București, 22 decembrie 2022

Către: ***CURTEA CONSTITUȚIONALĂ A ROMÂNIEI***

Domnului Marian ENACHE,

PREȘEDINTELE CURȚII CONSTITUȚIONALE

Domnule Președinte,

În conformitate cu prevederile **art. 146 lit. a) din Constituția României**, republicată, **art. 136 alin. (3) din Regulamentul Camerei Deputaților**, precum și ale **art. 15 alin. (1) și (2) din Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale**, republicată, deputații menționați în anexele atașate, formulăm prezenta

OBIECȚIE DE NECONSTITUȚIONALITATE

cu privire la ***Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normativ***

(**L828/2022, PI-x nr. 773/2022**),

pe care o considerăm **neconformă cu o serie de articole din Constituția României**, solicitând respectuos instanței de contencios constituțional **constatarea neconstituționalității** acesteia pentru motivele expuse în continuare.

CUPRINS

I. SITUAȚIA DE FAPT

Legea care face obiectul prezentei obiecții a fost inițiată în anul 2022, sub denumirea ***„Proiect de Lege privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative“*** de către Guvernul României.

Conform expunerii de motive, legea votată are ca obiect reglementarea cadrului juridic și instituțional referitor la organizarea și desfășurarea activităților din domeniile securitate cibernetică și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate.

Prin conținutul său normativ, legea votată face parte din categoria **legilor organice**, prima Cameră sesizată fiind Camera Deputaților, în conformitate cu dispozițiile art. 75 alin. (1) din Constituția României, republicată.

Proiectul de lege votat de Senat, în calitate de cameră decizională, Pl-x nr. 773/2022, înregistrat la Senat cu nr. L828/2022, încalcă flagrant **art. 1 alin. (5), art. 26, art. 30, art. 147 alin. (4) și art. 148 alin. (2) din Constituția României**.

II. TEMEIUL CONSTITUȚIONAL

Constituția României

Articolul 1 ***Statul român***

(3) România este stat de drept, democratic şi social, în care demnitatea omului, drepturile şi libertățile cetățenilor, libera dezvoltare a personalității umane, dreptatea şi pluralismul politic reprezintă valori supreme, în spiritul tradițiilor democratice ale poporului român şi idealurilor Revoluției din decembrie 1989, şi sunt garantate.

(4) Statul se organizează potrivit principiului separației şi echilibrului puterilor – legislativă, executivă şi judecătorească – în cadrul democrației constituționale.

(5) În România, respectarea Constituției, a supremației sale și a legilor este obligatorie.

Articolul 26 ***Viața intimă, familială şi privată***

(1) Autoritățile publice respectă şi ocrotesc viața intimă, familială şi privată.

(2) Persoana fizică are dreptul să dispună de ea însăşi, dacă nu încalcă drepturile şi libertățile altora, ordinea publică sau bunele moravuri.

Articolul 30 ***Libertatea de exprimare***

(1) Libertatea de exprimare a gândurilor, a opiniilor sau a credinţelor şi libertatea creaţiilor de orice fel, prin viu grai, prin scris, prin imagini, prin sunete sau prin alte mijloace de comunicare în public, sunt inviolabile.

(2) Cenzura de orice fel este interzisă.

(3) Libertatea presei implică şi libertatea de a înfiinţa publicaţii.

(4) Nici o publicaţie nu poate fi suprimată.

(5) Legea poate impune mijloacelor de comunicare în masă obligaţia de a face publică sursa finanţării.

(6) Libertatea de exprimare nu poate prejudicia demnitatea, onoarea, viaţa particulară a persoanei şi nici dreptul la propria imagine.

(7) Sunt interzise de lege defăimarea ţării şi a naţiunii, îndemnul la război de agresiune, la ură naţională, rasială, de clasă sau religioasă, incitarea la discriminare, la separatism teritorial sau la violenţă publică, precum şi manifestările obscene, contrare bunelor moravuri.

(8) Răspunderea civilă pentru informaţia sau pentru creaţia adusă la cunoştinţă publică revine editorului sau realizatorului, autorului, organizatorului manifestării artistice, proprietarului mijlocului de multiplicare, al postului de radio sau de televiziune, în condiţiile legii. Delictele de presă se stabilesc prin lege.

Articolul 147 ***Deciziile Curţii Constituţionale***

(1) Dispoziţiile din legile şi ordonanţele în vigoare, precum şi cele din regulamente, constatate ca fiind neconstituţionale, îşi încetează efectele juridice la 45 de zile de la publicarea deciziei Curţii Constituţionale dacă, în acest interval, Parlamentul sau Guvernul, după caz, nu pun de acord prevederile neconstituţionale cu dispoziţiile Constituţiei. Pe durata acestui termen, dispoziţiile constatate ca fiind neconstituţionale sunt suspendate de drept.

(2) În cazurile de neconstituţionalitate care privesc legile, înainte de promulgarea acestora, Parlamentul este obligat să reexamineze dispoziţiile respective pentru punerea lor de acord cu decizia Curţii Constituţionale.

(3) În cazul în care constituţionalitatea tratatului sau acordului internaţional a fost constatată potrivit articolului 146 litera b), acesta nu poate face obiectul unei excepţii de neconstituţionalitate. Tratatul sau acordul internaţional constatat ca fiind neconstituţional nu poate fi ratificat.

(4) Deciziile Curţii Constituţionale se publică în Monitorul Oficial al României. De la data publicării, ***deciziile sunt general obligatorii*** *şi au putere numai pentru viitor.*

Articolul 148 ***Integrarea în Uniunea Europeană***

(1) Aderarea României la tratatele constitutive ale Uniunii Europene, în scopul transferării unor atribuții către instituțiile comunitare, precum şi al exercitării în comun cu celelalte state membre a competențelor prevăzute în aceste tratate, se face prin lege adoptată în şedința comună a Camerei Deputaților şi Senatului, cu o majoritate de două treimi din numărul deputaților şi senatorilor.

(2) Ca urmare a aderării, prevederile tratatelor constitutive ale Uniunii Europene, precum şi celelalte reglementări comunitare cu caracter obligatoriu, au prioritate față de dispozițiile contrare din legile interne, cu respectarea prevederilor actului de aderare.

(3) Prevederile alineatelor (1) şi (2) se aplică, în mod corespunzător, şi pentru aderarea la actele de revizuire a tratatelor constitutive ale Uniunii Europene.

(4) Parlamentul, Preşedintele României, Guvernul şi autoritatea judecătorească garantează aducerea la îndeplinire a obligațiilor rezultate din actul aderării şi din prevederile alineatului (2).

(5) Guvernul transmite celor două Camere ale Parlamentului proiectele actelor cu caracter obligatoriu înainte ca acestea să fie supuse aprobării instituțiilor Uniunii Europene.

III. MOTIVE DE NECONSTITUȚIONALITATE

III.1. Art. 3 alin. (1) din legea adoptată încalcă dispozițiile art. 1 alin. (5) din Constituția României în componenta sa referitoare la principiul securității juridice, previzibilității și clarității normelor, astfel cum a fost dezvoltat într-o bogată jurisprudență constituțională[1], art. 26 și art. 30 din Constituția României, fiind contrar Deciziei CCR nr. 17/2015;

Conform art. 3 alin. (1) lit. c) din textul votat, *„(...) 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 fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la lit. b)“*.

Astfel, includerea 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.

Date fiind lipsa de claritate a textului citat şi sfera prea largă de persoane fizice şi juridice cărora li se adresează soluția legislativă, obligațiile prevăzute sunt imposibil de îndeplinit, spre exemplu, în cazul oricăreia dintre următoarele entități:

[1] Principii de claritate reafirmate în Decizia CCR nr. 17/2015 (în special în par. 86-97)

- un site cu foarte puțini utilizatori, administrat de un PFA la un ONG, care oferă un serviciu online (care este public prin natura sa);

- 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).

De asemenea sintagma de *„*(...) *sisteme informatice (...) 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",* face ca orice serviciu informatic care se bazează pe un sistem informatic (de ex. SaaS în cloud) să fie inclus in această definiție. Aceasta include de la un cont pe Facebook, Instagram, Gmail sau Yahoo până la un serviciu de acces la legislație online, un serviciu de notificări de la Parlamentul European sau orice alt serviciul online similar.

Potrivit dispozițiilor art. 1 alin. (5) din Constituție, *„În România, respectarea Constituției, a supremației sale și a legilor este obligatorie"*. Această obligație, care revine atât persoanelor fizice cât și persoanelor juridice, se aplică în egală măsură și Parlamentului, inclusiv în privința modului de exercitare a atribuției sale principale și esențiale, respectiv aceea de unică autoritate legiuitoare a țării, care constă în **elaborarea proiectelor de lege și adoptarea acestora ca legi ale statului român**.

Curtea Constituțională, a reținut, în jurisprudența sa constantă, că **respectarea prevederilor Legii nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative constituie un veritabil criteriu de constituționalitate** prin raportare la aplicarea art. 1 alin. (5) din Constituție. De asemenea, instanța constituțională a reținut că accesibilitatea și previzibilitatea legii sunt cerințe ale principiului securității raporturilor juridice, constituind garanții împotriva arbitrariului (Decizia nr. 139 din 13 martie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 336 din 3 mai 2019).

În acest sens, prin Decizia nr. 681/2021 și Decizia nr. 26/2012, Curtea Constituțională a reținut următoarele: *„Deși normele de tehnică legislativă nu au valoare constituțională, **Curtea constată că prin reglementarea acestora legiuitorul a impus o serie de criterii obligatorii pentru adoptarea oricărui act normativ, a căror respectare este necesară pentru a asigura sistematizarea, unificarea și coordonarea legislației, precum și conținutul și forma juridică adecvate pentru fiecare act normativ**. Astfel, respectarea acestor norme concură la asigurarea unei legislații care respectă principiul securității raporturilor juridice, având claritatea și previzibilitatea necesare.*

Totodată, trebuie avute în vedere și dispozițiile constituționale ale art. 142 alin. (1), potrivit cărora „Curtea Constituțională este garantul supremației Constituției", și pe cele ale art. 1 alin. (5) din Constituție, potrivit cărora, „în România, respectarea [...] legilor este obligatorie". Astfel, Curtea constată că reglementarea criticată prin nerespectarea normelor de tehnică legislativă determină apariția unor ***situații de incoerență și instabilitate, contrare principiului securității raporturilor juridice în componenta sa referitoare la claritatea și previzibilitatea legii****."*

Cu toate că principiul calității legii nu este enunțat în mod expres prin Constituție, acesta a fost recunoscut și consacrat prin jurisprudența Curții Constituționale, care a stabilit că **originea acestuia se regăsește în art. 1 alin. (5) din Legea fundamentală**. La modul general, s-a considerat că legea trebuie să îndeplinească anumite cerințe de claritate și previzibilitate pentru a putea fi respectată de destinatarii săi, în sensul adaptării corespunzătoare a conduitei de către aceștia.

În același sens, prin Decizia nr. 473/2013, Curtea Constituțională a statuat, de principiu, că *„orice act normativ trebuie să îndeplinească anumite condiții calitative, printre acestea numărându-se previzibilitatea, ceea ce presupune că acesta trebuie să fie suficient de precis și clar pentru a putea fi aplicat; astfel, formularea cu o precizie suficientă a actului normativ permite persoanelor interesate - care pot apela, la nevoie, la sfatul unui specialist - să prevadă într-o măsură rezonabilă, în circumstanțele speței, consecințele care pot rezulta dintr-un act determinat. Desigur, poate să fie dificil să se redacteze legi de o precizie totală și o anumită suplețe poate chiar să se dovedească de dorit, suplețe care nu trebuie să afecteze însă previzibilitatea legii."*

Textul normativ care face obiectul prezentei sesizări nu respectă cerințele de calitate a legii, sub aspectul clarității, previzibilității și preciziei normei, prevăzute de art. 36 alin. (1) din Legea nr. 24/2000, republicată, cu modificările și completările ulterioare, cerințe care se circumscriu principiului legalității prevăzut la art. 1 alin. (5) din Constituție.

Previzibilitatea unei norme presupune în mod obligatoriu ca destinatarul acesteia să aibă o reprezentare clară a aspectelor în funcție de care este obligat să își modeleze conduita. Or, prin lipsa de precizie și claritate, destinatarii normei juridice nu își pot forma o reprezentare clară a drepturilor și obligațiilor. Acest aspect contravine flagrant principiilor fundamentale ale legalității și securității juridice, statuate prin art. 1 alin. (5) din Constituție și prin jurisprudența constantă a Curții Constituționale.

Așadar, pentru motivul anterior precizat, ambiguitatea redacțională și lipsa de previzibilitate a legii supuse controlului de constituționalitate este evidentă, de necontestat, ceea ce determină serioase îndoieli cu privire la efectele pe care legea le-ar

putea produce (a se vedea, mutatis mutandis, Decizia nr. 619 din 11 octombrie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 6 din 4 ianuarie 2017, paragraful 45). Astfel, prin modul deficitar de redactare, legea contestată încalcă exigențele art. 1 alin. (5) din Constituție în componenta sa referitoare la calitatea și previzibilitatea legii, cu consecința neconstituționalității legii în ansamblul său.

Legea criticată încalcă principiul securității juridice, consacrat de art. 1 alin. (5) din Constituție, care stabilește că: *„în România, respectarea Constituției, a supremației sale şi a legilor este obligatorie“*. Concret, principiul securității juridice are drept componentă previzibilitatea legii.

Conform jurisprudenței Curții Constituționale, principiul securității juridice se referă la faptul că cetățenii trebuie protejați contra unui pericol creat de legiuitor, prin normele juridice pe care le propune și adoptă, în sens contrar fiind afectată însăși securitatea juridică a persoanei. Astfel, legiuitorul are *„obligația constituțională de a asigura atât o stabilitate firească dreptului, cât și valorificarea în condiții optime a drepturilor și a libertăților fundamentale“* (a se vedea Decizia nr. 51 din 25 ianuarie 2012, Decizia nr. 90 din 3 februarie 2012, Decizia nr. 240 din 3 iunie 2020, Decizia nr. 504 din 12 iunie 2020, Decizia nr. 454 din 4 iulie 2018, Decizia nr. 836 din 1 octombrie 2018, Decizia nr. 187 din 17 martie 2021, Decizia nr. 478 din 7 mai 2021 și Decizia nr.688 din 21 octombrie 2021).

De asemenea, în speță, subiecții legii și obligațiile lor sunt vagi și neclare. Art. 3 alin. (1) are pretenția de a defini domeniul de aplicare a acestei legi, dar identifică mai puțin subiecții legi. Cu toate acestea obligațiile principale pentru aceste categorii (art 21, art. 37, art. 41-44) se referă la *„persoanele prevăzute la art. 3“*, deși art. 3 enumeră rețelele și sistemele informatice unde se aplică legea. Un asemenea text vag nu îndeplinește cerințele explicitate de către CCR în par. 69 din Decizia nr. 17/2015, dar, și mai mult, excede din toate punctele de vedere măsurii din PNRR în cadrul căreia a fost promovat acest text legislativ.

În plus, articolul contestat nu respectă par. 69 al Deciziei CCR 17/2015, potrivit cu care:

„Or, dispozițiile legale în forma supusă controlului de constituționalitate prezintă ***un grad mare de generalitate****, obligațiile vizând totalitatea deținătorilor de infrastructuri cibernetice, constând în sisteme informatice, aplicații aferente, rețele şi servicii de comunicații electronice,* ***indiferent de importanța acestora care poate viza interesul național sau doar un interes de grup ori chiar particular****. Pentru a evita impunerea unei sarcini disproporționate asupra micilor operatori,* ***cerințele trebuie să fie proporționale cu riscurile la care sunt expuse rețeaua sau sistemul informatic în***

<u>cauză şi nu trebuie aplicat deținătorilor de infrastructuri cibernetice cu importanță nesemnificativă din punctul de vedere al interesului general</u>.”

Trebuie avut în vedere faptul că Internetul este un spațiu ubicuu - deci nu doar infrastructura informatică din România poate cauza probleme sistemelor informatice din România. A impune astfel de obligații **<u>la nivel național</u>** nu rezolvă problema de fond a asigurării securității, ci doar **împovărează operatorii de bună-credință din România**.

Chiar și Directivele NIS1 (în vigoare) și NIS2 (aproape de finalizarea procesului de adoptare) exceptează IMM-urile de la obligațiile din domeniul securității informatice - în acest sens, a se vedea și comentariul de la art. 22 cu privire la limitele pentru IMM-uri.

<u>III.2. Articolele 21-22 din legea adoptată încalcă dispozițiile art. 1 alin. (5), art. 26. art. 30 și art. 148 alin. (2) din Constituția României;</u>

Conform art. 21 din textul votat, *„**(1)** Persoanele prevăzute la art. 3 alin. (1) lit. b) și lit. c), au obligația de a notifica incidentele de securitate cibernetică prin intermediul PNRISC, de îndată, dar nu mai târziu de 48 de ore de la constatarea incidentului.“*

Conform art. 22 din textul votat, *„Incidentele de securitate cibernetică sunt notificate în PNRISC în condițiile Capitolului IV, Secțiunea a 2-a din Legea nr. 362/2018, cu modificările şi completările ulterioare.“*

Propunerea legislativă adoptată **nu se integrează organic în sistemul legislativ**, nefiind corelată cu obligațiile asumate de România la momentul aderării la Uniunea Europeană și cu prevederile din Tratatul privind funcționarea Uniunii Europene, fiind încălcate art. 1 alin. (5) și art. 148 din Constituție referitor la integrarea în Uniunea Europeană.

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 mici și mari la probabil câteva sute de mii de persoane juridice, aspect care este considerat excesiv de către legislația UE.

Astfel, derivă nerespectarea art. 148 alin. (2) din Constituţie, potrivit căruia reglementarea europeană are prioritate faţă de legea internă. Iar noua lege internă este contrară obligațiilor asumate (prioritatea dreptului comunitar).

Prin modalitatea de reglementare adusă în discuție de proiectul de lege votat, se încalcă acquis-ul comunitar, respectiv considerentul 53 din directiva NIS[2]:

„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 <u>proporționale</u> *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 <u>nu</u> ar trebui să se aplice microîntreprinderilor și întreprinderilor mici****."*

De asemenea, și pentru propunerea de Directivă NIS2 (recent adoptată de Parlamentul European) se face o limitare a obiectului de aplicare la anumite domenii și la întreprinderi medii și mari.

Aparent, sesizarea PNRISC de către victima unui incident de securitate cibernetică pare a fi benefică, deoarece respectiva platformă este special destinată rezolvării unor astfel de incidente. Dar, din cauza definirii neclare în proiectul de lege a noțiunii de incident de securitate cibernetică, se poate ajunge la situația în care pentru o simplă virusare sau pentru o aparentă virusare (=o nefuncționare normală) a unui laptop, orice persoană care are o activitate ce poate fi considerată (de către cine?) ca fiind de interes public să fie obligată să sesizeze PNRISC și, implicit, să pună la dispoziția specialiștilor PNRISC a laptopului, cu toate datele și informațiile cu caracter personal conținute de acel laptop. Aceasta este o intruziune importantă în viața privată a persoanei, intruziune asupra căreia deținătorul laptopului nu are, deși ar trebui să aibă, un drept de liberă apreciere, adică nu poate opta dacă sesizează sau nu PNRISC, ci există o obligație legală strictă, sancționată sever cu amendă contravențională, de a se adresa PNRISC și, implicit, de a pune la dispoziția unor terți o multitudine de date și informații privind viața privată, conținute, de exemplu, într-un laptop, care va fi accesat de terții care vor rezolva incidentul de securitate cibernetică.

De aceea, ar trebui ca obligația de raportare a incidentelor de securitate cibernetică (art. 21), astfel cum sunt definite în mod ambiguu prin art. 2, să fie prevăzută doar pentru autoritățile/instituțiile din sectorul public, lăsând pentru entitățile din mediul privat doar facultatea (nu obligația) de a sesiza PNRISC.

<u>III.3. Articolul 25 din legea adoptată încalcă dispozițiile art. 1 alin. (5), art. 26 și art. 30 din Constituția României, fiind contrar Deciziei CCR nr. 17/2015;</u>

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex:32016L1148

Conform art. 25 alin. (1) din legea votată, *„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 și interconectarea acestora cu terții și cu utilizatorii finali"*.

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.

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 legii votate privind securitatea cibernetică a României, **acești furnizori sunt obligați ca, la orice întrebare de la una din instituțiile din art. 10, să-și reclame/denunțe proprii clienți**. Fără a exista un mandat judecătoresc, fără autorizare expresă, acești furnizori sunt obligați să dea informații despre starea securității unui client, sau, mai grav, 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 alin. (2), informațiile sunt de o sensibilitatea extremă, mai ales când spectrul de aplicare de la art. 3 alin. (1) lit. 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 să raporteze orice potențială problemă a unui site de media care publică știri și investigații, care pot ajunge chiar către autoritățile despre care sunt materialele. 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**.

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

Deci mult clamata colaborare - este de fapt o obligație de delațiune (care nu există în niciun alt stat membru al UE) 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.

Scopul ar fi, conform declarațiilor publice ale MCID: *„Fiecare autoritate publică cu atribuții în domeniul securității cibernetice, pentru a-și putea exercita atribuțiile legale de protejare a rețelelor și sistemelor informatice, are nevoie de o colaborare loială cu furnizorii de servicii de securitate cibernetică. Această colaborare presupune inclusiv protejarea rețelelor și a sistemelor informatice ale acelor furnizori, care deservesc unor scopuri publice sau private.“*

De fapt, obligația impusă este o ignorare completă a importanței confidențialității în relația dintre doi 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).

De asemenea, această obligație împiedică experții și furnizorii de servicii de securitate informatică străini să își furnizeze 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 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.

III.4. Articolele 50-51 din legea adoptată încalcă dispozițiile art. 1 alin. (5), art. 26 și art. 30 din Constituția României, fiind contrar Deciziilor CCR nr. 91/2018 și 802/2018;

Conform art. 50 din legea votată, *„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) - 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 acest sens, extinderea domeniilor de securitate națională trebuie să se facă pe baza unei analize exhaustive și cu un text extrem de clar și nu vag (a se vedea în acest sens Decizia CCR nr. 91/2018 și Decizia CCR nr. 802/2018).

În măsura în care nu sunt definite noțiunile de *„a unor campanii de propagandă sau dezinformare”*, *„reziliența statului”* sau *„riscurile și amenințările de tip hibrid”*, ele practic pot să însemne orice apreciază Serviciul Român de Informații, ceea ce contrazice deciziile CCR menționate:

Conform par. 83 din Decizia CCR nr. 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****.”*

Conform par. 80 din Decizia nr. 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 conduita și nu pot fi capabili să prevadă, într-o măsură rezonabilă, consecințele care pot apărea dintr-un act determinat.”*

Art. 50 din textul votat propune extinderea domeniilor de securitate națională, inclusiv pentru aspecte dincolo de scopul legii de securitate cibernetică (a se vedea litera o) sau p). Aceasta ar trebui să se facă pe baza unei analize exhaustive și cu un text

extrem de clar, nu vag - a se vedea în acest sens Deciziile CCR nr. 91/2018 și nr. 802/2018.

A introduce toate rețelele şi sistemele informatice în sistemul de protecție a securității naționale (*„sectorul”* cibernetic al securității naționale), este **excesiv şi dăunător pentru libertatea de exprimare şi dreptul la viață privată**.

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 (Legea nr. 163/2021) sau nu. Unii termeni sunt definiți într-un fel (de ex. *„reziliență cibernetică”* care 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 neobediente 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 informații false ori de documente falsificate, cunoscând caracterul fals al acestora, dacă prin aceasta se pune în pericol securitatea națională, 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 nr. 51/1991 ca amenințări la adresa securității naționale, aceste critici deranjante pentru putere nu puteau fi încadrate 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.

III.5. Art. 41 din legea adoptată încalcă dispozițiile art. 1 alin. (5), în componenta sa referitoare la principiul securității juridice, previzibilității şi clarității normelor, art. 26 şi art. 30 din Constituția României;

Conform art. 41 din textul votat, *„(1) Persoanele prevăzute la art. 3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare, în conformitate cu prevederile art. 52 alin. (1)“*.

Acest proces de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare sunt aspecte complexe de securitate cibernetică care trebuie să fie implementate doar de autorități publice și firme mari, conform acquis-ului comunitar existent (a se vedea în acest sens Directivele NIS 1 și NIS 2, menționate mai sus).

Astfel, extinderea sferei persoanelor face ca spectrul de aplicare să fie exagerat de larg, generându-se o lipsă de previzibilitate cu privire la efectele pe care legea le-ar putea avea.

III.6. Art. 48 din legea adoptată încalcă dispozițiile art. 1 alin. (5) din Constituția României în componenta sa referitoare la principiul securității juridice, previzibilității și clarității normelor;

Sunt contravenții diferite omisiunea de *„notificare“* a incidentului de securitate cibernetică și omisiunea de *„comunicare completă“* a incidentului de securitate. Cu toate acestea, doar noțiunea de *„notificare“* este definită, în art. 22 (prin trimitere la o altă lege, respectiv la Legea nr. 362/2018), dar noțiunea de „comunicare completă“ nu este definită, astfel că nu se poate cunoaște dacă, atunci când ai raportat un incident, acea raportare a fost *„notificare“* sau *„comunicare completă“*.

IV. CONCLUZII.

În ciuda unor 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, 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, anterior menționată. Cu toate acestea, proiectul reia în mare parte instituții și principii care au fost criticate și în actul normativ declarat neconstituțional.

În considerarea tuturor argumentelor expuse, vă solicităm respectuos **admiterea prezentei obiecții de neconstituționalitate a Legii privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normativ** (**PI-x nr. 773/2022**)**.**

ANEXE

- L828/2022 (PL-x nr. 773/2022), în forma pentru promulgare.