ApTI– Asociația pentru Tehnologie și Internet
info@apti.ro
www.apti.ro

11 iunie 2014

Către Comisia pentru tehnologia informației și comunicațiilor din Camera Deputaților
În atenția domnului președinte Daniel Vasile Oajdea

Opinia ApTI cu privire la Proiectul de lege privind securitatea cibernetică

ApTI susține respingerea proiectul de lege privind securitatea cibernetică, întrucât aceasta 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.

Proiectul de lege privind securitatea cibernetică ar fi trebuie să fie bazat sau cel puțin corelat cu propunerea de Directiva NIS (Network & Information Security). Parlamentul European deja a adoptat această directivă în primă lectură pe 13 Martie 2014[1] dar procesul legislativ nu este încă încheiat la nivelul Uniunii Europene.

Din păcate, proiectul de lege ajuns în Camera Deputaților[2] nu doar ca nu are aproape nimic în comun cu ceea ce se dorește să se realizeze la nivel European prin Directiva NIS, ci creează niște premise extrem de grave pentru încălcarea dreptului la viață privată.

Sumar:

	Directiva NIS	**Proiect lege România**
Politică Securitatea Cibernetică sub coordonare civilă și control democratic	DA	NU
Listă actori vizați bine definită și solid justificată	DA – lista exhaustiva în Anexa II	NU – definiții vagi
Listă obligații actori vizați clară și proporțională	DA	NU
Acces la date informatice	NU – accesul se face doar cu mandat judecătoresc	DA – prin simplul „decizie motivată” din partea a 9 instituții

Problemele pot fi catalogate în 3 mari categorii:

I. În primul rând, la nivel European, **Directiva NIS are rolul de a ajuta firmele și instituțiile să minimizeze riscurile de securitate informatică**, iar când apar eventuale incidente, să le poată trata cât mai eficient și mai potrivit. În acest context, **statul are un rol de coordonare și asistență**. Versiunea curentă a textului Directivei NIS spune:

> *Art. 6.1 „Fiecare stat membru va desemna una sau mai multe autorități competente civile pe domeniul securității rețelelor și sistemelor informatice (numite de aici încolo 'autoritatea/autoritățile competente').”*

și clarifică termenul de „civil”:

> *(Recitalul 10a) „**Autoritățile competente și punctele unice de contact ar trebui 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 cazul proiectului de lege autohton, organizațiile propuse de acest proiect de lege să se ocupe de securitatea informatică sunt urmatoarele 4 noi instituții:

1. *Art. 6 - Sistemul National de Securitate Cibernetica (SNSC)*
2. *Art. 8 - Consiliul Operativ de Securitate Cibernetica (COSC)*
3. *Art. 10 - Centrul National de Securitate Cibernetica (CNSC)*
4. *Art. 15 - Sistemul National de Alerta Cibernetica (SNAC)*

care au sunt create astfel:

- *Art. 6 (3) „Activitatea SNSC este coordonată la nivel strategic de Consiliul Suprem de Apărare a Țării, denumit în continuare CSAT.”*
- *Art. 8 (2) „COSC este format din reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, Oficiului Registrului Național al Informațiilor Secrete de Stat, precum și Secretarul Consiliului Suprem de Apărare a Țării.”*
- *Art. 8 (3) „Conducerea COSC este asigurată de Consilierul Prezidențial pentru apărare și securitate națională, în calitate de președinte și Consilierul Primului Ministru pe probleme de securitate națională – în calitate de vicepreședinte.”*
- *Art. 8 (4) „COSC își desfășoară activitatea în conformitate cu propriul Regulament de organizare și funcționare, care se aprobă prin hotărâre a CSAT, la propunerea Consilierului Prezidențial pentru apărare și securitate națională, în termen de 60 de zile de la intrarea în vigoare a prezentei legi.”*
- *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. În acest*

scop, în structura SRI funcționează Centrul Național de Securitate Cibernetică, denumit în continuare CNSC."

- *Art. 15 (2) „Organizarea SNAC, măsurile specifice pe care autoritățile și instituțiile publice competente pentru fiecare nivel de alertă, precum și procedura de instituire a nivelelor de alertă și cerințele privind elaborarea planurilor de acțiune se aprobă prin norme metodologice, la propunerea SRI."*

Așadar, toate noile organizații conectate la nivel fundamental de aproape toate organizațiile cu rol de serviciu de informații, de aplicare a legii sau de apărare, fiind diametral opuse la ceea ce stipulează Directiva NIS – organizații civile și sub control democratic.

Aceste noi organizații dublează, într-o mai mare sau mai mică măsură ceea ce deja face CERT-RO. Mai mult decât atât, nici măcar CERT-RO nu corespunde cerințelor Directivei NIS pentru că această organizație are legături organizaționale cu organizații cu rol de serviciu de informații, de aplicare a legii și de apărare:

„CERT-RO este condus de un director general si de un director general adjunct, sprijiniti de Comitetul de coordonare format din reprezentanti ai:
a) Ministerului Comunicatiilor si Societatii Informationale;

b) Ministerului Apararii Nationale;

c) Ministerului Administratiei si Internelor;

d) Serviciului Roman de Informatii;

e) Serviciului de Informatii Externe;

f) Serviciului de Telecomunicatii Speciale;

g) Serviciului de Protectie si Paza;

h) Oficiului Registrului National al Informatiilor Secrete de Stat;

i) Autoritatii Nationale pentru Administrare si Reglementare in Comunicatii."[3]

II. În al doilea rând, Directiva NIS stipulează clar și exhaustiv ce organizații intră sub incidența sa. Directiva se referă la aceste organizații drept operatori de pe piață („market operators"), și cei vizați sunt (in această variantă a proiectului):

1. *Anexa II, pct. 1 „Lista operatorilor de pe piață:*
   1. Energie
   (a) Electricitate
   - Producători
   - Operatori de sisteme de distribuție și furnizori către consumatorii finali
   - Operatori de sisteme de transmisie de electricitate

(b) Petrol
- Conducte de transport al petrolului și instalații de stocare a petrolului
- Operatori de instalații de producție, rafinare, tratare, stocare și transport al petrolului
(c) Gaze naturale
- Furnizori
- Operatori de sisteme de distribuție și furnizori către consumatorii finali
- Operatori de instalații de transmisie, stocare a gazelor naturale și gazelor naturale lichefiate
- Operatori de instalații de producție, rafinare, tratare, stocare și transport al gazelor naturale
- Operatori pe piața gazelor naturale"

2. *Anexa II, pct. 2 „2. Transport*
(a) Transport rutier
(i) Operatori de sisteme de control al gestiunii traficului
(ii) Servicii de logistică auxiliare:
- depozitare și stocare
- manipulare cargo
- alte activități de suport al transporturilor
(b) Transport feroviar
(i) Căi ferate (manageri de infrastructură, companii integrate și operatori de transport feroviar)
(ii) Operatori de sisteme de control al gestiunii traficului
(iii) Servicii de logistică auxiliare:
- depozitare și stocare
- manipulare cargo
- alte activități de suport al transporturilor
(c) Transport aerian
(i) Transportatori aerieni (transport de mărfuri și pasageri)
(ii) Aeroporturi
(iii) Operatori de sisteme de control al gestiunii traficului
(iv) Servicii de logistică auxiliare:
- depozitare și stocare
- manipulare cargo
- alte activități de suport al transporturilor
(d) Transport naval
(i) Transportatori navali (riverani, de coastă sau maritimi, atât de mărfuri cât și de pasageri)"

3. *Anexa II, pct. 4 „4. Infrastructuri ale pieței financiare: piețe regulate, instituții de comerț multilateral, instituții de comerț organizat și birouri de decontare centrale"*
unde „piețele reglementată", „instituțiile de comerț multilateral" și „instituțiile de comerț organizat" sunt definite astfel:
   1. *Art. 3, pct. 11 a „prin 'piață reglementată' se înțelege piață reglementată așa cum este definită prin punctul 14 al Articolului 4 al Directivei 2004/39/EC a Parlamentului European și a Consiliului Europei[1a];*
   [1a] Directiva 2004/39/EC a Parlamentului European și a Consiliului Europei din 21 Aprilie 2004 pe subiectul piețelor și instrumentelor financiare (OJ L 45, 16.2.2005, p. 18)"
   2. *Art. 3, pct. 11 b „prin 'instituție de comerț multilateral' se înțelege instituție de comerț organizat așa cum este definită prin punctul 15 al Articolului 4 al Directivei 2004/39/EC;"*
   3. *Art. 3, pct. 11 c „prin 'instituție de comerț organizat' se înțelege o instituție sau sistem de comerț multilateral, care nu este o piață reglementată, o instituție de comerț multilateral*

sau un birou de decontare central, operată de o firmă de investiții sau de un operator pe piață, în care mai mulți terți care vând și cumpără obligațiuni, produse financiare structurate sau instrumente financiare derivate pot interacționa în cadrul sistemului în așa fel încât să dea naștere la contracte în conformitate cu Titlul II al al Directivei 2004/39/EC;"

4. *Anexa II, pct. 5 a „5a. Producția și furnizarea de apă potabilă"*
5. *Anexa II, pct. 5 b „5b. Lanțul alimentar"*
6. *Anexa II, pct. 5 c „5c. Internet Exchange-uri"*

În cazul proiectului de lege autohton, textul propunerii legislative spune, foarte ambiguu:

- *Art. 5, pct. 8 „infrastructuri cibernetice - infrastructuri din domeniul tehnologiei informației, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice"*
- *Art. 5, pct. 9 "infrastructuri cibernetice de interes național (ICIN) - infrastructurile cibernetice care susțin servicii publice sau de interes public , ori servicii ale societății informaționale, a căror afectare poate aduce atingere securității naționale, sau prejudicii grave statului roman ori cetățenilor acestuia"*
- *Art. 19 (1) „La nivel național se constituie Catalogul ICIN, care se aproba în termen de 90 de zile de la intrarea în vigoare a acestei legi, prin hotărâre a Guvernului."*
- *Art. 19 (2) „Catalogul ICIN se întocmește de către Ministerul pentru Societatea Informațională, cu consultarea COSC, la propunerea CNSC sau după caz, a CERT-RO, potrivit cetinelor legale."*
- *Art. 19 (3) „Identificarea ICIN se realizează pe baza criteriilor de selecție cuprinse în metodologia elaborata de Serviciul Român de Informații și Ministerul pentru Societatea Informațională și aprobata, în termen de 60 de zile de la intrarea în vigoare a prezentei legi, prin hotărâre de Guvern."*
- *Art. 19 (4) „La elaborarea Catalogului ICIN, Ministerul pentru Societatea Informațională va colabora și cu ANCOM, în situația persoanelor juridice de drept privat care dețin calitatea de furnizori de rețele publice sau servicii de comunicații electronice destinate publicului."*

Așadar **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".

Ținând cont de această definiție extrem de vagă, obligațiile deținătorilor de „infrastructuri cibernetice" devin excesive:

1. Art. 16 „Deținătorii de infrastructuri cibernetice au următoarele obligații:
   a) să aplice politici de securitate cibernetică, cu respectarea cerințelor minime de securitate stabilite la nivel național de Ministerul pentru Societatea Informațională, ANCOM sau de către alte autorități publice competente potrivit legii;
   b) să identifice și să implementeze măsuri tehnice și organizaționale adecvate pentru a gestiona eficient riscurile de securitate în infrastructurile cibernetice proprii sau aflate în responsabilitate;"

Dacă ținem cont de faptul că oricine poate fi considerat deținător de „infrastructurii cibernetice", chiar și persoanele private, din cauza definiției foarte vagi și foarte largi a „infrastructurilor cibernetice",

atunci cerința ca toți deținătorii să aplice politici de securitate în concordanță cu cerințele stabilite de varii instituții ale statului și să identifice și implementeze măsuri tehnice și organizaționale pentru a gestiona riscurile de securitate devine brusc imposibilă pentru vasta majoritate a potențialilor deținători de „infrastructuri cibernetice”.

Când vine vorba de ICIN, situația este și mai gravă pentru că textul propunerii legislative nu spune nimic despre care sunt acestea sau, cel puțin, care sunt criteriile după care vor fi catalogate.

În fapt, **proiectul de lege este un cec în alb** care poate fi folosit, după eventuala adoptare, pentru a controla orice actor de pe piața de comunicații și servicii informatice, potențialul pentru abuzuri fiind enorm.

Ambiguitățile nu se opresc doar la cine intra sub incidența acestei legi, ci se extind și la ce obligații au cei care intra sub incidența sa.

Directiva NIS nu cere urmarea unor anume proceduri de securitate informatică ci doar cere ca operatorii de pe piață să facă tot posibilul pentru a-și securiza sistemele și să raporteze incidentele, atunci când acestea apar.

Proiectul de lege autohton, pe de altă parte, cere să fie respectate proceduri create de instituții ale statului, și, mai mult de cât atât, nici nu le specifică ci le lasă la latitudinea respectivelor instituții, prin articolul 16 punctul a), citat mai sus, care se referă la cerințele „minime de securitate stabilite la nivel național de Ministerul pentru Societatea Informațională, ANCOM sau de către alte autorități publice competente potrivit legii”.

Nu se specifică nicăieri în textul proiectului de lege care ar fi aceste cerințe, sau dacă ele vor fi în conformitate cu standardele de securitate informatică recunoscute internațional și stabilite de organizații cu experiență în domeniu (în marea lor majoritate acestea fiind organizații private).

> Ca o paranteză, „securitate cibernetică” nici măcar nu este un termen consacrat. Termenul consacrat este „securitate informatică”. Aceasta este o problemă foarte serioasă pentru că organizațiile care deja au politici de securitate informatică și au puse în practică măsuri tehnice și organizaționale pentru gestionarea riscurilor de securitate informatică bazate pe standarde și/sau proceduri recunoscute internațional pot fi puse în situația de a se trezi în neconformitate cu regulile create de o serie de instituții locale care, foarte probabil, nu au nici pe departe același nivel de expertiză în domeniu ca organizațiile care se ocupa de stabilirea de standarde și proceduri de securitate informatică menționate mai devreme. Mai mult, auditul de securitate informatica are niște prevederi foarte clare pentru experții în securitate informatică, ca parte a unor proceduri și standarde recunoscute internaționale – ca un sistem de certificări voluntare și nu obligatorii.

Problemele cu obligațiile create de textul acestui proiect de lege nu se opresc la aceste ambiguități, însă din motive de timp pe care îl putem aloca acestei analize, ne rezumăm la cele majore.

III. Nu în ultimul rând, Directiva NIS, la nivel fundamental, are ca scop protecţia datelor cetăţenilor.

În acest scop, protecția datelor este fundamentală pentru securitatea juridică și consolidarea garanțiilor și protecția persoanelor și a sferei private a acestora, pentru asigurarea că persoanele dețin controlul asupra propriilor date cu caracter personal și au încredere în mediul digital, precum și în vederea creării unei culturi de gestionare a riscurilor și de îmbunătățire a schimbului de informații între actorii din sectorul public și cel privat[4].

Directiva NIS propune:

> *(Recitalul 15) „Cum majoritatea rețelelor și sistemelor informatice sunt private, cooperarea dintre sectorul public și cel privat este esențială. Operatorii de pe piață ar trebui încurajați să-și creeze propriile mecanisme de cooperare informale pentru a realiza NIS. Aceștia ar trebui să coopereze cu sectorul public și să facă schimb de informații și bune practici, inclusiv schimbul reciproc de informații relevante și suport operațional și informație analizată strategic, în cazul incidentelor. Pentru a încuraja în mod eficient schimbul de informații și bune practici, este esențial ca operatorii de pe piață, care participă la astfel de schimburi, să nu fie dezavantajați ca rezultat al cooperării. Sunt necesare protecţii adecvate pentru a asigura că astfel de cooperare nu va expune acești operatori la riscuri mai mari de conformitate sau noi răspunderi ca rezultat al legislațiilor privitoare la, de exemplu, competiție, proprietate intelectuală, protecția datelor sau cybercriminalitate, și nici nu îi va expune la riscuri operaționale și de securitate sporite.”*

Mai mult decât atât, 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:

> Art. 17 (1) „Pentru realizarea securității cibernetice, deținătorii de infrastructuri cibernetice au următoarele responsabilități: a) sa acorde sprijinul necesar, la solicitarea motivata 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 sa permită accesul reprezentanților desemnați în acest scop la datele deținute, relevante în contextul solicitării”

Ca o concluzie dorim să subliniem doua idei principale:

1. Securitatea informatică este un subiect important pentru societatea informațională, dar care se bazează întâi pe cooperarea actorilor importanți din domeniul ITC și nu prin obligații impuse de lege într-un proces legislativ care ignora interesele grupurilor țintă. Nu putem decât să constatăm că

procesul de dezbatere al proiectului a fost inexistent până când acesta a fost trimis în Parlament, ba mai mult guvernul nu a respectat, încă o dată dispozițiile legii 52/2003 privind transparența decizională.

2. **Este importantă o discuție serioasă și așezată pe acest subiect delicat, indiferent de diverse interese instituționale de moment.** În acest context nu putem să nu observăm că unul din obiectivele de reglementare din această lege a fost deja „acordat" SRI printr-un proiect finanțat din fonduri europene: „ Sistem național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic" [5]

Resurse:

[1] http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0244
[2] http://www.cdep.ro/proiecte/2014/200/60/3/pl263.pdf
[3] http://www.cert-ro.eu/despre.php
[4] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-514.755+01+DOC+PDF+V0//RO&language=RO
[5] https://www.sri.ro/finantare-europeana-accesata-de-sri-sistem-national-de-protectie-a-infrastructurilor-it-c-de-interes-national-impotriva-amenintarilor-provenite-din-spatiul-cibernetic.html