

Propuneri de amendamente - Proiect de lege privind securitatea informatică

17 iunie 2014

Preambul

Organizațiile susțin, în principal, respingerea proiectul de lege privind securitatea cibernetică și 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 concepție, propunând o serie de măsuri cu efect limitativ asupra dreptului la viață privată în zona digitală și încalcă în mod evident reglementările europene discutate astăzi pe subiectul securității informației. De asemenea, **subiectul instituției 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 nivelul Uniunii Europene, **este foarte probabil ca, în funcție de textul exact adoptat la nivel european, să fie necesară modificarea și completarea legii naționale** privind securitatea informatică. Din acest motiv, ar fi oportună respingerea proiectului actual și propunerea unui nou proiect după adoptarea directivei UE.

În subsidiar, dacă decideți adoptarea acestui proiect este necesar a se rezolva cel puțin problemele majore identificate mai jos:

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

Directiva NIS nu specifică nicăieri ca organizațiile care intra sub incidența sa sunt obligate în vreun fel să permită accesul la sistemele proprii sau, cu atât mai puțin, la datele personale deținute, acest aspect fiind reglementat la nivelul fiecărui stat membru. Textul proiectului de lege autohton, în schimb, acordă unei întregi pleiade de organizații cu rol de serviciu de informații, de aplicare a legii sau de apărare dreptul să ceară și să obțină accesul la aceste sisteme și date, fără implicarea vreunui judecător, fără vreo referire la protecția datelor și doar cu o foarte vagă referire la vreo limită bazată pe principiul proporționalității care poate fi ocolită extrem de facil.

- 2. Lista subiecților 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 propune folosirea acestei liste drept standard și pentru acest proiect.

3. **Desemnarea unei autorități competente care să întrunească condițiile minimale dezbătute la nivel european - „organisme civile, 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.” (Considerentul 10 a)¹**

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 definit în Codul Penal. Ar trebui modificat apoi întregul act normativ pentru a menționa 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	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

¹ 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\(COD\)](#))

continuare deținători de infrastructuri cibernetice.		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 întregul act normativ pentru a menționa această 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 „organisme civile, 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 în domeniul securității informatice care îndeplinește cerințele de mai sus și ar putea îndeplini acest rol este, în acest moment, CERT RO
Art. 17 (1) Pentru realizarea securității cibernetice, deținătorii de infrastructuri cibernetice au următoarele responsabilități: a) să acorde sprijinul necesar, la solicitarea	Art. 17 (1) Pentru realizarea securității cibernetice, deținătorii de infrastructuri cibernetice au următoarele responsabilități: a) să acorde sprijinul necesar, la solicitarea motivată	Accesul la datele informatice se poate face doar printr-o percheziție informatică în conformitate cu Codul de Procedură Penală.

motivată a Serviciului Român de Informații, Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Oficiului Registrului Național al Informațiilor Secrete de Stat, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, CERT-RO și ANCOM, în îndeplinirea atribuțiilor ce le revin acestora și să permită accesul reprezentanților desemnați în acest scop la datele deținute, relevante în contextul solicitării;	a CERT-RO, în îndeplinirea atribuțiilor acesteia. Accesarea datelor informatice fără acordul scris al deținătorului se poate face numai în condițiile și cu procedura prevăzute de lege pentru percheziția informatică. Sau varianta – <i>Art. 17 (1) Pentru realizarea securității cibernetice, deținătorii de infrastructuri cibernetice au următoarele responsabilități:</i> <i>a) să acorde sprijinul necesar la solicitarea motivată CERT-RO . Accesul la datele deținute se face în conformitate cu prevederile Codului de Procedură Penală.</i> <i>Art. 17¹ (1) Pentru realizarea securității cibernetice, deținătorii de infrastructuri cibernetice au dreptul de a colabora cu CERT-RO, pe baza unor protocoale negociate între parti conform HG 494/2011, inclusiv prin transferul datelor informatice legate în mod direct de caz, doar dacă exista doar acordul scris al deținătorului de sistem informatic cu privire la datele respective.</i> <i>(2) Aceste date informatice trimise CERT Ro pot fi folosite doar în scopurile definite prin HG 494/2011 și nu pot fi utilizate în cursul unei proceduri penale sau civile.</i>	Căutarea, accesarea, identificarea, selectarea, strangerea și transferul (ridicarea) de date informatice înseamnă percheziție informatică și pentru aceasta trebuie autorizație de la judecător. Cu toate acestea, textul legal nu trebuie să împiedice cooperarea între deținătorii de sisteme informatice și CERT România în vederea asigurării securității informatice. Astfel, art. 17/1 al/ 1 lit. a) este pus în concordanță cu art. 3 al. 2 din proiect
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 31¹	Pentru a permite CERT RO să îndeplinească

	(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 reprezentanți ai asociațiilor industriilor de comunicații electronice n) 2 reprezentanți ai asociațiilor patronale din domeniul tehnologiei informației o) 2 reprezentanți ai asociațiilor și/sau fundațiilor active în domeniul drepturilor omului.	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 - conducte de transport al petrolului și depozite de petrol - operatori ai instalațiilor de producție, de rafinare și de tratare a petrolului, de depozitare și de transport (c) Gaze naturale - furnizori - operatori de sisteme de distribuție și comercianți cu amănuntul către consumatorii finali	Pentru a defini în mod exhaustiv subiecții legii și a corela legea română cu propunerea de Directivă NIS.

	- operatori de sisteme de transport al gazelor naturale, operatori de sisteme de depozitare și operatori de sisteme GNL - operatori ai instalațiilor de producție, de rafinare, de tratare, de depozitare și de transport al gazelor naturale - operatori de pe piața gazelor naturale 2. Transporturi (a) Transportul rutier (i) operatori de control al gestionării traficului (ii) servicii logistice auxiliare: - antrepozitare și depozitare, - manipularea mărfurilor și - alte servicii auxiliare de transport (b) Transportul feroviar (i) căi ferate (gestionari de infrastructură, întreprinderi integrate și operatori de transport feroviar) (ii) operatori de control al gestionării traficului (iii) servicii logistice auxiliare: - antrepozitare și depozitare, - manipularea mărfurilor și - alte servicii auxiliare de transport (c) Transportul aerian (i) transportatori aerieni (transport aerian de marfă și de pasageri) (ii) aeroporturi (iii) operatori de control al gestionării traficului (iv) servicii logistice auxiliare: - antrepozitare, - manipularea mărfurilor și	
--	---	--

	- alte servicii auxiliare de transport (d) transporturi maritime (i) transportatori maritimi (societăți de transport maritim și costier de pasageri și societăți de transport maritim și costier de mărfuri) 4. Infrastructuri ale pieței financiare: piețele reglementate, sisteme multilaterale de tranzacționare, sisteme organizate de tranzacționare, contrapărți centrale/case de compensare 5a. Producția și aprovizionarea cu apă 5b. Lanțul distribuției de alimente	
--	--	--

Susținători:

Asociația pentru Apărarea Drepturilor Omului în România – Comitetul Helsinki (APADOR-CH)

Asociația pentru Tehnologie și Internet (ApTI)

Activewatch Agenția de Monitorizare a Preses

17 Iunie 2014