ROMÂNIA
Avocatul Poporului
Str. George Vraca nr. 8, Sector 1, București
www.avp.ro
Tel.: +40-21-312.71.01, Fax: +40-21-312.49.21, E-mail: avp@avp.ro
Tel. dispecerat: +40-21-312.71.34, E-mail: petitii@avp.ro

AVOCATUL POPORULUI
REGISTRATURĂ GENERALĂ
IEȘIRE NR. 32636 / 27. DEC. 2022

Domnului Marian Enache,

Președintele Curții Constituționale

CURTEA CONSTITUȚIONALĂ
REGISTRATURĂ JURISDICȚIONALĂ
NR. 9125 / 27 DEC 2022

În conformitate cu dispozițiile art. 146 lit. a) din Constituție și ale art. 15 alin. (1) lit. h) din Legea nr. 35/1997 privind organizarea și funcționarea instituției Avocatul Poporului, republicată, vă transmitem, alăturat, **sesizarea de neconstituționalitate** referitoare la prevederile **Legii privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (PL-x nr. 773/2022, L828/2022).**

Vă asigur, Domnule Președinte, de înalta mea considerație,

Avocatul Poporului,

Renate Weber

ROMÂNIA
Avocatul Poporului
Str. George Vraca nr. 8, Sector 1, București
www.avp.ro
Tel.: +40-21-312.71.01, Fax: +40-21-312.49.21, E-mail: avp@avp.ro
Tel. dispecerat: +40-21-312.71.34, **E-mail**: petitii@avp.ro

În conformitate cu dispozițiile art. 146 lit. a) din Constituția României și ale art. 15 alin. (1) lit. h) din Legea nr. 35/1997 privind organizarea și funcționarea instituției Avocatul Poporului, republicată,

Avocatul Poporului formulează,
în termenul legal prevăzut de art. 15 alin. (2) din Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale, republicată, prezenta

Sesizare de neconstituționalitate

referitoare la prevederile Legii privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (*PL-x nr. 773/2022, L828/2022*), din perspectiva următoarelor

MOTIVE DE NECONSTITUȚIONALITATE

Normele legale indicate mai jos, cuprinse în **Legea privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (*PL-x nr. 773/2022, L828/2022*),** prin care este reglementat cadrul juridic și instituțional referitor la organizarea și desfășurarea activităților din domeniile securității cibernetice și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate, încalcă prevederile **art. 1 alin. (5), art. 11 și art. 148 alin. (4) din Constituție, referitoare, pe de-o parte, la lipsa de previzibilitate și claritate a normei legale, iar, pe de altă parte, la încălcarea angajamentelor internaționale în materie de securitate cibernetică asumate de România.**

1. Prevederile art. 3 alin. (1) lit. c) teza finală din Legea privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (PL-x nr. 773/2022, L828/2022) contravin art. 1 alin. (5) din Constitutia României din perspectiva considerentelor prezentate mai jos

Astfel, potrivit dispozițiilor **art. 3 alin. (1)** din Legea criticată *„În domeniul securității cibernetice, prezenta lege se aplică următoarelor:* ***a)*** *rețelele și sistemele informatice deținute, organizate, administrate, utilizate sau aflate în competența autorităților și instituțiilor publice din domeniul apărării, ordinii publice, securității naționale, justiției, situațiilor de urgență. Oficiului Registrului Național al Informațiilor Secrete de Stat;* ***b)*** *rețelele și sistemele informatice deținute de persoanele fizice și juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale;* ***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)***".

Sintagma prevăzută în **art. 3 alin. (1) lit. c) teza finală din Legea precitată** relevă un grad sporit de generalitate, întrucât nu sunt identificate și definite în mod clar și previzibil persoanele fizice și juridice care furnizează servicii publice ori de interes public, în contextul în care acestea sunt altele decât persoanele fizice și juridice de drept privat care dețin rețelele și sistemele informatice pe care le utilizează în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale. Ca atare, în această categorie pot fi cuprinse, după caz, orice fel de persoane fizice și juridice care furnizează servicii publice ori de interes public fără a face vreo distincție, fiind așadar imposibil să fie identificate cu exactitate persoanele cărora le incumbă obligațiile prevăzute de actul normativ criticat. Altfel spus, apreciem că, **legiuitorul, în acest caz, nu a identificat în mod riguros subiecții vizați prin reglementările în cauză.**

În lipsa unor determinări clare ale legii cu privire la destinatarii concreți ai acesteia, autoritatea executivă, Guvernul, își va exercita funcția sa legală de adoptare a hotărârii, potrivit art. 108 alin. (2) din Constituție, pentru organizarea executării legii, în mod defectuos. Faptul că legiuitorul primar lasă o marjă largă de apreciere legiuitorului delegat cu privire la categoriile de persoane fizice și juridice care furnizează servicii publice ori de interes public, fără indicarea unor criterii de identificare concise poate conduce la o reglementare infralegală trunchiată, incompletă sau prea generală, dar în niciun caz exhaustivă. Apreciem că, această modalitate deficitară de reglementare poate fi corectată numai pe calea controlului de constituționalitate exercitat de Curtea Constituțională și nu pe calea controlului exercitat de instanțele de judecată, întrucât acestea din urmă se pot pronunța numai asupra legalității hotărârilor de Guvern, însă controlul de legalitate devine unul formal în lipsa unor prevederi legale primare clare și previzibile.

Hotărârea Guvernului survine atunci când executarea unor prevederi din lege reclamă stabilirea de măsuri sau a unor reguli subsecvente, care să asigure corecta aplicare a acestora sau organizarea corespunzătoare a unor activități. Deci, hotărârile Guvernului se adoptă întotdeauna în baza legii, fiind *secundum legem* și urmărind organizarea executării și executarea în concret a legii sau, cu alte cuvinte, punerea în aplicare sau ducerea la îndeplinire a legilor.

Așadar, este obligatoriu ca legea să realizeze, la nivel primar, un cadru normativ clar, precis și previzibil, atât pentru persoanele fizice și juridice supuse acestor măsuri, cât mai ales pentru instanțele de judecată, după caz, întrucât acestea pentru a realiza un eventual control de legalitate asupra unui act administrativ (hotărâre de guvern) în corpul legii trebuie să existe repere clare și previzibile la care să se poată raporta în vederea verificării legalității actului administrativ dedus judecății.

În acest sens, legiuitorul primar sau, cu caracter excepțional, legiuitorul delegat este cel care trebuie să reglementeze modul concret de aplicare al legii. Faptul că legiuitorul are o marjă largă de apreciere nu înseamnă că se poate degreva de atributul său de legiferare, cu atât mai mult cu cât doar acesta are dreptul suveran de a aprecia întinderea și amploarea măsurilor pe care le stabilește prin lege, iar domeniul de reglementare în cauză nu aparține actelor cu caracter infralegal. Transferând marja de apreciere către Guvern care stabilește, implicit, criteriile în funcție de care se apreciază care sunt destinatarii normei legale criticate, legiuitorul lasă cale liberă arbitrarului și abuzului de putere. În concluzie, aprecierea asupra oportunității și proporționalității măsurilor în cauză îi revine numai legiuitorului primar, cu respectarea Legii fundamentale și a jurisprudenței instanței de contencios constituțional.

Prin urmare, având în vedere obiectul de reglementare al legii, respectiv organizarea și desfășurarea activităților din domeniile securității cibernetice și apărare cibernetică, precum și mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în aceste domenii, considerăm că

aceste prevederi trebuie apreciate și reglementate la nivelul legiuitorului primar, respectiv de Parlamentul României și nu ulterior, la nivel infralegal, prin hotărâri ale Guvernului.

În consecință, faptul că legiuitorul primar pune în sarcina Guvernului stabilirea prin hotărâre de Guvern, inițiată de Ministerul Cercetării, Inovării și Digitalizării, a categoriilor de persoane prevăzute la art. 3 alin. (l) lit. c), adoptată în maximum 60 de zile de la data intrării în vigoare a prezentei legi, nu reprezintă o rezolvare a problemei, deoarece norma primară nu stabilește în mod clar și concret criteriile în limita cărora Guvernul, ca putere executivă, trebuie să pună legea în executare, întrucât aria de acoperire a subiecților este foarte largă.

Astfel că, lipsa de previzibilitate și claritate a noilor reglementări determină imposibilitatea identificării destinatarilor legii, precum și conformarea acestora la îndeplinirea obligațiilor prevăzute în sarcina lor. Or, pentru a fi înțeleasă și respectată de către destinatarii săi, legea trebuie să îndeplinească anumite cerințe de claritate, astfel încât acești destinatari să își poată adapta în mod corespunzător conduita în acord cu prevederile art. 1 alin. (5) din Constituție, precum și art. 6, art. 8 și art. 23 din Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată și modificată, care prevăd, în esență, că ***„proiectul de act normativ trebuie să instituie reguli necesare, suficiente și posibile care să conducă la o cât mai mare stabilitate și eficiență legislativă”***, iar *„soluțiile pe care le cuprinde trebuie să fie temeinic fundamentate, luându-se în considerare interesul social, politica legislativă a statului român și cerințele corelării cu ansamblul reglementărilor interne și ale armonizării legislației naționale cu legislația comunitară și cu tratatele internaționale la care România este parte, precum și cu jurisprudența Curții Europene a Drepturilor Omului*”.

Tot în acest sens, instanța de contencios constituțional a constatat că autoritatea legiuitoare are obligația de a edicta norme care să respecte trăsăturile mai sus arătate, în acord cu dispozițiile art. 8 alin. (4) teza întâi din Legea nr. 24/2000, modificată, care prevede că *„textul legislativ trebuie să fie formulat clar, fluent și inteligibil, fără dificultăți sintactice și pasaje obscure sau echivoce"*, iar potrivit art. 36 alin. (1) din aceeași lege, *"actele normative trebuie redactate într-un limbaj și stil juridic specific normativ, concis, sobru, clar și precis, care să excludă orice echivoc, cu respectarea strictă a regulilor gramaticale și de ortografie*".

Mai mult, Curtea Constituțională a constatat că prin reglementarea normelor de tehnică legislativă 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 necesară (a se vedea **Decizia Curții Constituționale nr. 17/2015, nr. 26/2012, nr. 903/2010 și nr. 189/2006**).

De asemenea, Curtea Constituțională a mai statuat și faptul că, legea trebuie să precizeze cu suficientă claritate întinderea și modalitățile de exercitare a puterii de apreciere a autorităților în domeniul respectiv, ținând cont de scopul legitim urmărit, pentru a oferi persoanei o protecție adecvată împotriva arbitrariului (a se vedea **Deciziile Curții Constituționale nr. 348/2014 și nr. 302/2017**).

Așadar, *„o dispoziție legală trebuie să fie precisă, neechivocă și să instituie norme clare, previzibile și accesibile a căror aplicare să nu permită arbitrariul sau abuzul și că norma juridică trebuie să reglementeze în mod unitar, uniform și să stabilească cerințe minimale aplicabile tuturor destinatarilor săi*” (**a se vedea și Decizia Curții Constituționale nr. 637/2015, paragraful 34**).

În concluzie, pentru ca legea să satisfacă cerința de previzibilitate, aceasta trebuie să precizeze cu suficientă claritate și precizie întinderea și modalitățile de exercitare a puterii de

apreciere a autorităţilor în domeniul indicat şi ţinând cont şi de scopul legitim urmărit, pentru a oferi o protecţie suficientă şi adecvată împotriva arbitrarului.

În acelaşi sens, Curtea Europeană a Drepturilor Omului a statuat că legea trebuie, într-adevăr, să fie accesibilă justiţiabilului şi previzibilă în ceea ce priveşte efectele sale. 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.

În plus, nu poate fi considerată „*lege*" decât o normă enunţată cu suficientă precizie, pentru a permite cetăţeanului să îşi adapteze conduita în funcţie de aceasta, apelând la nevoie la consiliere de specialitate în materie, el trebuie să fie capabil să prevadă, într-o măsură rezonabilă, faţă de circumstanţele speţei, consecinţele care ar putea rezulta dintr-o anumită faptă (a se vedea Hotărârea din 4 mai 2000, pronunţată în Cauza Rotaru împotriva României, paragraful 52, şi Hotărârea din 25 ianuarie 2007, pronunţată în Cauza Sissanis împotriva României, paragraful 66).

În situația în care puterea executivă emite hotărârea de Guvern în aplicarea unor norme neclare și mult prea generale acesta va întâmpina dificultăți în identificarea tuturor destinatarilor legii, deoarece din formularea propusă (persoane fizice şi juridice care furnizează servicii publice ori de interes public) rezultă o arie mult prea largă de categorii profesionale (spre exemplu: avocați, notari, medici de familie ș.a.) care devine greu de cuprins și mai ales de reglementat pentru că fiecare dintre aceste categorii își desfășoară activitatea conform unor legi speciale, în funcție de activitatea desfășurată de acestea, specifice fiecărei categorii în parte.

Mai mult decât atât, fără a nega necesitatea asigurării securității şi apărării cibernetice, ca dimensiune a securității naționale, menționăm că actul normativ criticat impune persoanelor prevăzute la **art. 3 alin. (1) lit. c)** o serie de sarcini oneroase, cu impact economic semnificativ asupra acestora, întrucât sunt nevoiți să suporte din bugetele proprii cheltuielile necesare îndeplinirii obligațiilor prevăzute de lege în acest sens, și menționăm aici cele stabilite prin **art. 21 alin. (1), art. 24, art. 29, sau art. 37 din Lege,** potrivit cărora:

- **art. 21 alin. (1)** „*Persoanele prevăzute la art. 3 alin. (l) lit. b) şi c), au obligaţia de a notifica incidentele de securitate cibernetică prin intermediul PNRISC, de îndată dar nu mai târziu de 48 de ore de la constatarea incidentului*";

- **art. 24**

„***(1) Asigurarea rezilienţei în spaţiul cibernetic se realizează prin implementarea de măsuri proactive şi reactive de către instituţiile şi persoanele prevăzute la art. 3.***

(2) Măsurile proactive *sunt destinate prevenirii incidentelor de securitate cibernetică şi descurajării autorilor atacurilor din spaţiul cibernetic şi includ:*

a) constituirea şi antrenarea echipelor de răspuns la incidente de securitate cibernetică;

b) asigurarea de resurse umane specializate pentru dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri şi măsuri de control tehnic privind apărarea şi securitatea cibernetică;

c) constituirea şi operarea Centrelor Operaţionale de Securitate;

d) constituirea unei rezerve de resurse şi de capabilităţi întrunite de securitate cibernetică care să poată fi utilizate în caz de necesitate;

e) dezvoltarea unor capabilităţi proactive, care să permită cunoaşterea anticipativă a ameninţărilor din spaţiul cibernetic;

f) finanţarea pentru dezvoltarea capabilităţilor de securitate şi apărare cibernetică, inclusiv din perspectiva cercetării, dezvoltării, inovării şi digitalizării în domeniu şi asimilării tehnologiilor emergente;

g) cooperarea şi schimbul de informaţii între autorităţile competente şi sectorul privat pentru identificarea ameninţărilor cibernetice;

h) identificarea serviciilor, reţelelor şi sistemelor informatice, conform competenţelor fiecărei instituţii responsabile de administrare şi asigurarea managementului acestora;

i) implementarea de soluţii de securitate cibernetică, care să crească capacitatea de detecţie şi capabilităţile de prevenţie la atacuri cibernetice;

j) dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri şi măsuri de control tehnic privind apărarea şi securitatea cibernetică;

k) demonstrarea nivelului de maturitate atins de capabilităţile de securitate cibernetică în cadrul exerciţiilor organizate la nivel naţional sau internaţional;

l) instruirea personalului din cadrul persoanelor prevăzute la art. 3 în domeniul securităţii cibernetice, prin realizarea periodică de campanii de informare, conştientizare şi igienă cibernetică la nivel organizaţional.

***(3) Măsurile reactive** sunt destinate reducerii efectelor atacurilor cibernetice şi includ:*

a) punerea în aplicare a planurilor de răspuns la incidente şi de contingenţă în domeniul securităţii cibernetice;

b) utilizarea rezervei de resurse şi de capabilităţi de securitate cibernetică;

c) restabilirea funcţionalităţii reţelelor şi sistemelor informatice din cadrul instituţiilor afectate;

d) diseminarea informaţiilor despre evenimentele cibernetice prin alerte în mediul interinstituţional pentru evaluarea riscului şi diminuarea posibilităţilor de exploatare a vulnerabilităţilor;

e) descurajarea prin atribuirea publică a autorilor atacurilor cibernetice, conform atribuţiilor legale";

- **art. 29** „***(1) Persoanele prevăzute la art.3 au obligaţia să elaboreze planuri proprii de acţiune pentru fiecare tip de alertă cibernetică, potrivit metodologiei prevăzută la art. 28 alin. (l).*** *(2) La declararea stărilor de alertă cibernetică, persoanele prevăzute la art. 3 pun în aplicare măsurile din planurile prevăzute la alin. (l)*";

- **art. 37** „***Persoanele prevăzute la art. 3 au obligaţia de a asigura, pentru personalul propriu, formarea profesională, educaţia şi instruirea în domeniul securităţii şi apărării cibernetice prin cursuri, exerciţii, conferinţe, seminarii, precum şi alte tipuri de activităţi***".

Aşadar, în sarcina destinatarilor noii legi, astfel cum sunt indicaţi la art. 3 din Lege, printre obligaţiile impuse se află **luarea de măsuri proactive şi reactive pentru asigurarea rezilienţei în spaţiul cibernetic** (cum ar fi: constituirea şi antrenarea echipelor de răspuns la incidente de securitate cibernetică; asigurarea de resurse umane specializate pentru dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri şi măsuri de control tehnic privind apărarea şi securitatea cibernetică ş.a.), dar şi **obligaţia de a asigura, pentru personalul propriu, formarea profesională, educaţia şi instruirea în domeniul securităţii şi apărării cibernetice prin cursuri, exerciţii, conferinţe, seminarii, precum şi alte tipuri de activităţi**.

Pentru corectitudinea reglementării, precizăm că, în domeniul managementului incidentelor de securitate cibernetică, noua lege prevede ca A.N.C.O.M., M.Ap.N., M.A.I., M.A.E., S.R.I., S.I.E., S.T.S., S.P.P. şi O.R.N.I.S.S. să acorde sprijin, la cerere, proprietarilor, administratorilor, posesorilor şi/sau utilizatorilor de reţele şi sisteme informatice aflate în domeniul lor de competenţă, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgenţă pentru remedierea efectelor incidentelor de securitate cibernetică.

În acest context, **toate obligaţiile ce revin persoanelor prevăzute la art. 3 alin. (1) lit. c),** în special pentru persoane fizice şi juridice care furnizează servicii publice ori de interes public, care după cum am arătat poate fi şi un agent economic de drept privat, **impuse de noua lege, nu doar că sunt în**

sarcina lor exclusivă, dar îndeplinirea acestora devine extrem de oneroasă, mai ales că pentru implementarea tuturor măsurilor dispuse prin lege nu este prevăzută acordarea vreunui sprijin financiar din partea statului.

Totodată, limitarea exercițiului unor drepturi ale persoanelor fizice și juridice vizate de actul normativ criticat în considerarea unor drepturi colective și interese publice, ce vizează siguranța națională, rupe justul echilibru care ar trebui să existe între interesele și drepturile individuale, pe de o parte, și cele ale societății, pe de altă parte, legea criticată nereglementând garanții suficiente care să permită asigurarea unei protecții eficiente față de riscurile de abuz.

Or, în condițiile în care măsurile adoptate prin textul de lege criticat nu au un caracter clar, precis și previzibil, iar ingerința statului în exercitarea activității persoanelor fizice și juridice prevăzute în legea criticată, nu este formulată clar, riguros și exhaustiv, caracterul strict necesar într-o societate democratică nu este pe deplin justificat, iar proporționalitatea măsurii nu este asigurată prin reglementarea unor garanții corespunzătoare, fapt pentru care apreciem că se încalcă prevederile **art. 1 alin. (5) din Constituție**.

2. Prevederile art. 50 lit. p) din Legea privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (PL-x nr.773/2022, L828/2022) contravin art. 1 alin. (5) din Constitutia României pentru următoarele considerații

Dispozițiile **art. 50** prevăd că: „*La articolul 3 din Legea nr. 51/1991 privind securitatea națională a României, republicată în Monitorul Oficial al României, Partea I, nr. 190 din 18 martie 2014, cu modificările și completările ulterioare, după litera m) se introduc trei noi litere, literele n) – p), cu 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****»*”.

Astfel, examinând prevederile art. 50 lit. p) din actul normativ criticat, se observă că legiuitorul extinde domeniile de securitate națională, inclusiv pentru aspecte care exced scopului legii de securitate cibernetică.

Mai mult, prin această reglementare se are în vedere, în fapt, modificarea Legii nr. 51/1991 privind securitatea națională a României în sensul extinderii atribuțiilor Serviciului Român de Informații, care, în vederea asigurării securității naționale va realiza acțiuni specifice acestui serviciu și în ceea ce privește *acțiunile 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*”, fără însă ca legiuitorul să definească sau să identifice ce sunt sau cum se pot identifica ***campaniile de propagandă sau dezinformare, de natură a afecta ordinea constituțională***, lăsând la latitudinea Guvernului prin acte infralegale sau, după caz, la latitudinea Serviciului Român de Informații să aprecieze care sunt acestea.

Într-o situație pe care o apreciem similară celei învederate în acest caz, Curtea Constituțională, prin **Decizia nr. 379/2019**, a considerat că, în ceea ce privește „*aceste aspecte și caracterul intruziv al activităților specifice culegerii de informații care presupun restrângerea exercițiului unor drepturi sau al unor libertăți fundamentale ale omului, se constată că este obligatoriu ca acestea să se realizeze într-un cadru normativ clar, precis și previzibil, atât pentru persoana supusă acestei măsuri, cât și pentru organele de urmărire penală și pentru instanțele de judecată. În caz contrar, s-ar ajunge la posibilitatea încălcării într-un mod aleatoriu/abuziv a drepturilor fundamentale, esențiale într-un stat de drept, [...]. Este îndeobște admis că*

drepturile [...] nu sunt absolute, însă ***limitarea lor trebuie să se facă respectând dispoziţiile art. 1 alin. (5) din Legea fundamentală, iar gradul de precizie a termenilor şi a noţiunilor folosite trebuie să fie unul ridicat, dată fiind natura măsurilor intruzive reglementate*** (a se vedea în acest sens şi **Deciziile Curții Constituționale nr. 91/2018 și nr.802/2018**).

Ca atare, în măsura în care nu este definită, în mod clar şi riguros, sintagma „*campanii de propagandă sau dezinformare*" considerăm că din modul vag şi general de reglementare al sintagmei analizate rezultă că se poate circumscrie unei ameninţări la adresa securităţii naţionale orice faptă/acţiune cu sau fără conotaţie de campanie de propagandă sau dezinformare. Cu alte cuvinte, sfera de aplicare a dispoziţiei criticate este atât de largă, încât faţă de orice persoană se poate reţine exercitarea unei acţiuni care constituie ameninţare la adresa securităţii naţionale.

În consecinţă, pentru aceste considerente Curtea Constituţională a apreciat că, în acest sens „*caracterul deschis al sintagmei criticate determină posibilitatea introducerii sau excluderii de elemente în/din această categorie, acţiune care se răsfrânge şi asupra limitelor de aplicare a dispoziţiei de lege criticate. În acest mod, limitele de aplicare a dispoziţiei de lege criticate nu mai pot fi cunoscute de destinatarii normei, care, astfel, nu îşi pot corecta conduita şi nu pot fi capabili să prevadă, într-o măsură rezonabilă, consecinţele care pot apărea dintr-un act determinat*", motiv pentru care a declarat ca fiind neconstituţionale prevederile criticate în acest caz (a se vedea **Decizia Curții Constituționale nr. 91/2018**).

Aşadar, gradul de precizie al termenilor şi noţiunilor folosite trebuie să fie unul ridicat, dată fiind natura măsurilor intruzive reglementate. De asemenea, dispoziţiile în cauză trebuie să se realizeze într-un cadru normativ clar, precis şi previzibil, reglementat la nivel primar, de Parlament, prin lege, în caz contrar, s-ar ajunge la posibilitatea încălcării în mod abuziv a drepturilor fundamentale ale cetăţenilor.

Prin urmare, considerăm că modul de redactare al art. 50 lit. p) din actul normativ criticat este lipsit de claritate, precizie şi previzibilitate şi este contrar dispoziţiilor art. 1 alin. (5) din Constituţie.

3. Prevederile art. 21 şi art. 22 din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative (PL-x nr. 773/2022, L828/2022) contravin art. 11 şi art. 148 alin. (4) din Constituţia României din perspectiva următoarelor considerente

Prin dispoziţiile **art. 21 şi art. 22 din legea criticată,** legiuitorul primar vine în completarea atât a destinatarilor vizaţi de Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, modificată, privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, cât şi în privinţa sarcinilor impuse acestora[1], creând astfel un paralelism legislativ, care, pe alocuri, cuprinde reglementări chiar contrare, ceea ce generează şi mai multă incoerenţă legislativă.

Astfel, **art. 21** prevede că: „*(1)* ***Persoanele prevăzute la art. 3 alin. (1) lit. b) şi lit. c), au obligaţia de a notifica incidentele de securitate cibernetică prin intermediul PNRISC, de îndată dar nu mai târziu de 48 de ore de la constatarea incidentului****. (2) Dacă incidentele de securitate cibernetică nu pot fi comunicate complet în termenul prevăzut la alin. (1), acestea se transmit în cel mult 5 zile calendaristice de la notificarea iniţială, informaţiile putând fi completate şi ulterior cu cele care reies din investigaţiile realizate pe baza evenimentului. (3) Fără a aduce atingere normelor aplicabile în materie de raportare, confidenţialitate, secret*

[1] A se vedea art. 22 „*Incidentele de securitate cibernetică sunt notificate în PNRISC în condiţiile Capitolului IV, Secţiunea a 2-a din Legea nr. 362/2018, cu modificările şi completările ulterioare*".

profesional și protecția informațiilor clasificate, autoritățile care au în responsabilitate rețele și sisteme informatice prevăzute la art. 3 alin. (1) lit. a), notifică incidentele de securitate cibernetică prin intermediul PNRISC, iar **art. 22** menționează că: „***Incidentele de securitate cibernetică sunt notificate în PNRISC în condițiile capitolului IV, secțiunea a 2-a din Legea nr. 362/2018, cu modificările și completările ulterioare***".

În fapt, **Legea nr. 362/2018, modificată,** stabilește cadrul juridic și instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu, fiind o transpunere a **Directivei (UE) 2016/1148.**

În acest sens, potrivit **pct. 53 din 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, „***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 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***".

Din analiza actului normativ criticat se observă că, prin noile dispoziții, legiuitorul primar impune anumite obligații persoanelor fizice și juridice, care sunt disproporționate și contrare **pct. 53 din 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, directivă transpusă la nivel național prin Legea nr. 362/2018.

În contextul în care directiva precitată a fost deja transpusă în legislația națională, prin Legea nr. 362/2018, modificată, orice încercare de extindere a ariei destinatarilor prevăzuți în directivă și, respectiv, prin Legea nr. 362/2018, dar și a sarcinilor impuse acestora apare în afara coordonatelor constituționale, motiv pentru care, în opinia noastră, legea dedusă controlului de constituționalitate aduce atingere angajamentelor internaționale în materie de securitate cibernetică asumate și transpuse deja în legislația națională de România, **încălcându-se astfel dispozițiile art. 11 alin. (1) și ale art. 148 alin. (4) din Constituție.**

Astfel, conform art. 148 alin. (4) din Constituție, Parlamentul, Președintele României, Guvernul și autoritatea judecătorească garantează aducerea la îndeplinire a obligațiilor rezultate din actul aderării la Uniunea Europeană și din celelalte reglementări comunitare cu caracter obligatoriu.

Din examinarea art. 21 și art. 22 din Legea criticată, indicate mai sus în forma adoptată, se observă că dispozițiile acestora completează Legea nr. 362/2018, modificată, contrar însă prevederilor Directivei (UE) 2016/1148. Considerăm, așadar, că aceste prevederi încalcă acquis-ului comunitar [reglementat prin art. 16 alin. (11) și a considerentului nr.53 din directiva NIS 4], care impune că, reglementările naționale adoptate în acest sens trebuie să evite impunerea unei sarcini financiare și administrative disproporționate asupra operatorilor de servicii esențiale și a furnizorilor de servicii digitale. În acest caz, cerințele necesare a fi respectate trebuie să fie în acord cu cele prevăzute de Directiva (UE) 2016/1148. În cazul furnizorilor de servicii digitale, aceste cerințe nu trebuie să se aplice microîntreprinderilor și întreprinderilor mici (directiva NIS 4), ci doar la întreprinderile medii și mari (directiva NIS2).

Cu privire la aceste aspecte, în jurisprudența sa, Curtea Constituțională a reținut că **legiuitorul național este obligat să efectueze operațiunea transpunerii unei directive în mod corect, în acord cu scopul și spiritul directivei europene transpuse**, care, în cazul de față, vizează strict domeniul rețelelor și serviciilor de comunicații electronice. Or, dispozițiile criticate cuprind reglementări care excedează cadrului de reglementare al Directivei (UE) 2016/1148,

contravenind principiului loialității constituționale care presupune ca Parlamentul să legifereze în acord cu **art. 148 alin. (4) din Constituție**.

În altă ordine de idei, **ca urmare a aderării României la Uniunea Europeană, în temeiul art. 148 alin. (2) și (4) din Constituție, prevederile reglementărilor europene cu caracter obligatoriu au prioritate față de dispozițiile contrare din legile interne**.

Prin urmare, **actul normativ criticat este în contradicție cu dreptul Uniunii Europene în materia comunicațiilor electronice.**

Totodată, Curtea Constituțională a României a reținut că **art. 20 din Constituție** cuprinde reguli care privesc, de fapt, transpunerea în practică a dispozițiilor constituționale privind drepturile, libertățile și îndatoririle fundamentale ale cetățenilor și care trebuie interpretate prin coroborare cu dispozițiile art. 11 din Constituție, ce consacră corelația dintre dreptul internațional și dreptul intern (**Decizia Curții Constituționale nr. 103/2001**).

În concluzie, apreciem că prevederile art. 21 și art. 22 din *Legea privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative* aduc atingere prevederilor **art. 11 și art. 148 din Constituția României**.

Având în vedere competența sa generală în privința protecției drepturilor și libertăților omului, Avocatul Poporului apreciază că **argumentele de neconstituționalitate reținute justifică pronunțarea de Curtea Constituțională a unei soluții de admitere a prezentei sesizări de neconstituționalitate.**

AVOCATUL POPORULUI,

RENATE WEBER