

L 828/2022

Biroul permanent al Senatului

828 / 28 dec. 2022



R O M Â N I A
CURTEA CONSTITUȚIONALĂ
CABINETUL PREȘEDINTELUI

Palatul Parlamentului

Calea 13 Septembrie nr.2, Intrarea B1, Sectorul 5, 050725, București, România

Telefon: (+40-21) 313.25.31; Fax: (+40-21) 312.54.80

Internet: <http://www.ccr.ro> E-mail: pres@ccr.ro

Dosar nr.2948A/2022

CURTEA CONSTITUȚIONALĂ
REGISTRATURĂ JURISDICȚIONALĂ
NR. **9143** / **27 DEC 2022**

SENATUL ROMÂNIEI
Nr. // **3259** / **27.12.2022**

Doamnei
Alina-Ștefania GORGHIU
Președintele Senatului

În conformitate cu dispozițiile art.16 alin.(2) din Legea nr.47/1992 privind organizarea și funcționarea Curții Constituționale, vă trimitem, alăturat, în copie, sesizarea formulată de Avocatul Poporului, referitoare la neconstituționalitatea Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative.

Vă adresăm rugămintea de a ne comunica punctul dumneavoastră de vedere până la data de 3 februarie 2023 (inclusiv în format electronic, la adresa de e-mail ccr-pdv@ccr.ro), ținând seama de faptul că dezbaterile Curții Constituționale vor avea loc la data de 15 februarie 2023.

Vă asigurăm, doamnă Președinte, de deplina noastră considerație.

Președinte,
ROMANIA
Mărioara ENACHE



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

CURTEA CONSTITUȚIONALĂ

Dosar nr. 294PA1 2022

AVOCATUL POPORULUI

REGISTRATURĂ GENERALĂ

IEȘIRE NR. 32636, 27. DEC. 2022

Domnului Marian Enache,

Președintele Curții Constituționale,

CURTEA CONSTITUȚIONALĂ

REGISTRATURĂ JURISDIȚIONALĂ

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





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 Constituția 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. Oficiul 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. (1) 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 concurează 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 autorităților în domeniul indicat și ținând cont și de scopul legitim urmărit, pentru a oferi o protecție suficientă și adecvată împotriva arbitrarului.

În același sens, Curtea Europeană a Drepturilor Omului a statuat că legea trebuie, într-adevăr, să fie accesibilă justițiabilului și previzibilă în ceea ce privește efectele sale. Pentru ca legea să satisfacă cerința de previzibilitate, ea 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 arbitrarului.

În plus, nu poate fi considerată „lege” decât o normă enunțată cu suficientă precizie, pentru a permite cetățeanului să își adapteze conduita în funcție de aceasta, apelând la nevoie la consiliere de specialitate în materie, el trebuie să fie capabil să prevadă, într-o măsură rezonabilă, față de circumstanțele speței, consecințele care ar putea rezulta dintr-o anumită faptă (a se vedea Hotărârea din 4 mai 2000, pronunțată în Cauza Rotaru împotriva României, paragraful 52, și Hotărârea din 25 ianuarie 2007, pronunțată 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 și 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 și 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. (1) lit. b) și 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”;

- **art. 24**

„(1) Asigurarea rezilienței în spațiul cibernetic se realizează prin implementarea de măsuri proactive și reactive de către instituțiile și persoanele prevăzute la **art. 3**.

(2) Măsurile proactive sunt destinate prevenirii incidentelor de securitate cibernetică și descurajării autorilor atacurilor din spațiul cibernetic și includ:

a) constituirea și 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 și măsuri de control tehnic privind apărarea și securitatea cibernetică;

c) constituirea și operarea Centrelor Operaționale de Securitate;

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

e) dezvoltarea unor capacități proactive, care să permită cunoașterea anticipativă a amenințărilor din spațiul cibernetic;

f) finanțarea pentru dezvoltarea capacităților de securitate și apărare cibernetică, inclusiv din perspectiva cercetării, dezvoltării, inovării și digitalizării în domeniu și asimilării tehnologiilor emergente;

g) cooperarea și schimbul de informații între autoritățile competente și sectorul privat pentru identificarea amenințărilor cibernetice;

h) identificarea serviciilor, rețelelor și sistemelor informatice, conform competențelor fiecărei instituții responsabile de administrare și asigurarea managementului acestora;

i) implementarea de soluții de securitate cibernetică, care să crească capacitatea de detecție și capabilitățile de prevenție la atacuri cibernetice;

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

k) demonstrarea nivelului de maturitate atins de capabilitățile de securitate cibernetică în cadrul exercițiilor organizate la nivel național sau internațional;

l) instruirea personalului din cadrul persoanelor prevăzute la art. 3 în domeniul securității cibernetice, prin realizarea periodică de campanii de informare, conștientizare și igienă cibernetică la nivel organizațional.

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

a) punerea în aplicare a planurilor de răspuns la incidente și de contingență în domeniul securității cibernetice;

b) utilizarea rezervei de resurse și de capabilități de securitate cibernetică;

c) restabilirea funcționalității rețelelor și sistemelor informatice din cadrul instituțiilor afectate;

d) diseminarea informațiilor despre evenimentele cibernetice prin alerte în mediul interinstituțional pentru evaluarea riscului și diminuarea posibilităților de exploatare a vulnerabilităților;

e) descurajarea prin atribuirea publică a autorilor atacurilor cibernetice, conform atribuțiilor legale”;

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

- **art. 37** „**Persoanele prevăzute la art. 3 au obligația de a asigura, pentru personalul propriu, formarea profesională, educația și instruirea în domeniul securității și apărării cibernetice prin cursuri, exerciții, conferințe, seminarii, precum și alte tipuri de activități”.**

Așadar, în sarcina destinatarilor noii legi, astfel cum sunt indicați la art. 3 din Lege, printre obligațiile impuse se află luarea de măsuri proactive și reactive pentru asigurarea rezilienței în spațiul cibernetic (cum ar fi: constituirea și 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 și măsuri de control tehnic privind apărarea și securitatea cibernetică ș.a.), dar și obligația de a asigura, pentru personalul propriu, formarea profesională, educația și instruirea în domeniul securității și apărării cibernetice prin cursuri, exerciții, conferințe, seminarii, precum și alte tipuri de activități.

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. și O.R.N.I.S.S. să acorde sprijin, la cerere, proprietarilor, administratorilor, posesorilor și/sau utilizatorilor de rețele și sisteme informatice aflate în domeniul lor de competență, activitate sau responsabilitate pentru adoptarea de măsuri reactive de primă urgență pentru remedierea efectelor incidentelor de securitate cibernetică.

În acest context, toate obligațiile ce revin persoanelor prevăzute la art. 3 alin. (1) lit. c), în special pentru persoane fizice și juridice care furnizează servicii publice ori de interes public, care după cum am arătat poate fi și 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 Constituția 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 dispozițiile art. 1 alin. (5) din Legea fundamentală, iar gradul de precizie a termenilor și a noțiunilor folosite trebuie să fie unul ridicat, dată fiind natura măsurilor intruzive reglementate (a se vedea în acest sens și Deciziile Curții Constituționale nr. 91/2018 și nr.802/2018).

Ca atare, în măsura în care nu este definită, în mod clar și riguros, sintagma „campanii de propagandă sau dezinformare” considerăm că din modul vag și general de reglementare al sintagmei analizate rezultă că se poate circumscrie unei amenințări la adresa securității naționale orice faptă/acțiune cu sau fără conotație de campanie de propagandă sau dezinformare. 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.

În consecință, pentru aceste considerente Curtea Constituțională a apreciat că, în acest sens „*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 destinatarul 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*”, motiv pentru care a declarat ca fiind neconstituționale prevederile criticate în acest caz (a se vedea **Decizia Curții Constituționale nr. 91/2018**).

Așadar, gradul de precizie al termenilor și noțiunilor folosite trebuie să fie unul ridicat, dată fiind natura măsurilor intruzive reglementate. De asemenea, dispozițiile în cauză trebuie să se realizeze într-un cadru normativ clar, precis și 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 cetățenilor.

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

3. Prevederile art. 21 și art. 22 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. 11 și art. 148 alin. (4) din Constituția României din perspectiva următoarelor considerente

Prin dispozițiile art. 21 și art. 22 din legea criticată, legiuitorul primar vine în completarea atât a destinatarilor vizați de Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, modificată, privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cât și în privința sarcinilor impuse acestora¹, creând astfel un paralelism legislativ, care, pe alocuri, cuprinde reglementări chiar contrare, ceea ce generează și mai multă incoerență legislativă.

Astfel, art. 21 prevede că: „(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. (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 inițială, informațiile putând fi completate și ulterior cu cele care reies din investigațiile realizate pe baza evenimentului. (3) Fără a aduce atingere normelor aplicabile în materie de raportare, confidențialitate, secret*

¹ A se vedea art. 22 „*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*”.

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, [REDACTED]



RENA TE WEBER



R O M Â N I A
CURTEA CONSTITUȚIONALĂ
CABINETUL PREȘEDINTELUI

SENATUL ROMÂNIEI
Nr. 325 / 22.12.2022

Palatul Parlamentului

Calea 13 Septembrie nr.2, Intrarea B1, Sectorul 5, 050725, București, România

Telefon: (+40-21) 313.25.31; Fax: (+40-21) 312.54.80

Internet: <http://www.ccr.ro> E-mail: pres@ccr.ro

Dosar nr.2926A/2022

Biroul permanent al Senatului

828 / 22.12.2022

CURTEA CONSTITUȚIONALĂ
REGISTRATURĂ JURISDICȚIONALĂ

NR. 9099 / 22 DEC 2022

Doamnei

ALINA-ȘTEFANIA GORGHIU

PREȘEDINTELE SENATULUI

1528/2022
În conformitate cu dispozițiile art.16 alin.(2) din Legea nr.47/1992 privind organizarea și funcționarea Curții Constituționale, vă comunicăm, alăturat, în copie, sesizarea formulată de deputați aparținând Grupului parlamentar al Uniunii Salvați România și de deputați neafiliați, referitoare la Legea privind securitatea și apărarea cibernetică precum și pentru modificarea și completarea unor acte normative (PL-x nr.773/2022).

Vă adresăm rugămintea de a ne comunica punctul dumneavoastră de vedere până la data de 03 februarie 2023 (inclusiv în format electronic, la adresa de e-mail ccr-pdv@ccr.ro), ținând seama de faptul că dezbaterile Curții Constituționale vor avea loc la data de 15 februarie 2023.

Vă asigurăm, doamnă Președinte, de deplina noastră considerație.

ROMÂNIA
PREȘEDINTE

MARIAN ENACHE

CURTEA CONSTITUȚIONALĂ

Dosar nr. 7926A/2022



ROMANIA

CURTEA CONSTITUȚIONALĂ
REGISTRATURĂ JURISDIȚIONALĂ

NR. 9054 / 22 DEC 2022

Parlamentul României
Camera Deputaților
Secretar general

București,
Nr. 2/11596/22.12.2022

Domnului

Marian ENACHE
Președintele Curții Constituționale

Stimate domnule Președinte,

În temeiul dispozițiilor art.27 alin.(1) din Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale, republicată, vă transmitem alăturat, sesizarea formulată de deputați aparținând Grupului parlamentar al Uniunii Salvați România și de deputați neafiliați, referitoare la Legea privind securitatea și apărare cibernetică precum și pentru modificare și completarea unor acte normative (Plx.773/2022).

Cu deosebită considerație,

SECRETAR GENERAL

SILVIA -CLAUDIA MIHALCEA



PARLAMENTUL ROMÂNIEI
GRUPUL PARLAMENTAR USR

INTRĂRE/IEȘIRE Nr. 33-16/989
Ziua 22 Luna 12 Anul 2022



ROMANIA

PARLAMENTUL ROMÂNIEI
CAMERA DEPUTAȚILOR
SECRETAR GENERAL
Nr. 2/11596
2022 Luna 12 Ziua 22

Parlamentul României Camera Deputaților Grupul parlamentar USR

Către: SECRETARIATUL GENERAL AL CAMEREI DEPUTAȚILOR
Doamnei Silvia-Claudia MIHALCEA

Doamnă Secretar General,

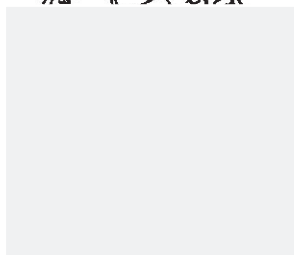
În temeiul art. 146 lit. a) din Constituția României, republicată, art. 136 alin. (3) din Regulamentul Camerei Deputaților, precum și art. 15 alin. (1) și (2) din Legea nr. 47/1992 privind organizarea și funcționarea Curții Constituționale a României, republicată, cu modificările și completările ulterioare, vă depunem alăturat obiecția de neconstituționalitate a *Legii privind securitatea și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (Pl-x nr. 773/2022)*, solicitându-vă să o înaintați Curții Constituționale a României, în ziua depunerii.

Cu stimă,

În numele semnatarilor,

Lider Grup USR

Liviu-Ionuț MOȘTEANU



Grup Parlamentar USR

Telefon: 021.414.1058, 021.414.1059; Fax: 021.414.1062; e-mail: usrplus@cdep.ro

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 și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative***
(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;**
- II. TEMEIUL CONSTITUȚIONAL;**
- III. MOTIVE DE NECONSTITUȚIONALITATE;**
- IV. CONCLUZII.**

I. SITUAȚIA DE FAPT

Legea care face obiectul prezentei obiecții a fost inițiată în anul 2022, sub denumirea „*Proiect de Lege privind securitatea și apărarea cibernetică a României precum și pentru modificarea și 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 și social, în care demnitatea omului, drepturile și libertățile cetățenilor, libera dezvoltare a personalității umane, dreptatea și pluralismul politic reprezintă valori supreme, în spiritul tradițiilor democratice ale poporului român și idealurilor Revoluției din decembrie 1989, și sunt garantate.

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

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

Articolul 26 Viața intimă, familială și privată

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

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

Articolul 30 Libertatea de exprimare

(1) *Libertatea de exprimare a gândurilor, a opiniilor sau a credințelor și libertatea creațiilor 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 și libertatea de a înființa publicații.*

(4) *Nici o publicație nu poate fi suprimată.*

(5) *Legea poate impune mijloacelor de comunicare în masă obligația de a face publică sursa finanțării.*

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

(7) *Sunt interzise de lege defăimarea țării și a națiunii, îndemnul la război de agresiune, la ură națională, rasială, de clasă sau religioasă, incitarea la discriminare, la separatism teritorial sau la violență publică, precum și manifestările obscene, contrare bunelor moravuri.*

(8) *Răspunderea civilă pentru informația sau pentru creația adusă la cunoștință publică revine editorului sau realizatorului, autorului, organizatorului manifestării artistice, proprietarului mijlocului de multiplicare, al postului de radio sau de televiziune, în condițiile legii. Delictele de presă se stabilesc prin lege.*

Articolul 147 Deciziile Curții Constituționale

(1) *Dispozițiile din legile și ordonanțele în vigoare, precum și cele din regulamente, constatate ca fiind neconstituționale, își încetează efectele juridice la 45 de zile de la publicarea deciziei Curții Constituționale dacă, în acest interval, Parlamentul sau Guvernul, după caz, nu pun de acord prevederile neconstituționale cu dispozițiile Constituției. Pe durata acestui termen, dispozițiile constatate ca fiind neconstituționale sunt suspendate de drept.*

(2) *În cazurile de neconstituționalitate care privesc legile, înainte de promulgarea acestora, Parlamentul este obligat să reexamineze dispozițiile respective pentru punerea lor de acord cu decizia Curții Constituționale.*

(3) *În cazul în care constituționalitatea tratatului sau acordului internațional a fost constatată potrivit articolului 146 litera b), acesta nu poate face obiectul unei excepții de neconstituționalitate. Tratatul sau acordul internațional constat ca fiind neconstituțional nu poate fi ratificat.*

(4) *Deciziile Curții Constituționale se publică în Monitorul Oficial al României. De la data publicării, deciziile sunt general obligatorii și 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 și al exercitării în comun cu celelalte state membre a competențelor prevăzute în aceste tratate, se face prin lege adoptată în ședința comună a Camerei Deputaților și Senatului, cu o majoritate de două treimi din numărul deputaților și senatorilor.

(2) Ca urmare a aderării, prevederile tratatelor constitutive ale Uniunii Europene, precum și 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) și (2) se aplică, în mod corespunzător, și pentru aderarea la actele de revizuire a tratatelor constitutive ale Uniunii Europene.

(4) Parlamentul, Președintele României, Guvernul și autoritatea judecătorească garantează aducerea la îndeplinire a obligațiilor rezultate din actul aderării și 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 constituțională¹, 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 și sfera prea largă de persoane fizice și 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 în 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 serviciu 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 și 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 legii. 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 și 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

cauză și nu trebuie aplicat deținătorilor de Infrastructuri cibernetice cu importanță nesemnificativă din punctul de vedere al interesului general.

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 **la nivel național** 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.

III.2. Articolele 21-22 din legea adoptată încalcă dispozitiile art. 1 alin. (5), art. 26, art. 30 și art. 148 alin. (2) din Constituția României:

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 și 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 Constituție, potrivit căruia reglementarea europeană are prioritate față 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 NIS²:

„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.”

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.

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;

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 Institutile 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 sensibilitate 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 să 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 confidentiale 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 deservește 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 oricărui terț 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 destinatarul 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 și sistemele informatice în sistemul de protecție a securității naționale („sectorul” cibernetic al securității naționale), este **excesiv și dăunător pentru libertatea de exprimare și 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 să 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 știri, date sau informații false ori de documente falsificate, cunoscând caracterul fals al acestora, dacă prin aceasta se pune în pericol securitatea națională, se pedepsește 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 încălcă dispozițiile art. 1 alin. (5), în componenta sa referitoare la principiul securității juridice, previzibilității și clarității normelor, art. 26 și 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 rela 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 și apărarea cibernetică a României precum și pentru modificarea și completarea unor acte normative (PI-x nr. 773/2022).**

ANEXE

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

**TABEL SEMNĂTURI - Obiecția de neconstituționalitate a Legii privind
securitatea și apărarea cibernetică a României precum și pentru modificarea și
completarea unor acte normative
(Pl-x nr. 773/2022)**

Nr	Numele si Prenumele	partid	semnatura
1	Apostol Alin-Gabriel	USR	
2	Badea Mihai-Alexandru	USR	
3	Băltărețu Viorel	USR	
4	Barna Ilie Dan	USR	
5	Benga Tudor	Independent	
6	Berescu Monica-Elena	USR	
7	Blaga Daniel-Codruț	USR	
8	Botez Mihai-Cătălin	USR	
9	Bulai Iulian	USR	
10	Buzoianu Diana-Anda	USR	
11	Chichirău Cosette-Paula	USR	
12	Ciomei Radu Tudor	USR	
13	Cristian Brian	USR	
14	Dehelean Silviu	USR	
15	Drancă Andrei-Iulian	USR	
16	Drulă Cătălin	USR	
17	Fălcoi Nicu	USR	
18	Gheba Daniel-Sorin	USR	
19	Giurgiu Adrian	USR	
20	Hangan Pollyanna-Hanellore	USR	
21	Havârneanu Filip	USR	
22	Ilie Victor	USR	

**TABEL SEMNĂTURI - Obiecția de neconstituționalitate a Legii privind
securitatea și apărarea cibernetică a României precum și pentru modificarea și
completarea unor acte normative
(Pl-x nr. 773/2022)**

Nr	Numele si Prenumele	partid	semnatura
23	Ion Stelian-Cristian	USR	
24	Lazăr Ion-Marian	USR	
25	Lazăr Teodor	USR	
26	Lőrincz Ștefan-Iulian	USR	
27	Miftode Andrei Marius	USR	
28	Miruță Radu-Dinel	USR	
29	Molnar Radu-Iulian	USR	
30	Moșteanu Liviu-Ionuț	USR	
31	Murariu Oana	USR	
32	Năsui Claudiu-Iulius-Gavril	USR	
33	Neagu Denisa-Elena	USR	
34	Panait Radu	USR	
35	Popescu Mihai-Laurențiu	USR	
36	Pop Tudor Rareș	USR	
37	Prună Cristina-Mădălina	USR	
38	Rodeanu Bogdan-Ionel	USR	
39	Seidler Cristian-Gabriel	USR	
40	Stoica Diana	USR	
41	Terente Eugen	USR	
42	Todosiu Benjamin	USR	
43	Țoiu Oana-Silvia	USR	
44	Ungureanu Emanuel-Dumitru	USR	
45	Wiener Adrian	USR	

TABEL SEMNĂTURI - OBIECTA DE NECONFORMITATE A
 LEGII PRIVIND SECURITATEA ȘI APĂRAREA CIBERNETICĂ A
 ROMÂNIEI PRECUM ȘI PENTRU MODIFICAREA ȘI COMPLETAREA
 UNOR ALTE NORMATIVE CPL-X NR. 773/2022

Nr.	Nume și prenume	Deputați	Semnătura
1	Jordan Ionescu	NEAFILIAT	[Redacted]
2	GEORGE IONESCU	NEAFILIAT	
3	Antonel Ionescu	NEAFILIAT	
4	FLĂIȘU GABRIEL	NEAFILIAT	
5	ȘOVIȚĂ LA CĂTIN	NEAFILIAT	
6	CLAUDIU CHIRA	NEAFILIAT	
7	ALEXANDRU KOCSIS	NEAFILIAT	
8	MIȚEȘCU MARIAN	NEAFILIAT	
9	DANCA IONEL	NEAFILIAT	
10	RUCU DANIEL GHE	NEAFILIAT	
11	SFEȘTELEȘIU	NEAFILIAT	
12	VILCEA ALEXANDRU	NEAFILIAT	
13	BOLA BOGDAN	NEAFILIAT	