice a căror manifestare poate afecta infrastructura cibernetică a deţinătorului sau a unor terţi. (2) Notificarea prevăzută la alin. (1) se realizează în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord. (3) Furnizorii de servicii de securitate cibernetică care realizează audit de securitate pentru infrastructuri cibernetice de interes naţional au obligaţia de a se înregistra la Ministerul Comunicaţiilor şi pentru Societatea Informaţională, potrivit normelor aprobate prin ordin al ministrului, care stabilesc condiţiile pentru înregistrarea şi radierea acestora din Registrul Furnizorilor de Audit de Securitate Cibernetică.	Ce sunt vulnerabilitățile critice? Deci practic trebuie să notifice autoritatea, dar nu clientul? Și dacă clientul nu este din România? Și dacă clientul nu dorește ca amenințarea să fie notificată către statul român? Directiva NIS: Statele membre se asigură că administrațiile publice și operatorii de piață notifică autorității competente incidentele care au un impact semnificativ asupra securității serviciilor esențiale pe care le furnizează. Dacă se dorește acest lucru, atunci trebuie o lege separată și nu o decizie a MCSI – vezi decizia CCR.
~~**Art.23**~~ ~~(1) Furnizorii de servicii de găzduire internet care desfăşoară activităţi pe teritoriul României au obligaţia să acorde sprijin autorităţilor competente, respectiv organelor de urmărire penală, pentru punerea în aplicare, potrivit legii, a oricărui act de autorizare a restrângerii temporare a exerciţiului drepturilor şi libertăţilor persoanelor, emis de judecător.~~ ~~(2) Furnizorii de servicii de găzduire internet au obligaţia de a înregistra şi stoca date de~~	Articolul acesta nu are nicio legătură cu restul legii – este plasat aici în mod bizar și neclar – dacă el are vreun scop, atunci trebuie precizat din start. Propunem ștergerea lui integrală pentru că nu este corelat cu restul actului normativ.

~~jurnalizare a activităţilor din sistemele informatice deţinute care fac obiectul actului de autorizare de la alin. (1), pe toată perioada de valabilitate a acestuia.~~ ~~(3) Persoanele care sunt chemate să acorde spriijn tehnic la punerea în executare a actelor de autorizare, precum și persoanele care iau la cunoștință despre aceasta au obligaţia să păstreze secretul operațiunii efectuate, sub sancţiunea legii penale~~	
Art. 24 – (1) Notificarea incidentelor de securitate cibernetică se transmite în modalitatea stabilită de autoritatea competentă şi trebuie să conţină, în mod obligatoriu, următoarele elemente: a) elementele de identificare ale infrastructurii cibernetice afectate; b) descrierea incidentului; c) perioada de desfăşurare a incidentului; d) impactul incidentului. (2) Pentru gestionarea incidentelor de securitate cibernetică, deținătorii de infrastructuri cibernetice pot solicita sprijinul furnizorilor de servicii de securitate cibernetică sau al autorităților prevăzute de art. 9 lit. b) - e), potrivit competențelor acestora, cărora le pot pune la dispoziție date tehnice referitoare la incidentele şi atacurile cibernetice pe care le gestionează, cu asigurarea anonimizării datelor cu caracter personal ~~deţinute~~. (3) Datele tehnice transmise în condițiile prevăzute la alin. (2) nu vor conţine: a) informații clasificate; b) date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate.	În mod normal aceasta ar trebui să fie doar pentru ICIN. Anonimizarea datelor trebuie să fie ireversibilă, iar cuvântul deținute trebuie înlocuit cu „conținute în date tehnice”. La ce date se referă propunerea de lege? Și atacatorul este o terță entitate implicată și are interese legitime...
Art. 27 – (1) În situaţia în care în cadrul activităţilor de management al incidentului de securitate cibernetică sunt identificate informaţii sau fapte care pot indica săvârşirea unei infracţiuni care vizează infrastructuri cibernetice este obligatorie sesizarea organelor judiciare. (2) Autoritatea competentă are obligaţia	Orice atac informatic este o faptă penală. Se știe foarte bine că firmele private au reticențe – din motive multiple – să raporteze toate atacurile la poliție, iar articolul acesta este un element în plus pentru a face legea neaplicabilă. Pe de o parte o să existe un număr de mii de cereri către procurori, care vor fi suprasolicitați de cazuri cu autori necunoscuți.

să sprijine activităţile derulate de organele de cercetare penală pentru investigarea infracţiunilor ce vizează sistemele informatice aparţinând unor infrastructuri cibernetice aflate în competenţa acesteia.	Pe de altă parte trebuie să ne reamintim că dintr-un anumit moment procesul penal devine public și deci toată lumea va ști de atacul asupra unei anumite firme.
Art. 28 – În baza notificărilor primite şi a rezultatelor propriilor activităţi de identificare a ameninţărilor, riscurilor şi vulnerabilităţilor la adresa securităţii cibernetice, autorităţile competente emit înştiinţări adresate, după caz, publicului, altor autorităţi competente sau deţinătorilor de infrastructuri cibernetice aflaţi în aria de competenţă, cu privire la evenimente sau stări de fapt care afectează securitatea cibernetică a României.	Înștiințările ar trebui să fie publice.
Art. 29 – (1) Apărarea cibernetică cuprinde ansamblul de măsuri şi activităţi adoptate şi desfăşurate de autorităţile cu atribuţii în domeniul apărării ţării şi securităţii naţionale pentru protejarea infrastructurilor cibernetice destinate apărării naţionale şi a infrastructurilor cibernetice naţionale care susţin activităţile NATO şi UE. (2) Infrastructurile cibernetice destinate apărării naţionale şi măsurile privind apărarea cibernetică a acestora se stabilesc la intrarea în vigoare a prezentei legi şi se actualizează periodic prin hotărâre a Consiliului Suprem de Apărare a Ţării.	Ce este o infrastructură care susține activitatea UE? Firma românească care administrează portalul de date al Comisarului de Mediu UE este în această categorie? De ce?
CAPITOLUL VII - DISPOZIŢII FINALE	Vezi decizia CCR – măsurile ce afectează drepturile fundamentale trebuie reglementate prin lege.

Susținători

Asociația pentru Tehnologie și Internet
Centrul pentru Jurnalism Independent
ActiveWatch
Asociația Pentru Apărarea Drepturilor Omului în România – Comitetul Helsinki (APADOR-CH)
Centrul pentru Inovare Publică
Asociația Miliția Spirituală
Centrul de Resurse Juridice

București, 25.02.2016