Asociaţia pentru Tehnologie și Internet (ApTI) este o organizaţie neguvernamentală care acționează pentru protecția drepturilor civile digitale prin garantarea unui mediu digital liber și deschis.

Comentariile de mai jos privesc aspectele prioritare din textul legii, care pot afecta drepturile civile digitale, conform expertizei ApTI.

Din punct de vedere formal, observăm că textul propus dezbaterii publice este aproape identic cu cel făcut public de G4Media în mai-iunie 2022, ca atare ar fi fost de apreciat - pentru o transparența adecvată - să fie precizat exact care a fost parcursul lui de până acum și care sunt de fapt instituțiile care au fost implicate în scrierea acestui text.

De asemenea proiectul pare a susține idei mai vechi prin care “securitatea cibernetica” e un subiect în care doar statul are un interes, iar sectorul privat trebuie sa se supună, nu sa fie un partener egal.

Proiectul pare a eluda că există un interes major pentru securitate informatica atât din partea persoanelor fizice, cît și a persoanelor juridice. Scopul celor două entități diferă, drept pentru care uneori nici nu vrem ca datele protejate și private să fie puse la dispoziția statului. Cu atât mai mult, datele noastre, ale unor persoane private, și securitatea sistemelor pe care sunt stocate, nu trebuie să fie comunicate statului decât ca excepție, decât atunci când există un interes public superior interesului privat în cauză. **Aceste aspecte sunt deja definite limitat de directivele NIS1 si NIS2.**

1. Nu orice site trebuie să fie supus obligațiilor de securitate, doar cele din sectoare esențiale și de la firme mari și mijlocii, conform directivei NIS2

Includerea in **Art 3 (1) c)** a rețelelor și sistemelor informatice ale persoanelor juridice care ***furnizează servicii publice ori de interes public*** (fără a defini acești termeni în cuprinsul acestui act normativ) face ca spectrul de aplicare să fie exagerat de larg.

Obligația de notificare în 24 de ore și obligațiile de la **Art 40** sunt imposibil de îndeplinit pentru oricare din următoarele:

- un site cu 3 utilizatori, administrat de un PFA la ONG, care oferă un serviciu online (care este public prin definiție),
- un site care aparține unei publicații mici mass-media, serviciu gratuit sau plătit,
- un mic magazin offline (care și el are un serviciu public) dotat cu casă de marcat electronică (deci un sistem informatic).

Așadar, este de neînțeles includerea sectorului privat într-o singură categorie cu rețelele sectorului public în următoarea formulare:

*“c) **rețelele și sistemele informatice deținute, organizate, administrate sau utilizate** de*

autorități și instituții ale administrației publice centrale și locale, altele decât cele prevăzute la lit. a), ***precum și de persoane juridice care desfășoară*** *activități industriale, de cercetare științifică* ***sau furnizează servicii publice ori de interes public,*** *altele decât cele de la lit. b).”*

Recomandarea noastră este de corelarea a acestui subiect cu categoriile de rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de persoane juridice conform directivei NIS2 (citată și de autorii propunerii în expunerea de motive) și care probabil va intra în vigoare până la finalul lui 2022:

- limitarea actorilor privați cu obligații exclusiv la sectoarele acoperite de NIS1 și NIS2;
- limitarea la actori mari și mijlocii, și excluderea actorilor mici, inclusiv din aceste sectoare pentru a evita măsuri excesive și imposibil a fi implementate;
- acordarea unei singure obligației de notificare a incidentelor de securitate în legea de implementare a directivei NIS2.

2. Furnizorii de servicii de securitate cibernetică = delatori profesioniști

“Furnizorii de servicii de securitate cibernetică au obligația de a pune la dispoziția autorităților prevăzute la art. 10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau sistem informatic a deținătorului sau a unor terți”

Scopul unui furnizor de servicii de securitate este acela de a proteja și de a rezolva problemele clientului său. De obicei, furnizorii de servicii de securitate cibernetică sunt niște profesioniști tehnici care au obligații contractuale de confidențialitate extrem de stricte față de clienții lor (din România sau străinătate). O parte din informațiile la care au access, sau pe care le descoperă, sunt legate de incidente, amenințări, riscuri sau vulnerabilități.

Conform proiectului de lege privind securitatea cibernetică a României, acești furnizori sunt obligați ca, la orice întrebare de la una din instituțiile din **Art. 10**, să pârască proprii clienți. Fără mandat judecătoresc, fără autorizație precisă, acești furnizori sunt obligați să dea informații despre starea securității unui client, sau, mai rău, a unei întregi infrastructuri (ceea ce poate include informații personale și secrete ale mai multor clienți, fie ei direct afectați de o posibilă vulnerabilitate sau nu).

O asemenea obligație - care a făcut parte și din legea cu același obiect declarată neconstituțională prin decizia CCR 17/2015 - ar fi asemănătoare obligației unui auditor sau contabil ca în primul rând să pârască la ANAF și nu să își sfatuiască clientul ce trebuie să facă pentru a fi în legalitate.

3. Care sunt, de fapt, sistemele informatice din competența SRI? Le mai poate identifica cineva?

“Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul Român de Informații, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază pentru asigurarea securității și apărării cibernetice, respectiv pentru cunoașterea, prevenirea și contracararea amenințărilor cibernetice la adresa rețelelor și sistemelor informatice din domeniul lor de competență, activitate sau responsabilitate. În acest sens, stabilesc structuri și măsuri tehnice și organizatorice privind coordonarea și controlul activităților de securitate și apărare cibernetică.”

Cerem definirea separată, corectă și completă a **Art 10 alin d)** astfel încât să fie clar care sunt exact domeniile de competență ale fiecărei instituții. În prezent, textul este vag și folosește termeni generici: “*a rețelelor și sistemelor informatice din domeniul lor de competență, activitate sau responsabilitate.”*

O lege trebuie să fie clară pentru orice subiect. Citind, însă, textul de mai sus, este imposibil să știm, de exemplu, care ar putea fi sistemele informatice din domeniul de competență sau responsabilitate a SRI.

Includ acestea sistemele informatice instalate în alte instituții publice prin proiectul SII Analytics? Includ sisteme pe care le vor achiziționa - poate - pentru cloud-ul guvernamental? Includ sisteme informatice de interceptare a comunicațiilor electronice instalate de SRI, dar folosite astăzi de alte organe din domeniul cercetării penale (ca urmare a deciziei CCR 51/2016)?

Tocmai pentru a evita aceste neclarități ar trebui rescris textul în vederea clarificării și delimitării atribuțiilor fiecărei instituții.

Pentru fiecare instituție trebuie să fie precizat clar domeniul de competență: “”în vederea asigurării securității cibernetice a rețelelor și sistemelor informatice proprii”.

Dacă este cazul lărgirii acestui spectru la alte sisteme informatice - cum e cazul ANCOM - trebuie precizat rolul (coordonare, supraveghere, etc.) și definirea rețelelor și sistemelor informatice care pot intra în competența fiecărei instituții în parte.

În acest context ar trebui clarificat termenul “și în toate celelalte cazuri.” din **Art 13 (2) b)**. Se refera la cazurile din MCID? Alt caz nu mai rămâne în **Art 10**.

Tot din categoria neclarităților și neconcordanțelor observăm că **Art 13** din prezenta lege **nu se corelează cu legislația specifică cloud-ului**. Astfel în aceasta lege STS-ului îi revine obligația de a se ocupa de activitățile de securitate cibernetică cu privire la propriile infrastructuri (inclusiv cu privire la atacurile APT), în schimb în OUG 89/2022 este prevăzut contrariul.

Reamintim ca în conformitate cu decizia CCR 17/2015 legea trebuie să respecte criteriile de previzibilitate, stabilitate şi certitudine.

4. Nu trebuie incluse activitățile și sistemele din domeniul civil în domeniul militar

Definiția de la **Art 2 (2)** trebuie limitată pentru a se adresa exclusiv activităților legate de domeniul militar și a exclude activitățile sau sistemele informatice din sectorul civil. În caz contrar definiția și **Art de la 29 sau 30** vor privi întreg Internetul ca un spațiu de manevră a acțiunilor militare.

O altfel de interpretare ar încălca principiul enunțat de CCR prin declarația de necunostituționalitate din 17/2015: "*Instituțiile care se ocupă de domeniul securității cibernetice trebuie să fie organisme civile, sub controlul cetățenilor*". Vezi detalii în insemnarea Asociației pentru tehnologie și internet.

*a) apărare cibernetică - totalitatea activităților, mijloacelor și măsurilor utilizate pentru a contracara amenințările provenite din spațiul cibernetic și a atenua efectele acestora asupra sistemelor de comunicații și tehnologia informației, sistemelor de armament, rețelelor și sistemelor informatice, **exclusiv pentru** ce susțin capabilitățile militare de apărare;*

Nu exista nici o corelare dintre definițiile de la a) și r).

În acest context recomandăm și renunțarea la obligațiile din **Art 29**: "*participă la activități de descurajare în spațiul cibernetic;*" sau clarificarea acestora. Sunt incluse și activități precum scanarea de porturi, atacuri DDoS, încercări de enumerare a subdomeniilor? Este vorba, de fapt, de acțiuni ofensive făcute de un actor militar?

5. Accesul la PNRISC este neclar

"(2) Autoritățile prevăzute la art. 10 au acces garantat la PNRISC.
(3) Accesul la informațiile din PNRISC este restricționat prin politici de confidențialitate stabilite și implementate de DNSC."

Termenii din **Art 19 alin 2 si 3** sunt neclari și nu iau în considerare protectia datelor confidențiale trimise de subiecții legii (fie date legate de propriile vulnerabilitate, fie date personale).

O politică de confidențialitate nu poate fi un mecanism de protecție a acestor informații, pentru că DNSC poate redacta această politică după bunul plac.

Mai mult, ce treabă ar avea ORNISS sau SPP cu un incident declarat de un furnizor privat?

În opinia noastra **alin 2** trebuie reformulat ca "*Autoritățile să aibă acces - pe baza dreptului specific de a avea nevoie conform obligațiilor legale, stabilit in mod precis prin lege - la date statistice sau raporturi anonimizate*".

Alin 3 trebuie reformulat pentru a preciza că scopul acelor norme de confidențialitate este de a proteja datele personale și alte informații nepublice. Mai mult, scopul accesului este limitat la folosirea informațiilor în scopul asigurarii propriei securități informatice.

6. Să nu facem 7 legi cu 7 obligatii de raportare!

Obligația de notificare a incidentelor de securitate din **Art 20**, precum și obligatiile de la **Art 40** legate de “Securitatea lanțului de aprovizionare”, trebuie să fie incluse într-o singura lege - cum ar fi, de exemplu, în legea 362/2018 - care va trebui modificată pentru a include obligațiile din directiva NIS2, unde există și sancțiuni adecvate.

Obligațiile de notificare trebuie corelate cu restul obligațiilor de raportare - de exemplu, a breșelor de securitate care afectează date personale conform Regulamentului UE 679/2016 GDPR - astfel încât să nu fie necesară o raportare multiplă, diferită și cu termeni diferiți.

7. Dezbatere publică

În calitate de asociație legal constituită și în temeiul art. 6 alin. 7 din Legea nr. 52/2003 privind transparența decizională în administrația publică, vă adresăm prezenta cerere pentru a solicita organizarea unei întâlniri în care să se dezbată public proiectul de Lege privind securitatea și apărarea cibernetică a României. Reamintim că, potrivit art. 6 alin. 7 din Legea nr. 52/2003, organizarea unei întâlniri în care să se dezbată public proiectul de lege este obligatorie dacă acest lucru a fost cerut în scris de către o asociație legal constituită.

Având în vedere că acesta este un proiect de lege care ar trebui să stea la baza securizării infrastructurii digitale a României, credem că este necesară o dezbatere reală a tuturor aspectelor menționate.