Propuneri de amendamente - Proiect de lege privind securitatea informatică
23 septembrie 2014

Preambul

Organizaţiile semnatare susţin, **<u>în principal</u>**, **respingerea proiectul de lege privind securitatea cibernetică** şi propunerea unui nou proiect **numai** după adoptarea directivei UE **privind securitatea informatică (directiva NIS), aflată într-un stadiu avansat de adoptare**.

Actualul proiect are probleme fundamentale de concepţie, propunând o serie de măsuri cu efect limitativ asupra dreptului la viaţă privată în zona digitală şi încalcă în mod evident reglementările europene discutate astăzi pe subiectul securităţii informaţiei. De asemenea, **subiectul instituţiei competente conform acestei legi este o chestiune complexă**, care ar putea avea nevoie de dezbateri publice detaliate pentru a îndeplini criteriile adoptate în proiectul de directivă NIS la nivel european în prima lectură de către Parlamentul European. Cum această directivă nu este încă adoptată la nivel**ul Uniunii Europene, este foarte probabil ca, în funcţie de textul exact adoptat la nivel european, să fie necesară modificarea şi completarea legii naţionale** privind securitatea informatică. **Din acest motiv, ar fi oportună respingerea proiectului actual şi propunerea unui nou proiect după adoptarea directivei UE.**

<u>În subsidiar</u>, dacă decideţi adoptarea acestui proiect este necesar a se rezolva cel puţin problemele majore identificate mai jos:

1. **Accesul la datele informatice trebuie permis doar în condiţiile Codului de Procedură Penală.**

Directiva NIS nu specifică nicăieri ca organizaţiile care intra sub incidenţa sa sunt obligate în vreun fel să permită accesul la sistemele proprii sau, cu atât mai puţin, la datele personale deţinute, acest aspect fiind reglementat la nivelul fiecărui stat membru. Textul proiectului de lege autohton, în schimb, acordă unei întregi pleiade de organizaţii cu rol de serviciu de informaţii, de aplicare a legii sau de apărare dreptul să ceară şi să obţină accesul la aceste sisteme şi date, fără implicarea vreunui judecător, fără vreo referire la protecţia datelor şi doar cu o foarte vagă referire la vreo limită bazată pe principiul proporţionalităţii, care poate fi ocolită extrem de facil.

Orice articol care contrazice acest principiu încalcă dreptul la viaţă privată, după cum este subliniat de decizia Curţii Constituţionale 440/8 Iulie 2014[1]:

1 Disponibilă la http://www.ccr.ro/files/products/Decizia_440_20141.pdf

„**Solicitările de acces la datele reținute** în vederea utilizării lor în scopul prevăzut de lege, formulate de către organele de stat cu atribuții în domeniul securității naționale, **nu sunt supuse autorizării sau aprobării instanței judecătorești, lipsind astfel garanția unei protecții eficiente** a datelor păstrate împotriva riscurilor de abuz precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date. Această împrejurare este de natură a constitui o ingerință în drepturile fundamentale la viață intimă, familială și privată și a secretului corespondenței și, prin urmare, contravine dispozițiilor constituționale care consacră și protejează aceste drepturi."

2. **Lista subiecţilor legii trebuie definită în mod exhaustiv – de exemplu prin enumerarea tipurilor de infrastructuri vizate într-o Anexă a legii**

În proiectul actual avem doar niște descrieri foarte vagi al organizațiilor vizate. Acestea sunt atât de ambigue încât echipamentele oricărei organizații sau persoane (chiar și persoanele fizice) care are de a face cu rețelele de comunicații sau care folosește în orice fel rețele de comunicații pot fi catalogate cel puțin drept „infrastructuri cibernetice". Directiva NIS stipulează clar și exhaustiv ce organizații intră sub incidența sa - numiți operatori de piață – și propunem folosirea acestei liste drept standard și pentru acest proiect.

3. **Desemnarea unei autorităţi competente care să întrunească condiţiile minimale dezbătute la nivel european - „*organisme civile, sub completă supraveghere democratică şi nu ar trebui să îndeplinească nici un fel de rol de serviciu de informaţii, de aplicare a legii sau de apărare sau să aibă legături organizaţionale de orice fel cu organizaţii active în aceste domenii." (Considerentul 10 a)*[2]**

Propuneri concrete amendamente :

Text proiect de lege	Amendamente propuse	Motivare
Titlu: LEGEA SECURITĂȚII CIBERNETICE A ROMÂNIEI	LEGEA SECURITĂȚII **INFORMAȚIONALE** A ROMÂNIEI	Termenul stabilit la nivel internațional este securitatea informației sau securitatea sistemelor informatice, unde există standarde recunoscute (ex. ISO 27001) și auditori de securitatea informației recunoscuți internaționale (vezi de ex. ISACA – Chapter Romania). Termenul de sistem informatic este

2*Rezoluția legislativă a Parlamentului European din 13 martie 2014 referitoare la propunerea de directivă a Parlamentului European și a Consiliului privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune (*COM(2013)0048 *– C7-0035/2013 –* 2013/0027(COD)*)*

		definit în Codul Penal. Ar trebui modificat apoi intregul act normativ pentru a mentiona aceasta schimbare.
Art.2 Dispozițiile prezentei legi se aplică persoanelor juridice de drept public sau privat, care au calitatea de proprietari, administratori, operatori sau utilizatori de infrastructuri cibernetice, denumite în continuare deținători de infrastructuri cibernetice.	Art.2 Dispozițiile prezentei legi se aplică **exclusiv** persoanelor juridice **din Anexa 1**, care au calitatea de proprietari, administratori, operatori ~~**sau utilizatori**~~ de infrastructuri cibernetice, denumite în continuare deținători de infrastructuri cibernetice.	Legea trebuie limitată la deținătorii de sisteme informatice a căror disfuncționalități specifice pot afecta securitatea națională. Pentru claritatea legii, este necesară o listă exhaustivă a acestor furnizori care trebuie să respecte obligațiile legale, din care vor fi identificați ceea ce propunerea actuală denumește ICIN (infrastructuri cibernetice de interes național). Utilizatorul unui sistem informatic (care este o persoană fizică) nu poate asimilat cu deținătorul sistemului informatic (care poate fi o persoană juridică).
Art 8 – 15	Se modifică pentru eliminarea COSC si înlocuirea CNSC cu CERT – RO.	Vezi mai jos. Ar trebui modificat apoi intregul act normativ pentru a mentiona aceasta schimbare.
Art. 10 (1) Serviciul Român de Informații este desemnat autoritate națională în domeniul securității cibernetice, calitate în care asigură coordonarea tehnică a COSC, precum și organizarea și executarea activităților care privesc securitatea cibernetică a României.	Art 10 (1) **CERT-RO** este desemnat autoritate națională în domeniul securității cibernetice, precum și organizarea și executarea activităților care privesc securitatea cibernetică a României.	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 securităţii informatice care îndeplineşte cerinţele de mai sus şi ar putea îndeplini acest rol este, în acest moment, CERT RO
Art. 17 (1) Pentru realizarea securităţii cibernetice, deţinătorii de infrastructuri cibernetice au următoarele responsabilităţi: a) să acorde sprijinul necesar, la solicitarea motivată a Serviciului Român de Informaţii, Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, Serviciului de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază, CERT-RO şi ANCOM, în îndeplinirea atribuţiilor ce le revin acestora şi să permită accesul reprezentanţilor desemnaţi în acest scop la datele deţinute, relevante în contextul solicitării;	Art. 17 (1) Pentru realizarea securităţii cibernetice, deţinătorii de infrastructuri cibernetice au următoarele responsabilităţi: a) să acorde sprijinul necesar, la solicitarea motivată a CERT-RO, în indeplinirea atribuţiilor acesteia. Accesarea datelor informatice fără acordul scris al deţinătorului se poate face numai în condiţiile şi cu procedura prevăzute de lege pentru percheziţia informatică. ***Sau varianta –*** ***Art. 17 (1) Pentru realizarea securităţii cibernetice, deţinătorii de infrastructuri cibernetice au următoarele responsabilităţi:*** ***a) să acorde sprijinul necesar la solicitarea motivată CERT-RO . Accesul la datele deţinute se face în conformitate cu prevederile Codului de Procedură Penală.*** ***Art. 17^1 (1) Pentru realizarea securităţii cibernetice, deţinătorii de infrastructuri cibernetice au dreptul de a colabora cu CERT-RO, pe baza unor protocoale negociate intre parti conform HG 494/2011, inclusiv prin transferul datelor informatice legate in mod direct de caz, doar daca exista acordul scris al detinatorului de sistem informatic cu privire la datele respective.*** ***(2) Aceste date informatice trimise CERT Ro pot fi***	Accesul la datele informatice se poate face doar printr-o percheziţie informatică în conformitate cu Codul de Procedură Penală. Căutarea, accesarea, identificarea, selectarea, strangerea si transferul (ridicarea) de date informatice inseamna perchezitie informatica si pentru aceasta trebuie autorizatie de la judecator. Cu toate acestea, textul legal nu trebuie să împiedice cooperarea între deţinătorii de sisteme informatice şi CERT România în vederea asigurării securităţii informatice. Astfel, art. 17/1 al/ 1 lit. a) este pus in concordanta cu art. 3 al. 2 din proiect

	folosite doar in scopurile definite prin HG 494/2011 si nu pot fi utilizate in cursul unei proceduri penale sau civile.	
Art.27 – (1) (b) Serviciul Român de Informații pentru deținătorii de ICIN persoane juridice de drept public;	**Art.27 –** (1) (b) **CERT Romania** pentru deținătorii de ICIN persoane juridice de drept public;	Corelare cu Art 10.
Articol nou	**Art 31^1** (10) Se completează Art 12 (7) din HG 494/2011 cu literele: j) Avocatul Poporului k) Autoritatea Națională pentru Protecția Datelor cu Caracter Personal l) 2 reprezentanți ai instituțiilor de învățământ superior m) 2 reprezentați ai asociațiilor industriilor de comunicații electronice n) 2 reprezentați ai asociațiilor patronale din domeniul tehnologiei informației o) 2 reprezentați ai asociațiilor și/sau fundațiilor active în domeniul drepturilor omului.	Pentru a permite CERT RO să îndeplinească statutul de organizație civilă, sub completă supraveghere informatică.
Articol nou	**Anexa 1 - Lista categoriilor de persoane juridice conform art. 2** 1. Energie (a) Electricitate - furnizori - operatori de sisteme de distribuție și comercianți cu amănuntul către consumatorii finali - operatori de sisteme de transport al energiei electrice (b) Petrol	Pentru a defini în mod exhaustiv subiecții legii și a corela legea română cu propunerea de Directivă NIS.

	- conducte de transport al petrolului şi depozite de petrol - operatori ai instalaţiilor de producţie, de rafinare şi de tratare a petrolului, de depozitare şi de transport (c) Gaze naturale - furnizori - operatori de sisteme de distribuţie şi comercianţi cu amănuntul către consumatorii finali - operatori de sisteme de transport al gazelor naturale, operatori de sisteme de depozitare şi operatori de sisteme GNL - operatori ai instalaţiilor de producţie, de rafinare, de tratare, de depozitare şi de transport al gazelor naturale - operatori de pe piaţa gazelor naturale 2. Transporturi (a) Transportul rutier (i) operatori de control al gestionării traficului (ii) servicii logistice auxiliare: - antrepozitare şi depozitare, - manipularea mărfurilor şi - alte servicii auxiliare de transport (b) Transportul feroviar (i) căi ferate (gestionari de infrastructură, întreprinderi integrate şi operatori de transport feroviar) (ii) operatori de control al gestionării traficului (iii) servicii logistice auxiliare: - antrepozitare şi depozitare, - manipularea mărfurilor şi - alte servicii auxiliare de transport	

	(c) Transportul aerian (i) transportatori aerieni (transport aerian de marfă şi de pasageri) (ii) aeroporturi (iii) operatori de control al gestionării traficului (iv) servicii logistice auxiliare: - antrepozitare, - manipularea mărfurilor şi - alte servicii auxiliare de transport (d) transporturi maritime (i) transportatori maritimi (societăţi de transport maritim şi costier de pasageri şi societăţi de transport maritim şi costier de mărfuri) 4. Infrastructuri ale pieţei financiare: pieţele reglementate, sisteme multilaterale de tranzacţionare, sisteme organizate de tranzacţionare, contrapărţi centrale/case de compensare 5a. Producţia şi aprovizionarea cu apă 5b. Lanţul distribuţiei de alimente	

Susţinători:

Asociaţia pentru Apărarea Drepturilor Omului în România – Comitetul Helsinki (APADOR-CH)
Asociaţia pentru Tehnologie şi Internet (ApTI)
Activewatch Agenţia de Monitorizare a Presei
Centrul pentru Jurnalism Independent

Bucureşti, 23 Septembrie 2014