Data 22.12.2022
Doamnei Renate Weber
Avocatul Poporului

Petiție colectivă

Stimată doamnă Renate WEBER,

Pe data de 21.12.2022, Senatul Românie[i a adoptat un Proiect de Lege privind]securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (Număr Înregistrare Senat [L828/2022](), Număr înregistrare Camera Deputaților PL-x nr. 773/2022)

Proiectul a fost inițiat de Ministerul Cercetării, Inovării și Digitalizării și a avut un parcurs extrem de rapid și lacunar în dezbateri publice relevante cu societatea civilă și sectorul privat. A reușit "performanța" de a fi dezbătut și votat în toate comisiile desemnate ale ambelor camere ale Parlamentului în doar 9 zile calendaristice.

În ciuda unor mici modificări aduse pe parcursul dezbaterii proiectului, acesta ridică probleme cu privire la modul și felul lacunar în care este propus a fi reglementată securitatea cibernetică (și nu numai!), în special în contextul în care propunerea anterioară din partea Guvernului României a fost declarată neconstituțională în întregime în conformitate cu decizia CCR nr. 17/2015. Cu toate acestea, proiectul reia în mare parte instituții și principii care au fost criticate și în actul normativ declarat neconstituțional.

De asemenea proiectul a fost împins ca fiind jalonul 151 din PNRR, deci trebuie adoptat. Însă o citire atentă a PNRR ne indică că acesta face parte din [măsura "Asigurarea securității cibernetice a entităților publice și private care dețin infrastructuri cu valențe critice"]. Ori cele criticate mai jos - cum ar fi extinderea domeniului la firme private care oferă servicii publice sau extinderea atribuțiilor SRI pe "dezinformare și propagandă" nu au legătură deloc cu "infrastructuri cu valențe critice".

Organizațiile semnatare vă solicită să evaluați oportunitatea contestării Ordonanței de Urgență menționate la Curtea Constituțională a României. Detaliem mai jos argumentele noastre principale în ceea ce privește conținutul actului normativ și impactul său asupra drepturilor și libertăților garantate de Constituția României:

1. **Subiecții legii și obligațiile lor sunt vagi și neclare**

Pornim de la principiile de claritate reafirmate în decizia CCR 17/2015[1] (în special par 86-97), ca și de importanța specificității obligațiilor, astfel incat ele sa nu fie *aplicabile "deţinătorilor de infrastructuri cibernetice cu importanţă nesemnificativă din punctul de vedere al interesului general."* (par 69).

> *"Pentru ca legea să satisfacă cerinţa de previzibilitate, ea trebuie să precizeze cu suficientă claritate întinderea şi modalităţile de exercitare a puterii de apreciere a autorităţilor în domeniul respectiv, ţinând cont de scopul legitim urmărit, pentru a oferi persoanei o protecţie adecvată împotriva arbitrariului."*

Art 3 alin 1 are pretenția de a defini domeniul de aplicare a acestei legi, dar **identifică mai degrabă domeniul de aplicare** (anumite rețele și sisteme informatice), dar mai puțin subiecții legii.

> *Articolul 3*
>
> *(1) În domeniul securității cibernetice prezenta lege se aplică următoarelor:*
>
> *a) rețelele şi sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securităţii naţionale, justiției, situațiilor de urgență, Oficiului Registrului Național al Informațiilor Secrete de Stat.*
>
> *b) reţelele şi sistemele informatice deținute de persoanele fizice şi juridice de drept privat şi utilizate în vederea furnizării de servicii de comunicaţii electronice către autorităţile şi instituțiile administrației publice centrale şi locale.*
>
> *c) rețelele şi 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 fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la lit. b).*

Cu toate acestea obligațiile principale pentru aceste categorii (art 21,37, 41-44) se referă la "persoanele prevăzute la art 3", deși art 3 enumeră rețelele și sistemele informatice unde se aplică legea.

În acest context în primul rând textul din a doua parte din lit c) *"persoane fizice şi juridice care furnizează servicii publice ori de interes public"* - în lipsa oricărei definiții sau explicitări atât în text, cât și în expunerea de motive - face ca spectrul de aplicare să fie imens în contextul în care orice fel de serviciu online (sau serviciu al societății informaționale, ca să respectăm definiția din legea 365/2002 sau noul Regulament UE 2022/2065 (DSA)) este un serviciu public. Practic aici intră de la servicii oferite de Facebook sau Google, până la:

[1] DECIZIE nr. 17 din 21 ianuarie 2015 asupra obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind securitatea cibernetică a României Publicat în MONITORUL OFICIAL nr. 79 din 30 ianuarie 2015

a) un site cu 3 utilizatori/lună care oferă public orice serviciu online

b) un site care aparține unei publicații mici mass-media

c) o farmacie offline din orice comună (care și el are un serviciu public și de interes public) dotat cu casă de marcat electronică (deci un sistem informatic). Unei astfel de farmacii care nu are niciun angajat IT i-ar fi imposibil sa facă o analiza reala conform art 41, iar in condițiile unui incident informatic care s-ar petrece vineri seara, cu siguranța ar trebui sa-si petreacă cel puțin 72 de ore pentru a-și rezolva întâi problema de securitate, deci să-l obligi ca să raporteze incidentul in 48 de ore conform art 21, fără excepții, este si exagerat și contrar obiectivului legii. De exemplu in cazul obligației similare din art 33 din GDPR - Regulamentul UE 679/2016 termenul poate fi depășite tocmai pentru ca există excepții: *"fără întârzieri nejustificate și, dacă este posibil".*

Un asemenea text vag - în ciuda atenționărilor adresate pe tot parcursul legislativ- nu îndeplinește cerințele CCR explicitate în par 69 din decizia CCR 17/2015, dar, si mai mult, excede din toate punctele de vedere măsurii din PNRR în cadrul căreia a fost împins acest text legislativ.

O analiză mai atentă ne pune de fapt în imposibilitatea de a identifica exact subiecții legii care au obligațiile mai sus precizate:

- Termenul de "rețelele şi sistemele informatice" ***utilizate*** de autoritățile menționate la lit a) si c) este extrem de generic. Responsabilitatea juridică cu privire la aceste rețele și sisteme informatice aparține deținătorului sau administratorului rețelei sau sistemului respectiv (care poate sa fie o persoana juridica privată). De fapt acesta din urmă este, din punct de vedere practic, singurul care ar putea identifica un incident de securitate cibernetica, care ar trebui raportat în conformitate cu art 21. În cazul serviciilor online (oferite tot prin rețelele și sistemele informatice) este foarte probabil ca administratorul serviciului să nici nu știe dacă o asemenea autoritate folosește serviciile sale (de ex. De rețea socială, de trimitere newsletter, de găzduire fișiere), pentru el acesta fiind un client ca oricare alții, mai ales dacă serviciul este fără plată. Ca să ne dăm seama de dimensiunea problemei, să evidențiem că - în conformitate cu un studiu independent din 2021[2] - 72% din instituțiile publice din România foloseau în 2021 sisteme informatice gratuite pentru email - Yahoo, Gmail, Hotmail (toate furnizate de către furnizori privați din afara României). Deci cine va fi titularul obligațiilor de la art 21,37, 41-44 - furnizorul sau administratorul acelor rețele și sisteme informatice ori autoritățile publice care sunt utilizatori?
- Termenul de "rețelele şi sistemele informatice" ***organizate*** de autoritățile menționate la lit a) si c) este total impropriu și, discutând cu specialiști, nu am reușit să identificăm exact la ce se referă (și care nu s-ar încadra în categoria de deținute, administrate sau

[2] Aceasta este o problema in sine dpdv al respectarii Regulamentu UE 679/2016 (GDPR) Vezi detalii la ASCPD trage un semnal de alarma! GDPR-ul nu este respectat de către instituțiile publice din România! https://ascpd.ro/2022/01/31/ascpd-trage-un-semnal-de-alarma-gdpr-ul-nu-este-respectat-de-catre-institutiile-publice-din-romania/

utilizate). Termenul nu apare în nicio legislație specifică domeniului securității cibernetice din România sau Uniunea Europeană.

- Chiar și termenii din lit b) ridica probleme de interpretare în condițiile în care legislația în domeniul comunicațiilor electronice (OUG 111/2011) folosește termenii de furnizor de rețele și de servicii de comunicații electronice, care sunt definiți și folosiți (si notificați la ANCOM) în mod distinct. Astfel din interpretarea literala a textului alin b) ar rezulta ca furnizorul unei rețele (dar nu și a unui serviciu de comunicații electronice) ar intra în sfera subiecților propuși, ceea ce contravine chiar scopului declarat al legii. Nu e clar nici dacă furnizorul unei rețele private prin care nu este transmis un serviciu public de comunicații electronice (deci nu este obligatorie notificarea la ANCOM conform OUG 111) ar scăpa din această definiție.
- O altă consecință a formulării *"sisteme informatice … utilizate de autorități și instituții ale administrației publice centrale și locale*" este că toți furnizorii de aplicații software și servicii asociate, indiferent de natura aplicației și serviciului sau impactul riscului, vor trebui să răspundă cerințelor din prezenta lege, inclusiv obligațiile de proces și măsuri reactive și proactive. Pentru IMM-urile care deservesc cele 3.228 UAT-uri din România sunt posibile două consecințe negative - fie ieșirea din piață, întrucât conformarea cu cerințele de apărare cibernetică pentru un minister este oneroasă pentru un IMM, fie vânzarea serviciilor prin intermediul ADR și al cloud-ului guvernamental. În ambele variante se creează obligații nejustificate care distorsionează concurența fără justificare reală din punct de vedere al riscurilor și impactului potențial.

2. Obligația de delațiune de la profesioniști. Informatori 2.0

Propunerea de la art 25 reia o propunere din legea declarată neconstituțională în 2015 și creează o obligație de delațiune de la o categorie de profesioniști care, în mod normal, ar avea obligații de confidențialitate stricte pentru proprii clienți.

Articolul 25

(1) Furnizorii de servicii tehnice 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, respectiv, în maximum 5 zile de la data primirii solicitării, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art.3 alin.(1), precum şi interconectarea acestora cu terții şi cu utilizatorii finali.

Deși expunerea de motive și reacțiile publice clamează necesitatea "colaborării", ne aflăm în fața unei obligații precise, fără posibilitate de a fi refuzată sau apelată! **Acești furnizori sunt obligați ca, la orice "cerere motivată" de la una din instituțiile din Art. 10 (adică DNSC, MCID, ANCOM, MApN, MAI, MAE, ORNISS, SRI, SIE, STS și SPP), să pârască proprii clienți** cu privire la problemele lor sau potențiale probleme, daca problema poate reapare în orice alt context (ceea ce este foarte probabil în cazul oricărui incident, amenințare risc sau vulnerabilitate informatică). 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).

În ciuda limitării de la art 25 (2), informațiile sunt de o sensibilitatea extremă, mai ales când spectrul de aplicare de la art 3 (1) c) este atât de larg, încât ne putem aștepta ca autoritățile descrise la Articolul 10 să aibă acces la informații despre starea de securitate a oricărui site, oricărei aplicații web, operate de persoane fizice.

De exemplu, orice expert de securitate ar trebui sa raporteze orice potențială problemă a unui site de media care publică știri și investigații, care pot ajunge chiar către autoritățile despre care sunt unele din materialele publicate. Unele dintre redacțiile de investigație din România, și mai nou orice subiect al legii de implementare a directivei privind avertizorii de integritate, ar fi obligați să creeze sisteme de raportare anonimă (care ar trebui sa fie publice) a infracțiunilor de corupție - deci s-ar putea avea acces direct la informații despre infrastructura de avertizare.

Mai mult, și definiția de la art 2 lit l) “furnizor de servicii tehnice de securitate cibernetică” - în ciuda includerii cuvântului “tehnic” în definiție - are un rol mult mai larg decât auditorul de securitate (reglementat de art 31 și următoarele din legea 362/2018) și are, din definiția prezentată, un rol esențial nu doar pentru măsurile tehnice, ci și măsurile organizatorice care sunt implementate în vederea asigurării securității.[3]

De fapt, obligația impusă este o ignorare completă a importanței confidențialității în relația dintre 2 profesioniști privați - este ca și cum ai obliga să dai unei instituții publice în condiții incerte informații sensibile, similare cu: avocatul să dea informații despre ce face clientul său, doctorul să identifice punctele slabe ale propriului pacient sau lăcătușul să anunțe tipul de ușă folosită (și cum poate fi spartă).

Deci mult clamata colaborare - este de fapt o obligație de delațiune către 11 instituții publice pentru adunare de informații confidențiale de către stat pentru niște scopuri neclare. Formularea actuală presupune din start că furnizorii de servicii de securitate ar refuza să sprijine statul în interesul legitim al acestui de asigurare a apărării cibernetice.

Cum această obligație nu există în niciun alt stat membru al UE, practic furnizorii de servicii de securitate români sunt puși fie între opțiunea de la explica clienților din afara României că toate problemele lor s-ar putea sa fie la degetele a 11 instituții publice românești, fie a se muta în Bulgaria, Ungaria sau alte țări. Sau să devină Informatori 2.0.

De asemenea, această obligație împiedică experții și furnizorii de servicii de securitate informatică străini la a-și furniza serviciile în România pentru că în țările de origine (de exemplu în Germania) dezvăluirea unor astfel de informații oricăror terți este ilegală. Deci, astfel de furnizori internaționali de servicii de securitate informatică vor avea de ales între a respecta

[3] Pentru a intelege nivelul de complexitate și de sensibilitate a acestor informații, va recomandam ghidul ENISA
https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

legea în România sau a respecta legile celorlalte țări în care activează, rezultatul cel mai plauzibil fiind că se vor retrage din România și, prin urmare, firmele și organizațiile române vor avea de suferit din cauza lipsei accesului la expertiza de top internațională în domeniu.

3. **Extinderea atribuțiilor SRI, inclusiv pentru „campanii de propagandă sau dezinformare"**

Art 51 propune extinderea domeniilor de securitate națională, inclusiv pentru aspecte dincolo de scopul legii de securitate cibernetica - (vezi litera o) sau p) propuse. Aceasta ar trebui să se facă pe baza unei analize exhaustive și cu un text extrem de clar, nu vag - *vezi* în acest sens deciziile CCR nr.91/2018 și nr.802/2018.

> *Art. 50. La articolul 3 din Legea nr. 51/1991 privind securitatea națională a României, republicată în Monitorul Oficial, Partea I, nr. 190 din 18 martie 2014, cu modificările și completările ulterioare, după litera m), se introduc trei noi litere, literele n), o) și p), care vor avea următorul cuprins:*
>
> *"n) amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național;*
>
> *o) acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului în raport cu riscurile și amenințările de tip hibrid;*
>
> *p) acțiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spațiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituțională.".*

În măsura în care nu sunt definite clar ce înseamnă următoarele sintagme: "campanii de propagandă sau dezinformare" sau "reziliența statului" sau "riscurile și amenințările de tip hibrid", ele practic pot să însemne orice dorește Serviciul Român de Informații, ceea ce contrazice practicii CCR:

Vezi par 83 decizia CCR 91/2018

"Astfel, din modul de reglementare a sintagmei analizate, rezultă că se poate circumscrie unei amenințări la adresa securității naționale orice faptă/acțiune cu sau fără conotație penală care afectează un drept sau o libertate fundamentală. Cu alte cuvinte, sfera de aplicare a dispoziției criticate este atât de largă, încât față de orice persoană se poate reține exercitarea unei acțiuni care constituie amenințare la adresa securității naționale."

Și par 80 decizia CCR 802/2018:

"Caracterul deschis al sintagmei criticate determină posibilitatea introducerii sau excluderii de elemente în/din această categorie, acțiune care se răsfrânge și asupra limitelor de aplicare a dispoziției de lege criticate. În acest mod, limitele de aplicare a dispoziției de lege criticate nu mai pot fi cunoscute de destinatarii normei, care, astfel, nu își pot corecta conduită și nu pot fi capabili să prevadă, într-o măsură rezonabilă, consecințele care pot apărea dintr-un act

determinat."

Alți termeni ca "infrastructurilor informatice și de comunicații de interes național" sunt folosiți, fără a fi clar dacă se referă la terminologia din alte legi 2 sau nu. Unii termeni sunt definiți într-un fel (de ex. "reziliență cibernetică" care însă efectiv poate fi orice), dar sunt folosiți în cu totul alt context - "reziliența statului".

În ceea ce privește lit p), acum va deveni astfel infracțiune exprimarea unor opinii pe contrasensul acțiunii statale (de exemplu de vaccinare, ca sa luăm un subiect care a polarizat societatea românească) sau punerea unor întrebări incomode sau formularea de opinii contrare unei politici oficiale a statului, cum ar fi chiar politica de securitate cibernetică.

Calificarea ca amenințări la adresa securității naționale, a unor poziții publice împotriva cursului politicii oficiale a statului, va face ca autorii acestor poziții critice, îndreptate „împotriva curentului", să devină autori ai unei infracțiuni contra securității statului, prevăzută la art. 404 din Codul penal, infracțiune denumită „Comunicarea de informații false" și care are următorul conținut:

> *Comunicarea sau răspândirea, prin orice mijloace, de ştiri, date sau informaţii false ori de documente falsificate, cunoscând caracterul fals al acestora, dacă prin aceasta se pune în pericol securitatea naţională, se pedepseşte cu închisoarea de la unu la 5 ani*."

Până acum, din cauză că aceste poziții critice orientate împotriva curentului politicii oficiale nu erau calificate de Legea 51/1991 ca amenințări la adresa securității naționale, aceste critici deranjante pentru putere nu puteau fi încadrare în infracțiunea din art. 404 Cod penal. Acum, după includerea acestor critici în categoria amenințărilor la securitatea națională, va fi relativ simplu de inițiat dosare penale, pentru o infracțiune gravă – privind securitatea națională – criticilor mai mult sau mai puțin înverșunați, ai puterii politice, ceea ce este - in opinia noastră - încălcare a libertății de exprimare.

4. Extinderea obligațiilor contrar Directivelor UE NIS.

Prin noul articol 22 practic avem de-a face cu o extindere a Legii nr. 362/2018 (care implementează corect Directiva NIS), de la câteva sectoare critice și aproximativ 700 de firme și autorități (Operatori de servicii esențiale) la probabil câteva sute de mii de persoane juridice, aspect care este considerat excesiv inclusiv de către legislația UE.

Acest lucru ar fi, deci, o încălcare a acquis-ului comunitar, conform art 16 alin 11 și a considerentului nr.53 din directiva NIS[4], care explică de ce:

Pentru a evita impunerea unei sarcini financiare și administrative disproporționate asupra operatorilor de servicii esențiale și a furnizorilor de servicii digitale, cerințele ar trebui să fie

[4] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32016L1148

proporționale cu riscurile la care este expusă rețeaua și sistemul informatic în cauză, ținând seama de cea mai avansată tehnologie corespunzătoare unor astfel de măsuri. În cazul furnizorilor de servicii digitale, aceste cerințe nu ar trebui să se aplice microîntreprinderilor și întreprinderilor mici.

Și pentru directiva NIS2 (recent adoptată de Parlamentul European) se face o limitare la întreprinderi medii și mari.[5]

5. **Amenzi care pot închide o firmă**

Amenzile propuse în art 48 lit b) de la 1% din cifra de afaceri pentru prima abatere (!) până la 3% din cifra de afaceri la a doua abatere (!!). Corelând cu informațiile de mai sus, practic rezultă că orice neraportare a unui incident de securitate sau lipsa de cooperare în delațiunea către stat poate duce la o sancțiune care va duce la închiderea unei firme mici sau mijlocii, în contextul în care încălcarea în sine nu afectează securitatea națională. În orice act normativ european, amenzile din cifra de afaceri sunt excepția, doar în cazul în care primele amenzi nu sunt disuasive.

Având în vedere cele descrise mai sus, vă invităm să analizați potențialul de neconstituționalitate al legii privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative și oportunitatea sesizării Curții Constituționale a României.

Persoană de Contact: Bogdan Manolea, bogdan.manolea@apti.ro 0721 205 603

Semnatari:

Asociația pentru Tehnologie și Internet
APADOR-CH
Miliția Spirituală
Asociația Respiro
FILIA
Átlátszó Erdély
Centrul pentru Inovare Publică
Mediawise
Asociația Interlan
Asociația pentru Dezvoltarea Internetului
CeRe: Centrul de Resurse pentru participare publică

---

[5] Vezi Articolul 3 din varianta Directivei NIS2 adoptată de Parlamentul European:
Entități esențiale și importante
1. În sensul prezentei directive, următoarele entități sunt considerate ca fiind entități esențiale:
(a) entitățile de un tip menționat în anexa I care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la articolul 2 alineatul (1) din anexa la Recomandarea 2003/361/CE;
https://www.europarl.europa.eu/doceo/document/TA-9-2022-0383_EN.html#title2

Asociația Code for Romania - Codează pentru România
Centrul pentru Jurnalism Independent