DECIZIA nr.70
din 28 februarie 2023

referitoare la obiecţiile de neconstituţionalitate a dispoziţiilor art.3 alin.(1) lit.c), art.21 alin.(1), art.22, art.25, art.41, art.48 și art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative

Nepublicată

Marian Enache	**- președinte**
Mihaela Ciochină	**- judecător**
Cristian Deliorga	**- judecător**
Dimitrie-Bogdan Licu	**- judecător**
Laura-Iuliana Scântei	**- judecător**
Gheorghe Stan	**- judecător**
Livia Doina Stanciu	**- judecător**
Elena-Simina Tănăsescu	**- judecător**
Varga Attila	**- judecător**
Cristina Teodora Pop	**- magistrat-asistent**

1. Pe rol se află soluţionarea obiecţiilor de neconstituţionalitate a dispoziţiilor Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, obiecții formulate de un număr de 57 de deputați, aparținând grupului parlamentar al USR și deputați neafiliați, și, respectiv, de Avocatul Poporului.

2. Obiecţiile de neconstituţionalitate au fost înregistrate la Curtea Constituțională sub nr.9054 din 22 decembrie 2022 și sub nr.9125 din 27 decembrie 2022 și constituie obiectul Dosarelor nr.2926 A/2022 și nr.2948 A/2022.

3. **În motivarea obiecțiilor de neconstituționalitate** referitoare la prevederile *Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative* sunt formulate critici de neconstituționalitate intrinsecă, după cum urmează:

4. Cu privire la dispozițiile **art.3 alin.(1) lit.c) din legea criticată,** se susține că acestea sunt lipsite de claritate, întrucât reglementează o sfera prea largă de persoane fizice și juridice cărora li se adresează soluția legislativă analizată, aspect care determină incidența textului criticat în cazul oricărui serviciu informatic care se bazează pe un sistem informatic; sunt date drept exemplu, *SaaS în cloud*, conturile de *Facebook, Instagram, Gmail* sau *Yahoo*, serviciile de acces la legislație online, serviciu de notificări al Parlamentului European, precum și serviciile online similare celor anterior menționate.

5. Se arată că prevederile art.3 alin.(1) lit.c) din legea ce formează obiectul controlului de constituționalitate nu identifică și nu definesc, în mod clar și previzibil, persoanele fizice și persoanele juridice care furnizează servicii publice sau 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. În acest sens, este invocată jurisprudența Curții Constituționale referitoare la calitatea legii, respectiv Decizia nr.26 din 18 ianuarie 2012, Decizia nr.473 2013, Decizia nr.139 din 21 noiembrie 2019 și Decizia nr.681 din 21 octombrie 2021, precum și dispozițiile art.36 alin.(1) din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, fiind subliniată existența obligației constituționale a Parlamentului de a adopta legi care să respecte standardele de claritate, precizie și previzibilitate specifice calității legii, astfel cum acestea rezultă din prevederile art.1 alin.(5) din Constituție.

6. Se susține că, în condițiile lipsei de claritate, precizie și previzibilitate a textului criticat, autoritatea executivă, respectiv Guvernul, își va exercita atribuția prevăzută la art.108 alin.(2) din Constituție, de adoptare a hotărârii pentru organizarea executării legii criticate, în mod defectuos; astfel, autorii criticii argumentează 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 clare a acestora, fapt ce poate determina o reglementare infralegală trunchiată, incompletă sau prea generală, dar în niciun caz exhaustivă. Se susține că hotărârile Guvernului se adoptă întotdeauna în baza legii, fiind *secundum legem* și urmărind organizarea executării și executarea în concret a legii, motiv pentru care se apreciază că este obligatoriu ca legea să realizeze, la nivel primar, un cadru normativ clar, precis și previzibil, atât pentru

persoanele fizice și juridice destinatare ale legii, cât și pentru instanțele judecătorești, întrucât un eventual control de legalitate realizat asupra unui act administrativ, cum este o hotărâre a Guvernului, trebuie să poată fi raportat la repere clare și previzibile; or, transferând Guvernului marja de apreciere a criteriilor în funcție de care sunt determinați destinatarii normei legale criticate, legiuitorul lasă cale liberă arbitrarului și abuzului de putere. Așadar, se susține că soluția legislativă prin care legiuitorul primar transferă în sarcina Guvernului reglementarea, prin hotărâre a Guvernului, inițiată de Ministerul Cercetării, Inovării și Digitalizării, a categoriilor de persoane prevăzute la art.3 alin.(1) lit.c) din legea analizată, hotărâre care va fi adoptată în cel mult 60 de zile de la data intrării în vigoare a legii criticate, este în dezacord cu dispozițiile Legii fundamentale, deoarece norma primară nu stabilește în mod clar și concret criteriile în limita cărora Guvernul, ca putere executivă, este abilitat să asigure punerea în executare a legii criticate. Se arată că lipsa de claritate, precizie și previzibilitate a noilor reglementări determină imposibilitatea identificării exacte a destinatarilor legii analizate și, în consecință, a obligațiilor ce le revin potrivit aceleiași legi, astfel încât aceștia să își poată adapta conduita la exigențele impuse prin dispozițiile sale. Or, pentru a fi înțeleasă și respectată de către destinatarii săi, legea analizată trebuie să îndeplinească cerințele de claritate, precizie și previzibilitate prevăzute la art.1 alin.(5) din Constituție, precum și la art.6, art.8 și art.23 din Legea nr.24/2000. Se face trimitere la jurisprudența Curții Constituționale, respectiv la Deciziile nr.189 din 2 martie 2006, nr.903 din 6 iulie 2010, nr.26 din 18 ianuarie 2012, nr.348 din 17 iunie 2014, nr.17 din 21 ianuarie 2015, nr.63 din 13 octombrie 2015 și nr.302 din 4 mai 2017, fiind invocată, totodată, jurisprudența Curții Europene a Drepturilor Omului, respectiv 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.

7. Se arată, de asemenea, că dispozițiile art.3 alin.(1) lit.c) din *Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative* contravin principiului securității juridice reglementat de aceeași normă constituțională prevăzută la art.1 alin.(5) din Legea fundamentală. Se face trimitere la jurisprudența Curții Constituționale potrivit căreia statul are obligația constituțională de a asigura atât o stabilitate firească a dreptului, cât și valorificarea, în condiții optime, a drepturilor și a libertăților fundamentale, fiind indicate Deciziile nr.51 din 25 ianuarie 2012, nr.90 din 7 februarie 2012, nr.454 din 4 iulie 2018, nr.836 din 13 decembrie 2018, nr.240 din 3 iunie 2020, nr.504 din 30 iunie 2020, Decizia nr.187 din 17 martie 2021, Decizia nr.478 din 8 iulie 2021 și nr.688 din 21 octombrie 2021. De asemenea, este invocat paragraful 69 din Decizia nr.17 din 21 ianuarie 2015.

8. Se susține, totodată, că actul normativ criticat impune persoanelor prevăzute la art.3 alin.(1) lit.c) o serie de sarcini oneroase, care vor avea asupra acestora, un impact economic semnificativ, întrucât vor fi obligate să suporte din bugetele proprii cheltuielile necesare îndeplinirii obligațiilor prevăzute în sarcina lor prin legea care face obiectul sesizărilor. Se face referire, cu titlu exemplificativ, la obligațiile reglementate la art.21 alin.(1), art.24, art.29 și art.37 din legea analizată, arătându-se că, printre obligațiile anterior referite, se numără și cea de luare a măsurilor proactive și reactive pentru asigurarea rezilienței în spațiul cibernetic (cu titlu de exemplu: constituirea și antrenarea echipelor de răspuns la incidente de securitate cibernetică; de asigurare a resurselor umane specializate pentru dezvoltarea de strategii, norme, politici, proceduri, analize de risc, planuri și măsuri de control tehnic privind apărarea și securitatea cibernetică etc.), 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. Se arată că aceste obligații sunt reglementate în sarcina exclusivă a persoanelor prevăzute la art.3 alin.(1) lit.c) din *Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*, îndeplinirea lor fiind extrem de oneroasă, iar pentru realizarea acestora, legea analizată nu prevede acordarea niciunui sprijin financiar de către stat. Se arată că limitarea exercițiului unor drepturi ale persoanelor fizice și juridice vizate de actul normativ criticat, în considerarea unor drepturi colective și a unor interese publice ce vizează siguranța națională, încalcă justul echilibru care trebuie să existe între asigurarea drepturilor și intereselor legitime individuale, pe de o parte, și asigurarea interesului public, al societății, pe de altă parte, legea criticată nereglementând garanții suficiente care să asigurare o protecție eficientă a drepturilor și a intereselor individuale față de riscul apariției arbitrariului și al abuzului de putere.

9. Sunt invocate dispozițiile Directivei (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 (Directiva NIS 1) și ale Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr.910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2), despre care se afirmă că exceptează întreprinderile mici și mijlocii de la obligațiile din domeniul securității informatice.

10. Autorii criticilor apreciază concluziv că măsurile adoptate prin textul de lege criticat nu au un caracter clar, precis și previzibil, că ingerința statului în exercitarea activității persoanelor fizice și juridice prevăzute în legea criticată nu are un caracter strict necesar într-o societate democratică, că această ingerință nu este pe deplin justificată și că legea analizată nu respectă principiul proporționalității, întrucât nu prevede garanții adecvate în raport cu obligațiile instituite, pentru toate aceste motive, textul criticat încălcând prevederile art.1 alin.(5) din Constituție.

11. Referitor la dispozițiile **art.21 alin.(1) și ale art.22 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative,** se susține că, prin normele anterior menționate, legiuitorul primar completează *sfera destinatarilor* vizați de Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice, precum și *sarcinile* impuse acestora, creând astfel, un paralelism legislativ, care cuprinde și reglementări contrare, aspect care generează incoerență legislativă. Se arată că Legea nr.362/2018 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 (Directiva NIS 1). În acest context, se apreciază că textele criticate extind obligațiile de raportare a incidentelor cibernetice 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 Uniunii Europene. Se susține că, pentru acest motiv, dispozițiile legale criticate încalcă punctul 53 din Preambulul Directivei (UE) 2016/1148 (Directiva NIS 1), potrivit căruia „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." Se arată, totodată, că Directiva (UE) 2022/2555 (Directiva NIS 2) limitează aplicarea normelor privind asigurarea securității cibernetice la anumite domenii și la întreprinderile medii și mari, fiind excluse întreprinderile mici și mijlocii, prin urmare ar trebui ca obligația de raportare a incidentelor de securitate cibernetică, reglementată la art.21 din legea criticată, să fie prevăzută doar pentru autoritățile/instituțiile din sectorul public, lăsând pentru entitățile din mediul privat doar facultatea (nu obligația) de a face sesizări către Platforma națională pentru raportarea incidentelor de securitate cibernetică (PNRISC). Astfel, se arată că „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."

12. Pentru aceste motive, se susține că prin legea analizată, legiuitorul primar impune persoanelor fizice și juridice, obligații disproporționate în raport cu scopul legii și contrare atât punctului 53 din Preambulul Directivei (UE) 2016/1148 (Directiva NIS 1), cât și dispozițiilor Legii nr.362/2018, motive pentru care actul normativ criticat este în contradicție cu dreptul Uniunii europene în materia comunicațiilor electronice și contravine dispozițiilor art.11 alin.(1) și art.148 alin.(2) și (4) din Constituție.

13. Cu privire la prevederile **art.25 din legea ce formează obiectul sesizărilor**, se susține că acestea reiau o normă din cuprinsul legii declarate neconstituționale în anul 2015 și că ele creează o obligație de delațiune în sarcina unei categorii de profesioniști care, în mod normal, ar avea obligații de confidențialitate față de proprii clienți. Se arată că aceste persoane sunt obligate ca, la orice solicitare a unei instituții dintre cele prevăzute la art.10 din legea analizată, să-și reclame/denunțe clienții, fără a exista un mandat judecătoresc și fără o autorizare expresă; mai exact, acestea sunt obligate să furnizeze informații despre starea securității unui client sau a unei întregi infrastructuri (care poate include informații personale și secrete ale mai multor clienți, indiferent dacă aceștia sunt sau nu direct afectați de o posibilă vulnerabilitate). Se arată că obligația astfel reglementată a fost prevăzută în legea cu același obiect, declarată neconstituțională prin Decizia nr.17 din 21 ianuarie 2015.

14. Referitor la dispozițiile **art.41 din legea supusă controlului de constituționalitate,** se susține că procesul de management al riscurilor de securitate cibernetică specifice lanțului de

aprovizionare presupune aspecte complexe de securitate cibernetică care trebuie să fie implementate doar de autoritățile publice și de firmele mari, conform *acquis*-ului comunitar existent, făcându-se trimitere, în acest sens, la dispozițiile Directivei (UE) 2016/1148 (Directive NIS 1) și ale Directivei (UE) 2022/2555 (Directiva NIS 2). Se arată, totodată, că extinderea sferei persoanelor cărora le sunt aplicabile dispozițiile directivelor anterior menționate generează o lipsă de previzibilitate a efectelor pe care legea le-ar putea produce.

15. Cu privire la prevederile **art.48 din legea analizată,** se susține că acestea reglementează două contravenții diferite, respectiv *omisiunea de „notificare"* a incidentului de securitate cibernetică și *omisiunea de „comunicare completă*" a incidentului de securitate cibernetică. Cu toate acestea, se arată că doar noțiunea de „*notificare*" este definită la art.22 din legea criticată, prin trimitere la Legea nr.362/2018, iar noțiunea de „comunicare completă" nu este definită legal, motiv pentru care destinatarul legii nu poate să prevadă dacă atunci când a raportat un incident, respectiva raportare a constituit o „notificare" sau o „comunicare completă".

16. Referitor la dispozițiile **art.50 și art.51 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative,** se susține că, prin acestea - respectiv prin textul propus pentru litera p) a art.3 din Legea nr.51/1991 privind securitatea națională a României - legiuitorul extinde domeniile de securitate națională dincolo de scopul legii reglementate. Se arată, de asemenea, că legea criticată nu definește noțiunile de „*campanii de propagandă sau dezinformare*", de „*reziliența statului*" și de „*riscurile și amenințările de tip hibrid*", sfera acestora de aplicare fiind lăsată la aprecierea Guvernului, care le poate defini prin acte infralegale sau, după caz, la aprecierea Serviciului Român de Informații care va decide, în fiecare caz în parte, care sunt faptele care aparțin sferei sintagmelor anterior menționate. Se susține că această manieră de reglementare este contrară paragrafului 83 din Decizia nr.91 din 28 februarie 2018, prin care Curtea Constituțională a reținut că din modul de reglementare a sintagmei „aduc atingere gravă drepturilor şi libertăţilor fundamentale ale cetăţenilor români" rezultă că se poate circumscrie unei ameninţări la adresa securităţii naţionale orice faptă/acţiune cu sau fără conotaţie penală care afectează un drept sau o libertate fundamentală. 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", precum și paragrafului 80 din Decizia nr.802 din 6 decembrie 2018, potrivit căruia caracterul deschis al sintagmei „altor interese ale ţării" 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. Este invocată, totodată, Decizia nr.379 din 28 mai 2019. Se mai susține că introducerea tuturor rețelelor și a sistemelor informatice în sistemul de protecție a securității naționale este excesiv și încalcă libertatea de exprimare și dreptul la viață intimă, familială și privată. Se arată, de asemenea, că anumiți termeni din cuprinsul legii criticate, precum cel de „*infrastructuri informatice și de comunicații de interes național*", sunt folosiți fără a rezulta cu claritate, din ansamblul reglementării, dacă se referă la terminologia definită în cuprinsul altor legi (spre exemplu, prin Legea nr.163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G), în timp ce alți termeni, din cuprinsul aceluiași act normativ, beneficiază de o definiție legală (cum este, spre exemplu, noțiunea de „*reziliența cibernetică*"), dar sunt folosiți în cu totul alt context (spre exemplu, termenul „*reziliență*" este utilizat în sintagma „*reziliența statului*").

17. În ceea ce privește norma propusă pentru lit.p) a art.3 din Legea nr.51/1991, se arată că aceasta permite calificarea ca infracțiune a faptelor de exprimare a unor opinii neobediente prin raportare la acțiunile statale (de exemplu, opinii referitoare la campania de vaccinare), a faptelor de adresare a unor întrebări incomode sau a celor de formulare a unor opinii contrare politicii oficiale a statului; drept urmare, calificarea ca amenințări la adresa securității naționale a unor poziții publice contrare politicii oficiale a statului va face ca autorii acestora să devină subiecți activi ai infracțiunii prevăzute la art.404 din Codul penal cu denumirea marginală „Comunicarea de informații false", normă de incriminare potrivit căreia: „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."

18. În conformitate cu dispozițiile art.16 alin.(2) din Legea nr.47/1992 privind organizarea şi funcţionarea Curţii Constituţionale, sesizarea a fost comunicată **preşedinţilor celor două Camere ale Parlamentului, precum şi Guvernului, pentru a comunica punctele lor de vedere**.

19. **Președintele Camerei Deputaților** a trimis punctele sale de vedere, prin care apreciază că sesizările de neconstituționalitate sunt **neîntemeiate**, pentru următoarele considerente:

20. Cu privire la criticile de neconstituționalitate referitoare la lipsa de claritate a dispozițiilor art.3 alin.(1) lit.c) și ale art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, în ceea ce privește prevederile art.3 alin.(1) lit.c) din legea criticată, se arată că sintagma „rețelele și sistemele informatice ale persoanelor juridice care furnizează servicii publice ori de interes public”, utilizată în cuprinsul art.3 alin.(1) lit.c) din legea analizată are, conform art.2 lit.u) din aceeași lege, înțelesul definit la art.3 lit.l) din Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, beneficiind, astfel, de o definiție legală. Referitor la dispozițiile art.50 din legea care face obiectul controlului de constituționalitate, se susține că, potrivit Hotărârii Parlamentului României nr.22/2020 privind aprobarea Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024, obiectivele naționale de securitate vizează și asigurarea securității și protecției infrastructurilor de comunicații și tehnologia informațiilor cu valențe critice pentru securitatea națională, precum și cunoașterea, prevenirea și contracararea amenințărilor cibernetice derulate asupra acestora de către actori cu motivație strategică, de ideologie extremist-teroristă sau financiară, precum și că, în aceeași strategie, la pct.163, este indicat ca sursă de vulnerabilitate nivelul redus de securitate cibernetică a infrastructurilor de comunicații și tehnologia informației din domenii strategice (inclusiv ca efect al vulnerabilităților tehnologice și procedurale ale infrastructurilor deținute de operatorii de comunicații), care facilitează derularea de atacuri cibernetice de către actori statali sau non-statali. Se face trimitere, în acest sens, la considerentele Deciziei nr.455 din 4 iulie 2018. Sunt invocate, totodată, jurisprudența Curții Europene a Drepturilor Omului și jurisprudența Curții de Justiție a Comunităților Europene referitoare la standardele de calitate a legii, făcându-se trimitere la Hotărârile din 6 noiembrie 1980, 20 mai 1999, 4 mai 2000 și 24 august 2007 pronunțate de Curtea Europeană a Drepturilor Omului în cauzele *Sunday Times împotriva Regatului Unit al Marii Britanii și Irlandei de Nord*, *Rekvényi împotriva Ungariei, Rotaru împotriva României* și *Dragotoniu și Militaru-Pidhorni împotriva României*, precum și la Hotărârile din 22 octombrie 1987 și 14 iulie 1994 și pronunțate de Curtea de Justiție a Comunităților Europene în Cauzele *Foto-Frost împotriva Hauptzollamt Lübeck-Ost* și *Paola Faccini Dori împotriva Recreb Srl*. Se face trimitere, totodată, la Deciziile Curții Constituționale nr.717 din 29 octombrie 2015 şi nr.534 din 2 iulie 2020.

21. Pe de altă parte, se susține că, în condițiile în care prevederile art.61 alin.(1) din Constituție stabilesc că Parlamentul este organul reprezentativ suprem al poporului român şi unica autoritate legiuitoare a ţării, competenta de legiferare a acestuia cu privire la un anumit domeniu nu poate fi limitată dacă legea astfel adoptată respectă exigențele Legii fundamentale (se face trimitere la Decizia Curții Constituționale nr.157 din 2020). Prin urmare, opțiunea legiuitorului de a legifera în acest sens este un act de voință al Parlamentului, iar, în virtutea textului constituțional menționat, Parlamentul are competența de a institui, modifica şi abroga norme juridice de aplicare generală.

22. Pentru aceste motive, se susține că prevederile legale criticate întrunesc exigențele de precizie, previzibilitate şi claritate, cerințe la care Curtea Constituțională face referire în Decizia nr.17 din 21 ianuarie 2015.

23. Referitor la criticile de neconstituționalitate formulate cu privire la dispozițiile art.21 și art.22 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, se susține că, în procedura revizuirii Directivei (UE) 2016/1148 (Directiva NIS 1) s-a arătat că punerea acesteia în aplicare diferă foarte mult de la un stat membru la altul, inclusiv în ceea ce privește domeniul său de aplicare, a cărui delimitare a fost lăsată în mare măsură la latitudinea statelor membre și că directiva anterior menționată acorda statelor membre o marjă de apreciere foarte larga în ceea ce privește punerea în aplicare a obligațiilor de raportare privind securitatea și incidentele cibernetice, motiv pentru care aceste obligații au fost transpuse în moduri foarte diferite la nivelul fiecărui stat membru. Se susține, totodată, că, din considerentul 58 din Preambulul Directivei (UE) 2022/2555 (Directiva NIS 2), rezultă că procedurile reglementate prin actul european anterior menționat pot genera sarcini financiare și/sau administrative în vederea luării măsurilor adecvate pentru gestionarea riscurilor la care sunt expuse serviciile oferite pe piețele statelor membre, inclusiv în ceea ce privește clienții și beneficiarii terți și notificarea incidentelor de securitate cibernetică.

24. Se arată, totodată, că obligațiile în materie de securitate cibernetică prevăzute în Directiva (UE) 2022/2555 (Directiva NIS 2) trebuie considerate a fi complementare cerințelor impuse prestatorilor de servicii de încredere în temeiul Regulamentului (UE) nr.910/2014 și că acestora din urmă trebuie să li se impună să ia toate măsurile adecvate şi proporționale pentru a gestiona riscurile la care sunt expuse serviciile lor, inclusiv în ceea ce privește clienții şi beneficiarii terți şi să raporteze incidentele. Se susține că astfel de obligații în materie de securitate cibernetică şi de raportare ar trebui să vizeze, de asemenea, protecția fizică a serviciilor prestate.

25. Cu privire la criticile de neconstituționalitate referitoare la prevederile art.25 din legea criticată, se arată că - contrar susținerilor autorilor sesizării, conform cărora se creează o obligație de delațiune de la o categorie de profesioniști care, în mod normal, ar avea obligații de confidențialitate stricte pentru proprii clienți - potrivit alin.(2) al art.25 din legea analizată, datele şi informațiile prevăzute la alin.(1) al aceluiași articol nu vizează, prin scopul solicitării, date cu caracter personal şi date de conținut. Sunt invocate, în acest sens, dispozițiile art.45 şi ale art.47 alin.(2) din legea criticată.

26. Pentru aceleași motive, se susține că nu sunt întemeiate nici criticile de neconstituționalitate formulate cu privire la prevederile art.41, art.50 şi art.51 din legea analizată.

27. Referitor la dispozițiile art.48 din legea criticată, se susține că acestea sunt suficient de precis şi de clar redactate, pentru ca destinatarii normei să observe cu ușurință în ce condiții se notifică un incident de securitate cibernetică.

28. **Președintele Senatului și Guvernul** nu au comunicat punctele lor de vedere.

29. La dosarele cauzelor, **Directoratul Național de Securitate Cibernetică** a trimis un memoriu *amicus curiae*, prin care solicită respingerea obiecțiilor de neconstituționalitate.

30. Obiecţiile de neconstituţionalitate au figurat pe ordinea de zi din data de 15 februarie 2023, dată la care Curtea a conexat Dosarele nr.2926 A/2022 și nr.2948 A/2022 și, având în vedere complexitatea cauzei, în temeiul art.14 din Legea nr.47/1992 privind organizarea și funcționarea Curții Constituționale, a dispus amânarea dezbaterilor asupra cauzei pentru data de 28 februarie 2023.

CURTEA,

examinând obiecţiile de neconstituţionalitate, raportul judecătorului-raportor, punctele de vedere ale Preşedintelui Camerei Deputaţilor, dispoziţiile legale criticate, reține următoarele:

31. **Obiectul controlului de constituţionalitate**, astfel cum a fost formulat, îl constituie dispoziţiile *Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*. Analizând criticile de neconstituționalitate formulate de autorii obiecțiilor, Curtea reține însă că aceștia critică, în realitate, dispozițiile art.3 alin.(1) lit.c), art.21 alin.(1), art.22, art.25, art.41, art.48 și art.50 din *Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*, care au următorul cuprins:

- Art.3 alin.(1) lit.c): *„În domeniul securității cibernetice, prezenta lege se aplică următoarelor: […] 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).”***
- Art.21 alin.(1): *„Persoanele prevăzute la art.3 alin.(l) 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.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.”*
- Art.25: *„(1) Furnizorii de servicii tehnice de securitate cibernetică au obligația de a pune la dispoziția autorităților prevăzute la art.10, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, respectiv, în maximum 5 zile de la data primirii solicitării, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la, art.3 alin.(l), precum și interconectarea acestora cu terții și cu utilizatorii finali.*

(2) Datele și informațiile prevăzute la alin.(l) nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut.

(3) Datele și informațiile prevăzute la alin.(l) se transmit în scris, prin mijloace electronice sau prin orice altă modalitate stabilită de comun acord, în formatul și structura conforme raportării de incidente cibernetice în PNRISC, prevăzute la art.22.”

- Art.41: *„(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.(l).*

(2) Riscurile lanțului de aprovizionare includ cel puțin următoarele:

a) livrarea de soluții informatice false sau contrafăcute;

b) producție neautorizată;

c) manipulare frauduloasă a produselor și serviciilor software și hardware, respectiv a sistemelor și rețelelor informatice;

d) inserarea de componente software și hardware false sau contrafăcute;

e) servicii software și hardware periculoase pentru funcționare;

f) spionaj cibernetic;

g) compromiteri neintenționate ale sistemelor și rețelelor informatice;

h) practici deficitare de fabricație și dezvoltare de produse software și hardware."

- Art.48: *„(1) Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate infracțiuni potrivit legii:*

a) nerespectarea de către persoanele prevăzute la art.3 alin.(l) lit.b) și c) a obligației de notificare a incidentelor de securitate cibernetică, prin intermediul PNR1SC, în termenul prevăzut la art.21 alin.(l);

b) nerespectarea de către persoanele prevăzute la art.3 alin.(l) lit.b) și c) a obligației de comunicare completă a incidentelor de securitate cibernetică, prin intermediul PNRISC, în termenul și condițiile prevăzute la art.21 alin.(2) și art.22;

c) nerespectarea de către furnizorii de servicii de securitate cibernetică a obligației de a pune la dispoziția autorităților prevăzute la art.10 date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau sistem informatic al deținătorului sau al unor terți, în condițiile și la termenul prevăzut la art.25 alin.(l).

(2) Prin derogare de la dispozițiile art.8 alin.(2) lit.a) din Ordonanța Guvernului nr.2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr.180/2002, cu modificările și completările ulterioare, contravențiile prevăzute la alin.(l) se sancționează astfel:

a) cu amendă de la 5.000 lei la 50.000 lei, iar în cazul săvârșirii unei noi contravenții în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 200.000 lei;

b) pentru operatorii economici cu o cifră de afaceri netă de peste 1.000.000 lei, cu amendă în cuantum de până la 1% din cifra de afaceri netă, iar, în cazul săvârșirii unei noi contravenții, în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 3% din cifra de afaceri netă.

(3) Cifra de afaceri netă prevăzută la alin.(2) lit.b) este cea înregistrată de operatorul economic în ultimul exercițiu financiar.

(4) în vederea individualizării sancțiunii prevăzute la alin.(2), agentul de constatare și aplicare a contravenției ia în considerare gradul de pericol social concret al faptei și perioada de timp în care obligația legală a fost încălcată.

(5) Pentru persoanele fizice autorizate, întreprinderile individuale și întreprinderile familiale, cifrei de afaceri prevăzute la alin.(2) lit.b) îi corespunde totalitatea veniturilor realizate de respectivii operatori economici în exercițiul financiar anterior sancționării.

(6) Pentru persoanele juridice nou-înființate și pentru persoanele juridice care nu au înregistrat cifra de afaceri în exercițiul financiar anterior sancționării, amenda prevăzută la alin.(2) se stabilește în cuantum de minimum unu și maximum 25 de salarii minime brute pe economie.

(7) în măsura în care prezenta lege nu prevede altfel, contravențiilor prevăzute la alin.(l) li se aplică dispozițiile Ordonanței Guvernului nr.2/2001, aprobată cu modificări și completări prin Legea nr.180/2002, cu modificările și completările ulterioare."

- Art.50: *„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."

32. Dispoziţiile constituţionale pretins a fi încălcate sunt cele ale art.1 alin.(5) referitoare la calitatea legii, ale art.11 cu privire la dreptul internaţional şi dreptul intern, ale art.26 referitoare la viaţa intimă, familială şi privată, ale art.30 cu privire la libertatea de exprimare, ale art.147 alin.(4) referitoare la deciziile Curții Constituționale și ale art.148 alin.(2) și (4) referitoare la integrarea în Uniunea Europeană.

(1.) Admisibilitatea obiecţiilor de neconstituţionalitate

33. În prealabil examinării obiecţiilor de neconstituţionalitate, Curtea are obligaţia verificării condiţiilor de admisibilitate ale acestora, prin prisma titularului dreptului de sesizare, a termenului în care acesta este îndrituit să sesizeze instanţa constituţională, precum şi a obiectului controlului de constituţionalitate. Dacă primele două condiţii se referă la regularitatea sesizării instanţei constituţionale, din perspectiva legalei sale sesizări, cea de-a treia vizează stabilirea sferei sale de competenţă, astfel încât urmează să fie cercetate în ordinea antereferită, iar constatarea neîndeplinirii uneia dintre ele are efecte dirimante, făcând inutilă analiza celorlalte condiţii (Decizia Curţii

Constituţionale nr.66 din 21 februarie 2018, publicată în Monitorul Oficial al României, Partea I, nr.213 din 9 martie 2018, paragraful 38).

34. Obiecţiile de neconstituţionalitate îndeplinesc condiţiile prevăzute de art.146 lit.a) teza întâi din Constituţie atât sub aspectul titularilor dreptului de sesizare, întrucât au fost formulate de un număr de 57 de deputaţi, dintre care deputați aparţinând Grupului parlamentar al USR din Camera Deputaţilor şi deputați neafiliați, și respectiv de Avocatul Poporului, cât şi sub aspectul obiectului, fiind vorba de o lege adoptată, dar nepromulgată încă. Curtea observă că sesizările sunt semnate atât de deputaţi, cât şi de Avocatul Poporului, deputații semnând într-un număr suficient pentru a îndeplini condiţiile prevăzute de Constituţie pentru sesizarea Curţii Constituţionale.

35. Cu privire la termenul în care poate fi sesizată instanţa de contencios constituţional, potrivit art.15 alin.(2) din Legea nr.47/1992, acesta este de 5 zile de la data depunerii legii adoptate la secretarii generali ai celor două Camere ale Parlamentului, respectiv de 2 zile, începând de la acelaşi moment, dacă legea a fost adoptată în procedură de urgenţă. Totodată, în temeiul art.146 lit.a) teza întâi din Legea fundamentală, Curtea Constituţională se pronunţă asupra constituţionalităţii legilor înainte de promulgarea acestora, care, potrivit art.77 alin.(1) teza a doua din Constituţie, se face în termen de cel mult 20 de zile de la primirea legii adoptate de Parlament, iar, potrivit art.77 alin.(3) din Constituţie, în termen de cel mult 10 zile de la primirea legii adoptate după reexaminare.

36. În cauză, propunerea legislativă a fost adoptată de Camera Deputaţilor la data de 19 decembrie 2022, iar de Senat, în calitate de Cameră decizională, la data de 21 decembrie 2022. Legea a fost depusă la secretarii generali ai celor două Camere în vederea exercitării dreptului de sesizare asupra constituţionalităţii la data de 21 decembrie 2022, a fost trimisă Preşedintelui României la data de 23 decembrie 2022 pentru promulgare, iar, la data de 22 decembrie 2022 și, respective, 27 decembrie 2022, au fost formulate prezentele obiecţii de neconstituţionalitate. Prin urmare, având în vedere cele mai sus menționate, Curtea constată că acestea sunt admisibile (a se vedea, în acest sens, şi Decizia Curţii Constituţionale nr.67 din 21 februarie 2018, publicată în Monitorul Oficial al României, Partea I, nr.223 din 13 martie 2018, paragraful 70 prima ipoteză).

37. În consecinţă, Curtea Constituţională a fost legal sesizată şi este competentă, potrivit dispoziţiilor art.146 lit.a) din Constituţie, precum şi ale art.1, 10, 15 şi 18 din Legea nr.47/1992, republicată, să soluţioneze obiecţiile de neconstituţionalitate.

(2.) Analiza obiecţiilor de neconstituţionalitate

38. Examinând obiecţiile de neconstituţionalitate, Curtea reţine că principalele critici de constituționalitate formulate de autorii sesizărilor privesc lipsa de claritate, precizie și previzibilitate a soluțiilor legislative reglementate de art.3 alin.(1) lit.c) cu referire la teza finală, art.21 alin.(1), art.22, art.25, art.41, art.48 și art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, fiind invocată încălcarea prevederilor art.1 alin.(5) din Constituție în componenta referitoare la calitatea legii.

39. Analiza criticilor întemeiate pe dispozițiile art.1 alin.(5) din Constituție are ca punct de plecare însuși scopul legii, precum și obiectivele de reglementare avute în vedere de Legiuitor prin adoptarea Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative. Astfel, art.1 din legea criticată enunță la alin.(1) că scopul reglementării este acela de a stabili *„cadrul juridic și instituțional privind organizarea și desfășurarea activităților din domeniile securitate și apărare cibernetică, mecanismele de cooperare și responsabilitățile instituțiilor cu atribuții în domeniile menționate.”* Securitatea și apărarea cibernetică urmează să se realizeze în viziunea Legiuitorului primar, prin adoptarea și implementarea de politici și măsuri în scopul cunoașterii, prevenirii și contracarării vulnerabilităților, riscurilor și amenințărilor în spațiul cibernetic. În continuare, la art.2 sunt definiți mai mulți termeni și expresii folosite în cuprinsul legii criticate, relevante sub aspectul conținutului pentru criticile și argumentele autorilor sesizărilor (cu titlu de exemplu, Curtea reține definițiile de la lit.l) - furnizor de servicii tehnice de securitate cibernetică, lit.n) - incident de securitate cibernetică, lit.u) - rețele și sisteme informatice, lit.v) - rețele și sisteme informatice specifice apărării naționale, lit.x) - risc de securitate cibernetică, lit.z) - spațiu cibernetic, lit.aa) vulnerabilitate de securitate cibernetică, precum și conceptele de securitate cibernetică și de apărare cibernetică care sunt domeniile principale și speciale de reglementare a legii. Astfel, securitatea cibernetică este definită la lit.y) ca *„starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și non-repudierea informațiilor în format electronic a resurselor și serviciilor publice sau private din spațiul cibernetic,”* în timp ce apărarea cibernetică reprezintă *„totalitatea activităților, mijloacelor și măsurilor utilizate pentru a contracara amenințările cibernetice și a atenua efectele acestora asupra sistemelor de comunicații și tehnologia informației, sistemelor de armament, rețelelor și sistemelor informatice, care susțin capabilitățile militare de apărare (lit.a))”.*

40. Așadar, domeniile principale și speciale de reglementare a legii supuse analizei - securitatea cibernetică și apărarea cibernetică - prefigurează ele însele, criteriile în raport de care vor fi analizate și identificate soluțiile legislative ce fac obiectul controlului de constituționalitate, sub aspectul conținutului lor, a sferei subiecților de drept cărora li se aplică și a întinderii obligațiilor stabilite în sarcina acestora pentru ca legea în ansamblu să își realizeze scopul.

41. Conceptual, noțiunile de securitate cibernetică și apărare cibernetică trebuie analizate ele însele prin raportare la noțiunile deja consacrate în legislație și în jurisprudența Curții, respectiv cele care privesc securitatea națională și apărarea națională. Practic, atât securitatea cibernetică, cât și apărarea cibernetică sunt părți componente ale securității și apărării naționale și au ca finalitate însăși protejarea securității naționale și apărarea națională în spațiul cibernetic definit în legea analizată ca *„mediul virtual generat de rețelele și sistemele informatice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta”.*

42. Așadar, legea supusă controlului de constituționalitate are ca efect, printre altele, și extinderea noțiunii de securitate națională și apărare națională prin includerea spațiului cibernetic în sfera noțiunii anterior menționate. De altfel, chiar Organizația Tratatului Atlanticului de Nord (NATO) încă din anul 2016, a recunoscut spațiul cibernetic ca un domeniu de operațiuni distinct de domeniile de operațiuni clasice (NATO, Varșovia, 2016). Prin *Cyber Defence Pledge*, adoptată la 8 iulie 2016, statele membre NATO și-au asumat să dezvolte cea mai completă gamă de capabilități pentru a apăra infrastructurile și rețelele naționale, inclusiv acele sisteme naționale de care depinde NATO, să integreze apărarea cibernetică în operațiuni, să aloce resurse pentru identificarea și înțelegerea amenințărilor cibernetice, inclusiv prin schimbul de informații, evaluări, cooperare și schimbul de bune practici.

43. În finalul acestui cadru general de analiză a criticilor de neconstituționalitate, Curtea observă că domeniile principale și speciale de reglementare a legii criticate (securitatea și apărarea cibernetică) sunt de fapt concepte plurivalente, iar normele care succed pentru a reglementa conținutul obligațiilor specifice și sfera subiectelor de drept cărora li se adresează, se bucură ele însele de un grad mai mare de flexibilitate, astfel încât să poată fi eficiente prin raportare la ansamblul, dinamica și complexitatea riscurilor, amenințărilor și vulnerabilităților la adresa securității și apărării naționale. În jurisprudența sa (Decizia nr.455 din 4 iulie 2018, publicată în Monitorul Oficial al României, Partea I, nr.622 din 18 iulie 2018), Curtea Constituțională a observat totodată că, în ceea ce privește Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, securitatea națională este menționată în art.8 paragraful 2, art.10 și art.11 ca un prim scop legitim care poate sta la baza restrângerii drepturilor și libertăților prevăzute de aceste prevederi. Convenția pentru apărarea drepturilor omului și a libertăților fundamentale nu definește termenul de „securitate națională”, Curtea Europeană a Drepturilor Omului statuând că acesta nu poate fi definit în mod exhaustiv, bucurându-se de un nivel de elasticitate și flexibilitate care se reflectă în marja de apreciere a statului în această materie. Astfel, Curtea a reținut că principiile accesibilității și previzibilității nu necesită în mod necesar o definiție exhaustivă a noțiunii de „interese ale securității naționale”. Multe legi, care prin obiectul lor de reglementare trebuie să prezinte un anumit grad de flexibilitate, intră, în mod inevitabil, în categoria celor care folosesc termeni care sunt într-o măsură mai mare sau mai mică vagi și a căror interpretare și aplicare sunt chestiuni de practică (a se vedea Decizia de inadmisibilitate din 2 aprilie 1993, pronunțată în *Cauza Esbester împotriva Regatului Unit*). În virtutea acestor considerații generale, Curtea apreciază că aceasta este perspectiva din care trebuie analizate punctual obiecțiile de neconstituționalitate formulate de Avocatul Poporului, precum și de un număr de 57 de deputați cu privire la Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative. Ca atare, Curtea va avea în vedere jurisprudența sa în materie, prin care a consacrat faptul că noțiunea de securitate națională este un concept plurivalent, care vizează securitatea militară, socială, economică, informatică, financiară, iar noile domenii introduse prin legea criticată, respectiv securitatea și apărarea cibernetică sunt de fapt, componente ale securității și apărării naționale și au ca finalitate însăși protejarea securității naționale și apărarea națională în spațiul cibernetic.

44. Analizând criticile formulate cu privire la dispozițiile art.3 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, într-o interpretare sistematică a legii, Curtea observă că securitatea cibernetică este dependentă de implementarea unui nivel minim obligatoriu de măsuri, în mod uniform, la nivelul tuturor infrastructurilor informatice, indiferent de mărimea acestora. Astfel, art.3 din legea criticată reglementează expres tipurile de rețele și sisteme informatice cărora li se adresează normele juridice ce succed, în considerarea rolului și importanței acestor rețele și sisteme pentru buna funcționare a statului, a administrației, a serviciilor publice și a vieții economice și sociale. În funcție de această clasificare, legea analizată obligă autoritățile prevăzute la art.10 la diverse acțiuni, măsuri și activități de natură să protejeze securitatea cibernetică a rețelelor și sistemelor informatice prevăzute la art.3.

Prin soluțiile legislative pe care le conține, legea criticată este proiectată în jurul obiectivelor de protejare a infrastructurilor cibernetice și de cooperare loială între autoritățile publice pentru realizarea acestei protecții.

45. Cu privire la obligațiile născute în temeiul art.3 și următoarele, cu precădere la obligația de notificare prin PNRISC (art.21 și 22 din Lege) și obligația de notificare, la cerere, a incidentelor de securitate cibernetică (art.25), Curtea observă că acestea reprezintă doar mecanisme utile și uzuale pentru a realiza securitatea cibernetică a rețelelor și sistemelor informatice protejate. Astfel, o condiție premisă pentru realizarea securității cibernetice o reprezintă cooperarea între autoritățile prevăzute la art.10 și persoanele deținătoare de rețele și sisteme informatice vizate, colaborare care va realiza prin mecanismele de notificare a incidentelor reglementate de Legiuitorul primar prin legea supusă controlului.

46. Analizând criticile formulate cu privire la dispozițiile art.3 alin.(1) lit.c), cu referire punctuală la sintagma „precum și de persoane fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la lit.b)", Curtea constată că această sintagmă nu poate fi analizată în mod independent față de celelalte prevederi ale legii supuse controlului de constituționalitate sau fără a se ține cont de scopul avut în vedere de Legiuitor, care rezultă din interpretarea sistematică a actului normativ. În primul rând, Curtea observă că subiecții de drept la care se referă sintagma suspusă controlului de constituționalitate sunt determinați de legiuitor prin două atribute: un prim atribut este cel de clarificare și identificare a domeniului de acțiune a respectivilor subiecți de drept „care furnizează servicii publice ori de interes public". Atributul este clar în sensul în care nu se poate avea în vedere decât persoanele fizice și juridice care furnizează servicii publice sau servicii de interes public, indiferent de natura acestora. Al doilea atribut folosit pentru identificarea subiecților de drept este de fapt, unul de excludere, prin eliminarea din sfera persoanelor fizice și juridice reglementate la alin.c) a celor prevăzute anterior, la lit.b) a aceluiași articol 3, adică a persoanelor fizice sau juridice de drept privat, deținătoare de rețele și sisteme informatice, care furnizează un anume tip de servicii publice, respectiv servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale.

47. Așadar, se constată că sfera subiecților de drept la care se referă sintagma criticată este clarificată de Legiuitor atât prin identificarea domeniului lor de activitate (prestarea de servicii publice sau de servicii în interes public), cât și prin excluderea punctuală a unor persoane fizice și juridice de drept privat (care prestează un anume tip de servicii publice de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale), acestea din urmă fiind identificate expres în alin.b) al art.3 din legea analizată.

48. Curtea constată că prin modul în care motivează autorii criticile de neclaritate, lipsă de precizie și de previzibilitate pentru art.3 alin.(1) lit.c), în fapt acestea nu pot fi reținute drept critici întemeiate pe art.1 alin.(5) din Constituție întrucât ele nu vizează claritatea, precizia și previzibilitatea normei criticate, ci sfera de întindere și aplicabilitatea acesteia în raport de subiecții de drept cărora li se adresează. Întrucât sfera de întindere a unei legi este o chestiune care ține de aprecierea și competența Legiuitorului raportat la scopul urmărit, Curtea reține ca fiind necesară o analiză a criticilor prin raportare atât la întregul act normativ, cât și la ansamblul legislației incidente în materie, naționale și europene, fără a omite scopul final urmărit de legiuitor prin reglementare. Acest scop rezultă din interpretarea sistematică a prevederilor legii supuse controlului de constituționalitate, în special prin raportare la obiectivele legii reglementate în art.4 și a autorităților cu atribuții în domeniu (Capitolul III). Din analiza conjugată a ansamblului normativ al legii, rezultă că scopul final urmărit de Legiuitor este asigurarea securității și apărării cibernetice, ca elemente componente ale securității naționale și ale apărării naționale.

49. Cu alte cuvinte, serviciile publice sau serviciile de interes public prestate de persoanele fizice și juridice de drept privat enunțate în art.3 alin.(1) lit.c) vor fi analizate prin raportare la art.4 (obiectivele legii), în special la dispozițiile art.4 lit.a) (asigurarea rezilienței și protecției rețelelor și sistemelor informatice ce susțin funcțiile de apărare, securitate națională, ordine publică și guvernare), lit.c) (menținerea sau restabilirea climatului de securitate cibernetică la nivel național, prin cooperarea între autoritățile competente (...) și asigurarea unei reacții rapide și eficiente la amenințările provenite din spațiul cibernetic) și lit.e) (dezvoltarea și consolidarea unei culturi de securitate cibernetică la nivel național, prin conștientizarea vulnerabilităților, riscurilor și amenințărilor, respectiv formarea unei conduite proactive și preventive).

50. Analizând și alte norme legale naționale și europene în materie, Curtea reține că dispozițiile Directivei (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 (cunoscută ca Directiva NIS 1), publicată în Jurnalul Oficial al Uniunii Europene, seria L, nr.194 din 19 iulie 2016, au fost transpuse în legislația națională prin Legea nr.362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice, publicată în Monitorul Oficial al

României, Partea I, nr.21 din 9 ianuarie 2019. Actul normativ sus menționat prevede cadrul juridic şi instituțional, precum și măsurile şi mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor şi sistemelor informatice; totodată, legea anterior menționată prevede măsuri în scopul stimulării cooperării în domeniul reglementat. Astfel, Legea nr.362/2018 prevede la art.3, semnificația unor termeni și expresii folosite în cuprinsul său, sens în care lit.c) a articolului ante-referit prevede că prin sintagma „furnizor de servicii digitale" se înțelege orice persoană juridică care furnizează un serviciu digital, iar lit.l) a aceluiași articol reglementează sensul expresiei „reţea şi sistem informatic", prin care se înțelege: (i) o rețea de comunicații electronice în sensul prevederilor art.4 alin.(1) pct.6 din Ordonanța de urgență a Guvernului nr.111/2011 privind comunicațiile electronice, aprobată cu modificări şi completări prin Legea nr.140/2012, cu modificările și completările ulterioare; (ii) orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic; (iii) datele digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la pct.1 şi 2 ale aceleiași lit.l) a art.3 din Legea nr.362/2018, în vederea funcționării, utilizării, protejării şi întreținerii lor.

51. În aceste condiții, prevederile art.3 alin.(1) lit.a) și b) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative reglementează în sfera sa de aplicare, 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 și, respectiv, 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.

52. În privința dispozițiilor art.3 lit.c) din legea criticată, Curtea constată că aceste prevederi completează domeniul de aplicare al legii criticate cu: (i) rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de autorități și instituții ale administrației publice centrale și locale, altele decât cele prevăzute la art.3 lit.a) din actul normativ criticat, precum și cu (ii) rețelele și sistemele informatice deținute, organizate, administrate sau utilizate de persoane fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele prevăzute la art.3 lit.b) din aceeași lege. Prin urmare, în vederea asigurării unei securități cibernetice eficiente, legiuitorul a inclus printre persoanele fizice și juridice cărora le incumbă obligațiile reglementate prin legea criticată pe de o parte, autoritățile și instituțiile administrației publice centrale și locale care dețin, organizează, administrează sau utilizează rețele și sisteme informatice și care sunt distincte de autoritățile și instituțiile publice din domeniul ordinii publice, al securității naționale, al justiției, al situațiilor de urgență și al Oficiului Registrului Național al Informațiilor Secrete de Stat, iar pe de altă parte, persoanele fizice și juridice care furnizează servicii publice ori de interes public, care dețin, organizează, administrează sau utilizează rețelele și sistemele informatice și care sunt distincte de persoanele fizice și juridice de drept privat care dețin și utilizează rețelele și sistemele informatice în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale. Așadar, prin actul normativ analizat, au fost incluși în sistemul național de securitate cibernetică toți furnizorii de servicii publice sau de interes public de comunicații electronice, inclusiv persoanele fizice și juridice de mici dimensiuni, care aparțin categoriei întreprinderilor mici și mijlocii, dacă desfășoară activități în interes general, prin furnizarea unor servicii publice sau a unor servicii de interes public.

53. Acest mod de reglementare nu este însă unul lipsit de claritate, precizie și previzibilitate, întrucât noțiunile folosite în delimitarea legală a celor trei categorii de persoane fizice și juridice sunt definite de legiuitor în legislația în vigoare cu respectarea acelorași exigențe de calitate a legii.

54. Astfel, noțiunile de „serviciu public" și de „serviciu de interes public" sunt consacrate, atât în legislația primară, cât și în jurisprudența instanțelor judecătorești și în doctrina de drept administrativ, etimologia, obiectul, conținutul și limitele acestor sintagme fiind, așadar, cunoscute, motiv pentru care acestea nu pot da naștere unor interpretări arbitrare.

55. În acest sens, Curtea reține că dispozițiile art.2 alin.(1) lit.m) din Legea contenciosului administrativ nr.554/2004, publicată în Monitorul Oficial al României, Partea I, nr.1154 din 7 decembrie 2004, prevăd că „serviciul public" reprezintă *„activitatea organizată sau, după caz, autorizată de o autoritate publică, în scopul satisfacerii unui interes legitim public",* definiție ce presupune verificarea împrejurării dacă realizarea serviciului prestat urmărește satisfacerea unui interes general şi dacă aceasta implică, în mod direct sau indirect, o autoritate publică. De asemenea, Ordonanța de urgență a Guvernului nr.57/2019 privind Codul administrativ definește la art.5 lit.kk), „serviciul public" ca fiind *„activitatea sau ansamblul de activităţi organizate de o autoritate a administrației publice ori de o instituţie publică sau autorizată/autorizate ori delegată de aceasta, în scopul satisfacerii unei nevoi cu caracter general sau a unui interes public, în mod regulat şi continuu".*

56. În ceea ce privește noțiunea de „serviciu de interes public”, aceasta nu beneficiază de o definiție legală, dar sensul acestei noțiuni rezultă fără echivoc din interpretarea gramaticală, sistematică și teleologică a dispozițiilor legale în cadrul căreia este folosită de legiuitor. De principiu, sintagma analizată este utilizată în acte normative ce reglementează activități considerate de către legiuitor ca deservind un interes general al societății. În acest sens, Curtea reține că dispozițiile art.315 alin.(2) din Statutul profesiei de avocat, adoptat prin Hotărârea Consiliului Uniunii Naționale a Barourilor din România nr.64 din 3 decembrie 2011, prevăd că *„obligația avocaților de realizare a pregătirii profesionale continue se realizează în cadrul barourilor, al I.N.P.P.A. şi al formelor de exercitare a profesiei şi are drept scop îndeplinirea de către avocaţi a obligaţiei de perfecţionare a pregătirii profesionale, bazată pe o cultură juridică de calitate şi o pregătire temeinică, pentru îndeplinirea corespunzătoare a activităţilor de interes public pe care le implică folosirea titlului profesional de avocat.”* De asemenea, noțiunile de „serviciu public” și de „serviciu de interes public” sunt folosite în cuprinsul prevederilor art.175 alin.(2) Cod penal, potrivit cărora *„este considerată funcționar public, în sensul legii penale, persoana care exercită un serviciu de interes public pentru care a fost învestită de autorităţile publice sau care este supusă controlului ori supravegherii acestora cu privire la îndeplinirea respectivului serviciu public.”* Totodată, „interesul legitim public*”* este definit în art.2 alin.(1) lit.r) din Legea nr.554/2004 a contenciosului administrativ drept „*interesul care vizează ordinea de drept şi democraţia constituţională, garantarea drepturilor, libertăţilor şi îndatoririlor fundamentale ale cetăţenilor, satisfacerea nevoilor comunitare, realizarea competenţei autorităţilor publice”.*

57. Totodată, Curtea Constituțională, prin Decizia nr.781 din 5 decembrie 2017, paragraful 17, Decizia nr.270 din 23 aprilie 2019, paragraful 28 și prin Decizia nr.601 din 10 octombrie 2019, paragraful 23, a statuat că *„Noţiunea de „serviciu public” desemnează atât o formă de activitate prestată în folosul interesului public, cât şi o subdiviziune a unei instituţii din administraţia internă împărţită pe secţii, servicii etc. Din categoria serviciilor de interes public fac parte acele entităţi care, prin activitatea pe care o desfăşoară, sunt chemate să satisfacă anumite interese generale ale membrilor societăţii”*. Totodată, prin Decizia nr.661 din 29 octombrie 2019, paragraful 40, instanța de contencios constituțional a reținut că în doctrină s-a precizat că noţiunea de putere publică desemnează drepturile (prerogativele) speciale, exorbitante, de care dispune orice autoritate a administraţiei publice şi, implicit, orice autoritate publică, în vederea exercitării atribuţiilor sale şi pentru satisfacerea interesului public, care în cazul unui conflict cu cel particular trebuie să se impună. În baza prerogativelor de putere publică de care dispun, măsurile luate de aceste autorităţi se aplică direct, iar în cazul în care nu sunt respectate beneficiază de forţa de constrângere a statului. Totodată, s-a arătat că noţiunea de interes public desemnează necesităţile materiale şi spirituale ale cetăţenilor, la un moment dat.

58. Având în vedere dispozițiile legale și jurisprudența Curții Constituționale mai sus invocate, Curtea reține că sensul general al sintagmei „serviciu de interes public” poate fi acela de serviciu care satisface nevoile de natură materială și spirituală ale societății.

59. Mai mult, serviciile publice ori de interes public din România sunt reglementate și limitate ca număr, în mod implicit, fiind limitat și numărul rețelelor și sistemelor informatice (infrastructurile IT&C) pe care acestea se bazează. În acest sens, Codul administrativ prevede la Titlul II, „Reglementarea și înființarea serviciilor publice”, iar, potrivit art.593 din actul normativ anterior menționat, articol cu denumirea marginală „Stabilirea caracterului de serviciu public”, *„caracterul de serviciu public al unei activităţi sau al unui ansamblu de activităţi se recunoaşte prin acte normativ”*. În completarea dispoziției legale anterior menționate, art.594 al aceluiași cod, articol cu denumirea marginală „Actul de reglementare a unui serviciu public”, prevede elementele pe care actul normativ prin care se reglementează un serviciu public trebuie să le conțină (acestea fiind activitatea sau activitățile care constituie serviciul public respectiv; obiectivele serviciului public; tipul de serviciu public; obligațiile de serviciu public, dacă este cazul; structura responsabilă pentru prestarea serviciului public; modalitățile de gestiune; sursele de finanțare; modalități de monitorizare, evaluare şi control a modului de furnizare a serviciului public; sancțiuni; standarde de calitate şi de cost, în cazul în care acestea sunt stabilite potrivit legii; alte elemente stabilite prin lege).

60. În ceea ce privește sensul sintagmei „rețele și sisteme informatice” din cuprinsul art.3 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, acesta nu poate fi altul decât cel definit la art.3 lit.l) din Legea nr.362/2018, mai sus analizat, Legea nr.362/2018 constituind reglementarea generală în domeniul asigurării securității rețelelor şi sistemelor informatice.

61. Cu privire la sensul sintagmei „altele decât cele de la lit.b)” din cuprinsul art.3 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, Curtea reține că legea criticată protejează prioritar, la art.3 alin.(1) lit.a), rețelele și sistemele informatice ale autorităților și instituțiilor din sistemul național de ordine publică, de apărare națională, de securitate națională, din domeniul justiției, al situațiilor de urgență și

din cadrul Oficiului Național al Informațiilor Secrete de Stat [cu titlu exemplificativ, se încadrează în această categorie programul software din cadrul Sistemului național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor cibernetice („ȚIȚEICA") administrat de Serviciul Român de Informații care este, potrivit art.6 din Legea nr.51/1991 privind securitatea naţională a României și art.1 din Legea nr.14/1992 privind organizarea si functionarea Serviciului Român de Informații, autoritate publică cu atribuții în domeniul securității naționale], iar prin dispozițiile art.3 alin.(1) lit.b) din aceeași lege reglementează protecția rețelelor și a sistemelor informatice aparținând persoanelor 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 [cu titlu exemplificativ, fac parte din această categorie aplicațiile software ale Societății Naţionale de Radiocomunicaţii S.A care asigură difuzarea şi transportul programelor publice naţionale de televiziune ale Societăţii Române de Televiziune, ca instituție publică].

62. Prin raportare la aceste dispoziții legale de la alin.(1) lit.a) și b), prevederile art.3 alin.(1) lit.c) din legea criticată au în vedere toate celelalte persoane fizice și juridice, altele decât cele prevăzute la lit.a) și b), în condițiile în care acestea furnizează servicii publice sau de interes public, sintagme al căror sens a fost determinat mai sus [cu titlu exemplificativ, aparține acestei ultime categorii, sistemul software al operatorului privat de apă potabilă dintr-o localitate prin care se asigură furnizarea automată, calibrarea, purificarea și măsurarea apei potabile pentru populație, operatorul privat de servicii de apă potabilă fiind o persoană juridică de drept privat care prestează un serviciu de interes public, conform dispozițiilor art.1 alin.(2) lit.a) din Legea nr.51/2006 a serviciilor comunitare de utilități publice, publicată în Monitorul Oficial al României, Partea I, nr.121 din 5 martie 2013].

63. Având în vedere aceste considerente, Curtea constată că maniera de reglementare a domeniului de aplicare al Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, prevăzut la art.3 din legea criticată este una clară, precisă și previzibilă, iar caracterul extins al sferei de aplicare a legii analizate nu echivalează cu lipsa de claritate, precizie sau previzibilitate a normelor juridice care îl reglementează, reflectând scopul și obiectivele legii.

64. Prin urmare, Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative conține criterii suficiente pentru a determina cu claritate subiecții de drept, persoane fizice și juridice, cărora le revin obligațiile prevăzute în cuprinsul legii, prin simpla interpretare gramaticală și sistematică a prevederilor art.3 din actul normativ criticat.

65. Mai mult, având în vedere trimiterile făcute de autorii prezentelor sesizări la considerentele Deciziei nr.17 din 21 ianuarie 2015, publicată în Monitorul Oficial al României, Partea I, nr.79 din 30 ianuarie 2015, Curtea constată că Legea privind securitatea cibernetică a României (PL-x nr.263/2014), care a constituit obiectul sesizării de neconstituționalitate soluționate de Curtea Constituțională prin decizia antereferită, reglementa domeniul său de aplicare într-o manieră foarte generală, fără a distinge între categoriile de persoane care dețin, organizează, administrează sau utilizează rețele și sisteme informatice. Așadar, Legiuitorul, însușindu-și considerentele Deciziei nr.17 din 21 ianuarie 2015, a prevăzut la art.3 din noua lege adoptată – Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, - un domeniu de reglementare în cadrul căruia a distins între cele trei categorii de persoane prevăzute la lit.a)-c) ale art.3 alin.(1) anterior menționat, definindu-le pe acestea potrivit criteriilor mai sus analizate.

66. Pentru motivele mai sus arătate, Curtea reține că dispozițiile art.3 alin.(1) lit.c) din Legea privind securitatea și apărare cibernetică a României, precum și pentru modificarea și completarea unor acte normative sunt clare, precise și previzibile, fiind în acord cu exigențele specifice calității legii, astfel cum acestea rezultă din prevederile art.1 alin.(5) din Constituție, dar și din jurisprudența Curții Constituționale și a Curții Europene a Drepturilor Omului invocată de autorii sesizărilor.

67. Cu privire la standardele de calitate a legii, Curtea Constituțională, făcând trimitere la jurisprudența Curții Europene a Drepturilor Omului, a statuat în jurisprudența sa, că semnificaţia noţiunii de previzibilitate depinde într-o mare măsură de conţinutul textului analizat şi de domeniul pe care îl acoperă, precum şi de numărul şi de calitatea destinatarilor săi. S-a arătat prin aceeași jurisprudență, că principiul previzibilităţii legii nu se opune ideii ca persoana vizată să fie determinată să recurgă la îndrumări clarificatoare pentru a putea evalua, într-o măsură rezonabilă în circumstanţele cauzei, consecinţele ce ar putea rezulta dintr-o anumită faptă. S-a arătat că acesta este, în special, cazul profesioniştilor, care sunt obligaţi să dea dovadă de o mare prudenţă în exercitarea profesiei, motiv pentru care se aşteaptă din partea lor să acorde o atenţie specială evaluării riscurilor pe care aceasta le prezintă (Hotărârile din 15 noiembrie 1996, 24 mai 2007 și 20 ianuarie 2009, pronunţate în *Cauzele Cantoni împotriva Franţei*, paragraful 35, *Dragotoniu şi Militaru-Pidhorni împotriva României*, paragraful 35, și *Sud Fondi SRL şi alţii împotriva Italiei*, paragraful 109). Totodată, atât Curtea Constituțională, cât și Curtea de la Strasbourg au reţinut că formularea legilor nu poate prezenta o precizie absolută și că

una dintre tehnicile standard de reglementare constă în recurgerea mai degrabă la categorii generale decât la liste exhaustive. Astfel, s-a reținut că numeroase legi folosesc, prin forţa lucrurilor, formule mai mult sau mai puţin vagi, a căror interpretare şi aplicare depind de practică și că, oricât de clar ar fi redactată o normă juridică, în orice sistem de drept, există un element inevitabil de interpretare judiciară (a se vedea Decizia nr.717 din 29 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr.216 din 23 martie 2016).

68. În aceste condiții, Curtea reține că destinatarii legii criticate de autorii obiecțiilor pot determina cu claritate, precizie și previzibilitate persoanele fizice și juridice furnizoare de servicii de comunicații electronice cărora le incumbă obligațiile reglementate prin actul normativ ce face obiectul prezentelor obiecții de neconstituționalitate, aceste categorii de persoane fiind determinate sau determinabile. Pentru aceste motive nu poate fi reținută critica potrivit căreia legiuitorul primar a lăsat legiuitorului secundar o marjă largă de apreciere în vederea determinării, prin hotărâre a Guvernului, a persoanelor reglementate prin dispozițiile art.3 alin.(1) lit.c) din legea analizată. Astfel, prin raportare la prevederile legii supuse controlului de constituționalitate și interpretând sistematic prevederile sale, Curtea constată faptul că sfera de întindere a persoanelor fizice sau juridice private care prestează servicii publice sau de interes public nu poate să vizeze decât acele persoane fizice și juridice de drept privat care prestează servicii publice sau de interes public cu un impact asupra securității naționale în spațiul cibernetic, iar nu orice persoană fizică sau juridică de drept privat care prestează orice serviciu public sau de interes public.

69. Pentru aceste motive, Curtea reține că prin adoptarea Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, Parlamentul și-a exercitat de o manieră corectă, lipită de echivoc, atribuția constituțională prevăzută la art.61 alin.(1) din Legea fundamentală, creând un cadru legal al asigurării securității și apărării cibernetice clar, precis și previzibil, atât pentru persoanele fizice și juridice vizate de legea criticată, cât și pentru autoritățile statului implicate în procesul de interpretare și aplicare a dispozițiilor legale din cuprinsul acesteia.

70. Pe cale de consecință, Guvernul, în calitatea sa de legiuitor secundar, își va putea exercita, conform art.108 alin.(2) din Constituție, într-o manieră corectă și în acord cu rigorile impuse de dispozițiile Legii fundamentale, atribuția de organizare a executării legii criticate, prin adoptarea, conform art.52 alin.(1) din legea analizată, în termenul de 60 de zile de la data intrării acesteia în vigoare, a hotărârii inițiate de Ministerul Cercetării, Inovării și Digitalizării. Prin hotărârea Guvernului anterior menționată vor fi determinate categoriile concrete de persoane fizice și juridice dintre cele reglementate, cu titlu general, la art.3 alin.(1) lit.c) din legea criticată; stabilirea acestor categorii de persoane se va realiza însă, potrivit criteriilor de determinare prevăzute de însăși legea analizată. Astfel, categoriile de persoane – subiecți de drept se pot stabili prin hotărâre de Guvern numai prin luarea în considerare a criteriului de clarificare stabilit expres în lege (dacă prestează servicii publice sau servicii de interes public), a criteriului de eliminare (altele decât persoanele fizice sau juridice care prestează servicii publice de comunicații electronice pentru entități publice centrale sau locale) și a obiectivelor avute în vedere de legiuitor la art.4, prin identificarea numai a acelor categorii de persoane fizice sau juridice care prestează servicii publice sau de interes public care pot afecta securitatea cibernetică, deci și securitatea națională. În consecință, prin hotărârea prevăzută la art.52 alin.(1), Guvernul va organiza punerea în aplicare a prevederilor art.3 alin.(1) lit.c), ținând cont de ansamblul normativ al întregii legi. Or, o hotărâre de Guvern care este prevăzută de legea însăși pentru punerea în aplicare a unui articol din respectiva lege nu poate fi adoptată cu ignorarea întregului ansamblu normativ. Principiul legalității presupune ca actul administrativ să respecte nu doar norma legală de trimitere, ci ansamblul normativ aplicabil în respectivul domeniu de reglementare.

71. Pentru aceste considerente, Curtea reține că dispozițiile art.3 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative asigură și respectarea principiului securității raporturilor juridice, astfel cum acesta este reglementat prin dispozițiile art.1 alin.(5) din Constituție, iar, la nivel infralegal, prin exigențele Legii nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată în Monitorul Oficial al României, Partea I, nr.260 din 21 aprilie 2010. Referitor la acest principiu, Curtea Constituțională a reținut, în jurisprudența sa, 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 şi coordonarea legislației, precum şi conținutul şi forma juridică adecvate pentru fiecare act normativ. Astfel, respectarea acestor norme concură la asigurarea unei legislații care respectă principiul securității raporturilor juridice, având claritatea şi previzibilitatea necesară (a se vedea Decizia nr.26 din 18 ianuarie 2012, publicată în Monitorul Oficial al României, Partea I, nr.116 din 15 februarie 2012, Decizia nr.17 din 21 ianuarie 2015, publicată în Monitorul Oficial al României, Partea I, nr.79 din 30 ianuarie 2015, paragraful 96). În același sens, instanța de contencios constituțional a statuat că, pentru ca legea să satisfacă cerința de

previzibilitate, ea trebuie să precizeze cu suficientă claritate întinderea şi modalităţile de exercitare a puterii de apreciere a autorităților în domeniul respectiv, ţinând cont de scopul legitim urmărit, pentru a oferi persoanei o protecție adecvată împotriva arbitrariului (a se vedea Decizia nr.348 din 17 iunie 2014, publicată în Monitorul Oficial al României, Partea I, nr.529 din 16 iulie 2014, paragraful 17 și Decizia nr.302 din 4 mai 2017, publicată în Monitorul Oficial al României, Partea I, nr.566 din 17 iulie 2017, paragraful 56). De asemenea, s-a reținut, prin aceeași jurisprudență, că o dispoziție legală trebuie să fie precisă, neechivocă, să instituie norme clare, previzibile şi accesibile a căror aplicare să nu permită arbitrariul sau abuzul, precum și că norma juridică trebuie să reglementeze în mod unitar și uniform și să stabilească cerinţe minimale aplicabile tuturor destinatarilor săi (a se vedea Decizia nr.637 din 13 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr.906 din 8 decembrie 2015, paragraful 34). Or, având în vedere considerentele mai sus arătate, Curtea reține că dispozițiile art.3 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative sunt în acord cu exigențele constituționale anterior analizate.

72. Aceleași considerente sunt valabile, *mutatis mutandis*, și cu privire la criticile de neconstituționalitate referitoare la lipsa de claritate, precizie și previzibilitate a prevederilor art.21 alin.(1) și art.22 din legea criticată prin raportare la art.1 alin.(5) din Constituție, neputând fi reținute ca întemeiate.

73. În ceea ce privește critica privind caracterul foarte larg al domeniului de aplicare astfel reglementat, aspect care, potrivit susținerilor autorilor sesizărilor, ar contraveni punctului 53 din Preambulul Directivei (UE) 2016/1148, Curtea reține că, odată cu transformarea digitală rapidă și interconectarea societății, rețelele și sistemele informatice au devenit o componentă centrală a vieții de zi cu zi, inclusiv în cadrul schimburilor transfrontaliere. Or, extinderea semnificativă a amenințărilor la adresa securității cibernetice constituie o provocare majoră pentru societate, care generează nevoia de răspunsuri adecvate, coordonate și inovatoare din partea tuturor statele membre ale Uniunii Europene. În aceste condiții, standardele de protecție reglementate în materia securității cibernetice, impuse furnizorilor de servicii de comunicații electronice sau operatorilor economici, variază considerabil la nivelul statelor membre ale Uniunii Europene. Aceste diferențe generează însă costuri suplimentare pentru entitățile care oferă bunuri sau servicii la nivel transfrontalier, ele putând afecta în mod substanțial asemenea activități. Pentru aceste motive, cu prilejul revizuirii Directivei (UE) 2016/1148 (Directiva NIS 1), s-a arătat că transpunerea și aplicarea acesteia diferă foarte mult la nivelul statelor membre ale Uniunii Europene, inclusiv în ceea ce privește domeniul său de aplicare, a cărui delimitare a fost lăsată, în mare măsură, la latitudinea acestor state. Totodată, directiva anterior menționată oferă statelor membre o marjă foarte largă de apreciere în ceea ce privește transpunerea și îndeplinirea obligațiilor de raportare a incidentelor cibernetice, aspect care a determinat existența unor diferențe între statele membre în privința manierei de reglementare a acestor obligații la nivel național.

74. Curtea constată că introducerea în domeniul de aplicare a legii criticate, a categoriilor de persoane fizice și juridice care furnizează servicii publice sau de interes public prevăzute la art.3 alin.(1) lit.c) este în acord cu unul dintre scopurile Directivei (UE) 2022/2555 (Directiva NIS 2), respectiv acela prevăzut la punctul 7 din Preambulul directivei de *„a elimina divergențele mari dintre statele membre în această privință și pentru a asigura securitatea juridică în ceea ce privește măsurile de gestionare a riscurilor în materie de securitate cibernetică și obligațiile de raportare pentru toate entitățile relevante, ar trebui stabilit un criteriu uniform pentru a determina entitățile care intră în domeniul de aplicare al prezentei directive. Criteriul respectiv ar trebui să constea în aplicarea unei norme de plafonare a dimensiunii, potrivit căreia toate entitățile care se califică drept întreprinderi mijlocii în temeiul articolului 2 din anexa la Recomandarea 2003/361/CE a Comisiei, sau depășesc plafoanele aferente întreprinderilor mijlocii prevăzute la alineatul (1) din respectivul articol, și care își desfășoară activitatea în sectoarele și furnizează tipurile de servicii sau desfășoară activitățile reglementate de prezenta directivă intră în domeniul său de aplicare. Statele membre ar trebui, de asemenea, să prevadă ca anumite întreprinderi mici și microîntreprinderi, astfel cum sunt definite la articolul 2 alineatele (2) și (3) din respectiva anexă, care îndeplinesc criterii specifice ce indică un rol esențial pentru societate, pentru economie sau pentru anumite sectoare sau tipuri de servicii, să intre în domeniul de aplicare al prezentei directive.”* De altfel, și punctul 6 din același Preambul prevede faptul că: *„Odată cu abrogarea Directivei (UE) 2016/1148, domeniul de aplicare pe sectoare ar trebui să fie extins la o parte mai mare a economiei pentru a oferi o acoperire cuprinzătoare a sectoarelor și a serviciilor de importanță vitală pentru activitățile societale și economice esențiale din cadrul pieței interne. În special, prezenta directivă vizează depășirea deficiențelor legate de diferențierea dintre operatorii de servicii esențiale și furnizorii de servicii digitale, care s-a dovedit a fi caducă, deoarece nu reflectă importanța sectoarelor sau a serviciilor pentru activitățile societale și economice din cadrul pieței interne.”*

75. În acest context, Curtea reține că Directiva (UE) 2022/2555 (Directiva NIS 2) nu exceptează întreprinderile mici și mijlocii de la obligațiile din domeniul securității informatice, ci, dimpotrivă, furnizează mai multă claritate, precizie și predictibilitate cu privire la obligațiile acestora; totodată, directiva analizată introduce această categorie de persoane în toate cele șaisprezece sectoare de activitate care intră sub incidența acesteia. De asemenea, Directiva (UE) 2022/2555 (Directiva NIS 2) permite statelor membre să stabilească, prin acte normative interne, noi subiecți legali care să vină în realizarea strategiei securității cibernetice naționale a statului membru în cauză și obligă statele membre *„să adopte un cadru pro-activ de pregătire și de siguranță și securitate generale în caz de incidente sau amenințări cibernetice", prin politici de „igienă cibernetică", astfel cum rezultă din punctul 49 al Preambulului anterior menționat și „să adopte politici privind promovarea unei protecții cibernetice active ca parte a unei strategii defensive mai ample*", conform punctului 57 din același Preambul.

76. Or, în acest context legal european, legiuitorul român și-a exercitat dreptul a stabili soluții legislative care să răspundă scopului asigurării securității și apărării cibernetice adecvate a României.

77. Având în vedere considerentele mai sus invocate, Curtea reține că prevederile art.3 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, care includ în sfera destinatarilor legii inclusiv persoane fizice și juridice care furnizează servicii publice ori de interes public, altele decât cele de la alin.(1) lit.b) din cuprinsul aceluiași articol, extinzând, astfel, sfera persoanelor cărora le incumbă obligațiile prevăzute prin actul normativ criticat, la întreprinderile mici și mijlocii, nu contravin dispozițiilor constituționale ale art.148 alin.(2) și (4) referitoare la integrarea în Uniunea Europeană și nici prevederilor art.11 din Legea fundamentală cu privire la dreptul internaţional şi dreptul intern.

78. În ceea ce privește critica conform căreia dispozițiile art.3 alin.(1) lit.c) și cele ale art.21 alin.(1) și art.22 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative încalcă dreptul la viața intimă, familială și privată, precum și libertatea de exprimare, a căror încălcare a constituit unul dintre temeiurile admiterii de către Curtea Constituțională, prin Decizia nr.17 din 21 ianuarie 2015, a obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României (PL-x nr.263/2014), Curtea constată că prin legea care constituie obiectul prezentelor sesizări de neconstituționalitate, legiuitorul a legiferat garanții sporite necesare asigurării dreptului, respectiv a libertății fundamentale prevăzute la art.26 și, respectiv la art.30 din Constituție.

79. În acest sens, dispozițiile art.25 alin.(1) din legea analizată prevăd că furnizorii de servicii tehnice de securitate cibernetică au obligația de a pune la dispoziția autorităților prevăzute la art.10 din aceeași lege, 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) din actul normativ analizat, precum și interconectarea acestora cu terții și cu utilizatorii finali. În strictă corelare cu aceste prevederi, art.25, prevede la alin.(2), că datele și informațiile prevăzute la alin.(1) nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut. Or, această manieră de reglementare a obligației furnizorilor de servicii tehnice de securitate cibernetică de a furniza informațiile solicitate de autoritățile prevăzute la art.10 din legea criticată, exclude accesul acestora din urmă la datele și informațiile ce apațin sferei vieții intime, familiale și private a utilizatorilor de rețele și sisteme informatice, asigurându-le, totodată, acestora garanțiile specifice libertății de exprimare, astfel cum aceasta este prevăzută la art.30 din Constituție.

80. Totodată, legea criticată conține un capitol distinct, Capitolul IX, intitulat „Confidențialitatea și protecția securității datelor și informațiilor persoanelor fizice și juridice", care la art.45-47, instituie garanții în vederea protecției dreptului la viață intimă, familială și privată a persoanelor aflate în ipoteza de utilizatori de rețele și sisteme informatice vizate de prevederile legii criticate, dispoziții legale ce constituie tot atâtea garanții ale libertății de exprimare ale acestora.

81. Astfel, art.45 din legea criticată prevede că autoritățile prevăzute la art.10 din aceeași lege, care solicită și primesc date și informații de la orice persoană fizică și juridică în temeiul acestei legi, iau măsuri adecvate pentru a proteja interesele de securitate și comerciale ale acestora, ale persoanelor care furnizează datele și informațiile respective, precum și ale persoanelor la care se referă datele și informațiile în cauză, iar alin.(2) al aceluiași articol prevede că transmiterea de date și informații obținute potrivit legii analizate, de la orice persoană fizică și juridică de drept privat, poate fi efectuată numai pentru îndeplinirea atribuțiilor legale ale autorităților și instituțiilor care obțin aceste date și informații, cu garantarea păstrării confidențialității datelor cu caracter personal și a protecției intereselor și secretelor comerciale ale persoanelor fizice și juridice de drept privat. De asemenea, art.46 din legea criticată reglementează faptul că prelucrările de date cu caracter personal ce intră sub incidența acestei legi se efectuează cu respectarea reglementărilor legale privind protecția persoanelor fizice în ceea ce

privește prelucrarea datelor cu caracter personal; alin.(2) al art.46 anterior menționat prevede că notificările realizate în temeiul legii criticate nu afectează obligațiile operatorilor de date cu caracter personal stabilite potrivit art.33 și 34 din Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor); alin.(3) al aceluiași art.46 prevede că, în scopul îndeplinirii atribuțiilor ori furnizării serviciilor prevăzute de legea criticată, precum și în scopul prevenirii și răspunsului la incidentele de securitate cibernetică ori al cooperării la nivel național, comunitar și internațional în prevenirea și răspunsul la incidentele de securitate cibernetică, autoritățile prevăzute la art.10 din aceeași lege colectează, primesc, prelucrează și transmit date și informații ce pot constitui sau pot conține date cu caracter personal, în limitele legislației aplicabile, cu asigurarea respectării prevederilor alin.(2) al aceluiași articol, mai sus invocat. Nu în ultimul rând, art.47 din legea criticată prevede că acest act normativ nu afectează legislația națională privind protecția datelor cu caracter personal, fiind enumerate în special, Legea nr.506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare, Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice), cu modificările și completările ulterioare, și Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016, Legea nr.190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor), cu modificările ulterioare. La alin.(2) al art.47 din legea criticată se prevede că aceasta din urmă respectă drepturile fundamentale și principiile recunoscute în special de Carta drepturilor fundamentale a Uniunii Europene, inclusiv dreptul la respectarea vieții private și de familie, dreptul la protecția datelor cu caracter personal, dreptul la proprietate și integrarea persoanelor cu dizabilități, astfel încât nicio prevedere din prezenta lege nu trebuie să facă obiectul unei interpretări sau puneri în aplicare care nu este conformă cu Convenția pentru apărarea drepturilor omului și a libertăților fundamentale a Consiliului Europei.

82. În concluzie, Curtea constată că dispozițiile legale ce compun Capitolul IX al Legii privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative instituie garanții ale dreptului la viață intimă, familială si privată care nu au fost prevăzute în Legea privind securitatea cibernetică a României (PL-x nr.263/2014), a cărei neconstituționalitate a fost constatată de către instanța de contencios constituțional prin Decizia nr.17 din 21 ianuarie 2015. Așadar, însușindu-și considerentele deciziei antereferite, Legiuitorul a adoptat legea ce constituie obiectul prezentelor sesizări, în cuprinsul căreia a reglementat inclusiv garanțiile necesare asigurării dreptului la viață intimă, familială și privată și, implicit, a libertății de exprimare persoanelor fizice și juridice de drept privat care intră în domeniul său de aplicare, astfel cum acestea sunt garantate prin dispozițiile Legii fundamentale.

83. Având în vedere aceste considerente, dispozițiile art.3 alin.(1) lit.c) și cele ale art.21 alin.(1) și art.22 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative nu contravin dispozițiilor constituționale ale art.147 alin.(4) referitoare la deciziile Curții Constituționale.

84. Mai mult, analizând dispozițiile legale mai sus invocate, Curtea reține că sistemele de notificare prevăzute la art.21, art.22, respectiv la art.25 din legea criticată nu presupun colectarea de date de conținut și nici extragerea unilaterală și fără autorizare de date și informații de pe un sistem informatic, iar autoritățile care gestionează incidentele de securitate cibernetică semnalate sunt atât operatori de date cu caracter personal (prin efectul legislației privind datele cu caracter personal), cât și autorități cu atribuții expres prevăzute în domeniul securității cibernetice (atribuțiile acestora neputând fi confundate sau suprapuse cu cele ale organelor judiciare care realizează percheziții informatice, conform art.168 din Codul de procedură penală). Prin urmare, obligațiile care revin subiectelor de drept prevăzute la art.3 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative nu se referă nici la stocarea de date cu caracter personal ale cetățenilor, nici la accesul, în lipsa unui mandat judecătoresc, într-un sistem informatic și nici la alte proceduri intruzive în viața privată a cetățeanului.

85. În acest context, Curtea reține faptul că singura ipoteză legală care prevede accesul organelor statului la datele electronice cu caracter personal rămâne cea prevăzută la art.168 din Codul de procedură penală, articol ce reglementează percheziția informatică. Conform alin.(1) al art.168 anterior menționat, prin percheziție în sistem informatic sau a unui suport de stocare a datelor informatice se înțelege procedeul de cercetare, descoperire, identificare şi strângere a probelor stocate

într-un sistem informatic sau suport de stocare a datelor informatice, realizat prin intermediul unor mijloace tehnice şi proceduri adecvate, de natură să asigure integritatea informaţiilor conţinute de acestea. Percheziția informatică poate fi dispusă, în cursul urmăririi penale, la cererea procurorului, prin încheiere, de către judecătorul de drepturi și libertăți de la instanţa căreia i-ar reveni competenţa să judece cauza în primă instanţă sau de la instanţa corespunzătoare în grad acesteia în a cărei circumscripţie se află sediul parchetului din care face parte procurorul care efectuează sau supraveghează urmărirea penală. De asemenea, percheziția informatică poate fi dispusă în cursul judecăţii, de către instanță, din oficiu sau la cererea procurorului, a părţilor ori a persoanei vătămate. Așadar, percheziția informatică poate fi dispusă în cursul procesului penal, acesta presupunând, per se, începerea urmăririi penale într-o cauză de aceeași natură.

86. Or, ipoteza reglementată de dispozițiile legii criticate nu este cea a accesului la datele dintr-un sistem informatic sau de pe un suport de stocare a datelor informatice, ci vizează operațiunea de raportare de către persoanele prevăzute la art.3 alin.(1) din legea criticată a unor incidente cibernetice, operațiune cu caracter strict tehnic, ce nu presupune nici stocarea datelor cu caracter personal, nici intruziunea în conținutul acestor date. Pentru aceste motive, garanțiile impuse de legiuitor referitoare la asigurarea securității acestor date nu pot fi cele prevăzute de dispozițiile Codului de procedură penală în privința realizării percheziției cibernetice, neimpunându-se, așadar, controlul judecătoresc al operațiunilor strict tehnice de raportare a incidentelor cibernetice reglementate prin legea criticată cu respectarea strictă a scopului acesteia.

87. Cu privire la proporționalitatea obligațiilor ce revin subiectelor de drept care au în proprietate, administrare, organizare și utilizare rețele și sisteme informatice de tipul celor prevăzute de art.3 alin.(1) lit.c), potrivit actului normativ criticat, Curtea constată că aceste obligații sunt, de principiu, următoarele: 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 [prevăzută la art.21 alin.(1) criticat și de autorii obiecțiilor]; obligația de asigurare a reziliență în spațiul cibernetic, care se realizează prin implementarea de măsuri proactive și reactive [prevăzută la art.24 alin.(1) din legea criticată]; obligația de a pune la dispoziția autorităților prevăzute la art.10 din legea ce face obiectul sesizării, la cererea motivată a acestora, în termen de maximum 48 de ore de la data primirii solicitării, date și informații privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art.3 alin.(1) din aceeași lege, precum și interconectarea acestora cu terții și cu utilizatorii finali [prevăzută la art.25 alin.(1) criticat și de autorii obiecțiilor]; obligația de a elabora și de punere în aplicare a unor planuri proprii de acțiune pentru fiecare tip de alertă cibernetică [prevăzută la art.29 alin.(1) și (2) din legea criticată]; obligația de asigurare, pentru personalul propriu, a formării profesionale, educației și instruirii în domeniul securității și apărării cibernetice prin cursuri, exerciții, conferințe, seminarii, precum și alte tipuri de activități [prevăzută la art.37 din legea criticată]; obligația de a implementa procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare [prevăzută la art.41 criticat și de autorii obiecțiilor]; obligația de a desemna persoane responsabile de securitatea cibernetică [prevăzută la art.42 din legea criticată]; obligația de a dispune măsurile necesare pentru organizarea de cursuri de instruire în domeniul managementului riscurilor de securitate cibernetică specifice lanțului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor și programelor de instruire existente [prevăzută la art.43 din legea criticată]; obligația de a dezvolta capabilități avansate de testare și evaluare a riscurilor de securitate cibernetică în scopul identificării vulnerabilităților cibernetice ale echipamentelor, produselor software sau pieselor componente achiziționate sau dezvoltate la nivel instituțional [prevăzută la art.44 din legea criticată].

88. Analizând conținutul obligațiilor mai sus enumerate sub aspectul proporționalității lor și prin raportare la scopul legii criticate, precum și argumentele prin care autorii își întemeiază critica potrivit căreia prevederile art.21 alin.(1) instituie obligații disproporționate sub aspectul caracterului lor excesiv de oneros în sarcina persoanelor fizice și juridice prevăzute la art.3 alin.(1) lit.c) din aceeași lege - cum sunt, cu titlu exemplificativ, obligațiile de a asigura personalului propriu formarea profesională, educația și instruirea în domeniul securității și apărării cibernetice, prin participarea la cursuri, la exerciții, la conferințe, la seminarii, precum și la alte tipuri de activități – și fără să se prevadă acordarea unui ajutor financiar din partea statului, Curtea constată că evaluarea acestor categorii de costuri excedează competenței instanței de contencios constituțional care, conform art.2 alin.(3) din Legea nr.47/1992 privind organizarea și funcționarea Curții Constituționale, *„se pronunţă numai asupra constituţionalităţii actelor cu privire la care a fost sesizată, fără a putea modifica sau completa prevederile supuse controlului”.*

89. Cu privire la criticile de neconstituționalitate referitoare la dispozițiile art.25 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, potrivit cărora acestea creează o obligație de delațiune în sarcina unei categorii

de profesioniști care, în mod normal, ar avea obligații de confidențialitate față de proprii clienți, Curtea constată că nici această critică nu poate fi reținută în raport de motivele arătate de autorii obiecțiilor.

90. În acest sens, Curtea constată că obligațiile prevăzute prin textul criticat vizează exclusiv obligația furnizorilor de servicii tehnice de securitate cibernetică, de a pune la dispoziția autorităților prevăzute la art.10 din legea criticată, datele și informațiile referitoare la incidentele de securitate cibernetică sau la amenințări, la riscuri sau la vulnerabilități a căror manifestare poate afecta o rețea sau un sistem informatic dintre cele prevăzute la art.3 alin.(l) din legea criticată; totodată, obligația astfel reglementată vizează și interconectarea acestora cu terții și cu utilizatorii finali.

91. Curtea reține, de asemenea, că, potrivit art.2 lit.n) din legea criticată de autorii sesizărilor, prin „incident de securitate cibernetică" se înțelege un eveniment survenit în spațiul cibernetic care perturbă funcționarea uneia sau mai multor rețele și sisteme informatice și ale cărui consecințe sunt de natură a afecta securitatea cibernetică, iar, conform art.2 lit.b) din aceeași lege, noțiunea de „amenințare cibernetică" are sensul arătat la art.2 lit.f) din Ordonanța de urgență a Guvernului nr.104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr.11/2022, respectiv acela de *„orice circumstanţă, eveniment sau acţiune potenţială care ar putea cauza daune sau perturbări la nivelul reţelelor şi al sistemelor informatice, precum şi la nivelul utilizatorilor unor astfel de sisteme şi al altor persoane sau care poate avea un alt fel de impact negativ asupra acestora"*. Totodată, potrivit art.2 lit.x) din legea criticată, sensul noțiunii de „risc de securitate cibernetică" este cel prevăzut la art.2 lit.r) din Ordonanța de urgență a Guvernului nr.89/2022 privind înființarea, administrarea şi dezvoltarea infrastructurilor şi serviciilor informatice de tip cloud utilizate de autorităţile şi instituţiile publice, respectiv acela de „probabilitatea ca o ameninţare să se materializeze, exploatând o vulnerabilitate specifică reţelelor şi sistemelor informatice", iar, potrivit lit.aa) din cuprinsul aceluiași articol, prin „vulnerabilitate de securitate cibernetică" se înțelege o slăbiciune în proiectarea, implementarea, dezvoltarea, configurarea și mentenanța rețelelor și a sistemelor informatice sau a măsurilor de securitate aferente, care poate fi exploatată de către o amenințare.

92. Totodată, dispozițiile legale mai sus invocate trebuie interpretate în coroborare cu prevederile art.27 lit.b) din Legea nr.362/2018, care prevăd în sarcina operatorilor de servicii esențiale (OSE) și a furnizorilor de servicii digitale (FSD) obligația de a furniza informații suplimentare cu privire la incidentele de securitate cibernetică, Directoratul Național de Securitate Cibernetică putând solicita informații suplimentare operatorului sau furnizorului autor al notificării, în vederea îndeplinirii obligațiilor ce îi revin, cu menționarea termenului în care informațiile solicitate trebuie furnizate, dar și cu dispozițiile Secțiunii 2 – „Notificarea incidentelor de securitate" a Capitolului IV – „Asigurarea securităţii reţelelor şi sistemelor informatice" al aceleași legi, care prevăd la art.26 alin.(3) și (4), că notificarea incidentelor conține, în mod obligatoriu, următoarele informații: elementele de identificare ale infrastructurii şi operatorului sau furnizorului în cauză; descrierea incidentului; perioada de desfăşurare a incidentului; impactul estimat al incidentului; măsuri preliminare adoptate; lista de autorităţi ale statului afectate de incident; întinderea geografică potenţială a incidentului; date despre efecte potenţial transfrontaliere ale incidentului și, de asemenea, că notificarea prevăzută la alin.(1) şi (2) ale art.26 nu va conţine informaţii clasificate și date care pot aduce atingere drepturilor şi libertăţilor cetăţeneşti ori intereselor legitime ale unor terţe entităţi implicate în incident, în condiţiile legii.

93. Prin urmare, Curtea constată că obligațiile reglementate prin art.25 alin.(1) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative au ca obiect operațiuni strict tehnice de natură a asigura prestarea serviciilor la care fac referire dispozițiile art.3 din legea criticată, într-un climat de securitate cibernetică. Mai mult, alin.(2) al art.25 din legea criticată prevede că datele și informațiile mai sus analizate nu vizează, prin scopul solicitării, date cu caracter personal și date de conținut. Totodată, obligațiile prevăzute la art.25 alin.(1) din legea criticată vor fi îndeplinite cu respectarea prevederilor Capitolului IX al aceleiași legi, referitoare la confidențialitatea și protecția securității datelor și informațiilor persoanelor fizice și juridice analizate anterior.

94. Asadar, legea criticată stabilește în sarcina furnizorilor de servicii tehnice de securitate cibernetică doar obligații cu caracter tehnic, menite să asigure descoperirea și sancționarea în timp util a incidentelor, amenințărilor, riscurilor sau vulnerabilităților de securitate cibernetică, obligații care exclud furnizarea către autoritățile prevăzute la art.10 din legea criticată a unor date cu caracter personal sau a unor date de conținut, prin urmare, Curtea nu poate reține pretinsa încălcare de către persoanele prevăzute la art.3 din legea analizată a obligației de confidențialitate pe care o au față de clienții lor, în condițiile în care solicitarea are ca finalitate cunoașterea, prevenirea și rezolvarea unor incidente de securitate cibernetică, ale căror efecte pot prejudicia inclusiv clienții celor care au obligația legală a notificării.

95. Pentru aceste considerente, nu poate fi reținută nici încălcarea, prin dispozițiile art.25 din legea criticată, a dreptului la viață intimă, familială și privată și nici a libertății de exprimare, astfel cum acestea sunt prevăzute la art.26 și la art.30 din Constituție.

96. Totodată, având în vedere considerentele mai sus invocate, Curtea constată că art.25 din legea supusă controlului de constituționalitate reglementează obligații ce au ca finalitate descoperirea unor faptele de natură ilicită, lato sensu. Aceste aspecte nu exclud însă obligația furnizorilor de servicii tehnice de securitate cibernetică de a sesiza organele de urmărire penală, în ipoteza în care constată comiterea unor fapte prevăzute de legea penală, precum cele incriminate în cuprinsul Capitolul VI, intitulat „Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice" al Titlului VII – „Infracțiuni contra siguranței publice" din Partea specială a Codului penal, obligație ce rezultă din prevederile art.267 din Codul penal ce reglementează omisiunea sesizării.

97. Cu privire la criticile de neconstituționalitate referitoare la dispozițiile art.41 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, potrivit cărora procesul de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare presupune aspecte complexe de securitate cibernetică ar trebui să fie implementate exclusiv de autoritățile publice și de firmele mari, conform *acquis-ului* comunitar existent, făcându-se trimitere, în acest sens, la dispozițiile Directivei (UE) 2016/1148 (Directive NIS 1) și ale Directivei (UE) 2022/2555 (Directiva NIS 2), Curtea reține că și această critică este neîntemeiată.

98. În acest sens, Curtea reține că legislația europeană în vigoare cuprinde mai multe seturi de norme orizontale ce reglementează aspecte legate de securitatea cibernetică din diferite perspective, incluzând măsuri de îmbunătățire a securității lanțului de aprovizionare digital. Astfel, Directiva (UE) 2022/2555 (Directiva NIS 2), care a abrogat Directiva (UE) 2016/1148 (Directiva NIS 1), nu impune ca procesul de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare să fie implementat doar de autorități publice și firme mari. Explicația tehnică identificată în Preambulul Directivei NIS 2, precum și în cel al Regulamentului (UE) 2019/881 – Regulamentul privind securitatea cibernetică („EU Cyber Security Act"), are în vedere faptul că produsele și sistemele moderne din domeniul tehnologiei informației și a comunicațiilor (TIC) integrează adeseori una sau mai multe tehnologii și componente terțe (cum ar fi module software, biblioteci sau interfețe de programare a aplicațiilor) sau se bazează pe acestea, dependență care ar putea cauza riscuri suplimentare pentru securitatea cibernetică, dat fiind că vulnerabilitățile prezente în componentele terțe pot afecta și securitatea produselor, a serviciilor și a proceselor TIC. Pentru aceste motive, în numeroase cazuri, identificarea și documentarea unor astfel de dependențe le permite utilizatorilor finali de produse, servicii și procese TIC să își îmbunătățească activitățile de gestionare a riscurilor de securitate cibernetică, îmbunătățind, de exemplu, gestionarea vulnerabilității în materie de securitate cibernetică și procedurile de remediere a acesteia, astfel cum rezultă din punctul 11 al Preambulului Regulamentului (UE) 2019/881 – Regulamentul privind securitatea cibernetică („EU Cyber Security Act").

99. În aceste condiții, punctul 49 al Preambulului anterior menționat prevede că politicile de securitate cibernetică eficiente ar trebui să se bazeze pe metode de evaluare a riscurilor bine puse la punct, atât în sectorul public, cât și în sectorul privat, aceste metode fiind utilizate la diferite niveluri, fără a exista o practică comună în ceea ce privește aplicarea lor eficientă. Promovarea și dezvoltarea bunelor practici pentru evaluarea riscurilor și pentru soluții interoperabile de gestionare a riscurilor în cadrul organizațiilor din sectorul public și privat sunt considerate necesare pentru a spori nivelul de securitate cibernetică din Uniunea Europeană.

100. Având în vedere cele mai sus arătate, Directiva (UE) 2022/2555 (Directiva NIS 2) prevede, la art.2 alin.(1), cu privire la domeniul său de aplicare, că dispozițiile sale se aplică entităților publice sau private de tipul celor menționate în anexa I sau anexa II ale aceleiași directive, care se califică drept întreprinderi mijlocii în temeiul art.2 din anexa la Recomandarea 2003/361/CE sau care depășesc plafoanele pentru întreprinderile mijlocii prevăzute la alineatul (1) din respectivul articol și care prestează servicii sau își desfășoară activitățile în cadrul Uniunii Europene, dar și că art.3 alin.(4) din anexa la recomandarea anterior menționată nu se aplică în sensul acestei directive. Același art.2 anterior menționat, prevede, la alin.(2), că *„indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților de tipul celor menționate în anexa I sau II, în cazul în care: (a) serviciile sunt furnizate de: (i) furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului; (ii) prestatorii de servicii de încredere; (iii) registrele de nume de domenii de prim nivel și de furnizorii de servicii de sistem de nume de domenii; (b) entitatea este singurul furnizor dintr-un stat membru al unui serviciu care este esențial pentru susținerea unor activități societale și economice critice; (c) perturbarea serviciului furnizat de entitate ar putea avea un impact semnificativ asupra siguranței publice, a securității publice sau a sănătății publice; (d) perturbarea serviciului furnizat de entitate ar putea genera un risc sistemic semnificativ, în special pentru sectoarele*

în care o astfel de perturbare ar putea avea un impact transfrontalier; (e) entitatea este critică din cauza importanței sale specifice la nivel național sau regional pentru sectorul sau tipul de servicii în cauză sau pentru alte sectoare interdependente din statul membru; (f) entitatea este o entitate a administrației publice: (i) la nivel central, astfel cum este definită de un stat membru în conformitate cu dreptul intern; (ii) la nivel regional, astfel cum este definită de un stat membru în conformitate cu dreptul intern, care, în urma unei evaluări bazate pe riscuri, furnizează servicii a căror întrerupere ar putea avea un impact semnificativ asupra activităților societale sau economice critice."

101. În acest context legislativ european, Anexa I la Directiva (UE) 2022/2555 (Directiva NIS 2), intitulată „Sectoare cu o importanță critică ridicată", prevede la pct.8, sectorul „Infrastructură digitală", în cadrul căruia enumeră următoarele categorii de subiecte de drept: furnizorii de IXP (internet exchange point), furnizorii de servicii DNS, cu excepția operatorilor de servere pentru nume primare, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii de încredere, furnizorii de rețele publice de comunicații electronice, furnizorii de servicii de comunicații electronice accesibile publicului și urnizorii de IXP (internet exchange point), la pct.9 sectorul „Gestionarea serviciilor TIC (business-to-business)", din care fac parte furnizorii de servicii gestionate și furnizorii de servicii de securitate gestionate, iar la pct.10 sectorul „Administrație publică" care cuprinde: entitățile de administrație publică din administrația centrală, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern și entitățile de administrație publică la nivel regional, astfel cum sunt definite de un stat membru în conformitate cu dreptul intern. De asemenea, Anexa II la Directiva (UE) 2022/2555 (Directiva NIS 2), intitulată „Alte sectoare de importanță critică", prevede la pct.6, sectorul „Furnizori digitali", în care sunt incluși furnizorii de piețe online, furnizorii de motoare de căutare online și furnizorii de platforme de servicii de socializare în rețea.

102. Totodată, pentru a oferi asistență entităților esențiale și entităților importante care își desfășoară activitatea în sectoarele reglementate de Directiva (UE) 2022/2555 (Directiva NIS 2) în privința gestionării adecvate a riscurilor legate de lanțul de aprovizionare și de furnizori, Directiva (UE) 2022/2555 (Directiva NIS 2) reglementează la art.21, măsuri de gestionare a riscurilor în materie de securitate cibernetică. Conform alin.(1) al art.21 anterior menționat, *„Statele membre se asigură că entitățile esențiale și entitățile importante iau măsuri tehnice, operaționale și organizatorice adecvate și proporționale pentru a gestiona riscurile la adresa securității rețelelor și a sistemelor informatice pe care entitățile respective le utilizează pentru operațiunile lor sau pentru a furniza servicii și pentru a preveni sau reduce la minimum impactul incidentelor asupra beneficiarilor serviciilor lor și asupra altor servicii";* potrivit alin.(2) al aceluiași articol *„Măsurile menționate la alineatul (1) se bazează pe o abordare multi-risc care vizează protejarea rețelelor și a sistemelor informatice, precum și a mediului fizic al acestor sisteme împotriva incidentelor [...]."*

103. Curtea a analizat și noua Propunere de Regulament - Regulamentul privind securitatea cibernetică al Parlamentului European și al Consiliului privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentului (UE) 2019/1020 și a observat că acest nou document de referință european are ca scop să faciliteze și să asigure respectarea de către furnizorii de infrastructură digitală a cerințelor lanțului de aprovizionare potrivit Directivei (UE) 2022/2555 (Directivei NIS2).

104. Având în vedere reglementările europene mai sus analizate, Curtea reține că obligațiile reglementate prin dispozițiile art.41 din legea criticată sunt în acord cu normele de drept european care le prevăd.

105. În ceea ce privește critica potrivit căreia sfera de aplicare a dispozițiilor art.41 din legea criticată este mai largă decât cea prevăzută în Directiva (UE) 2016/1148 (Directive NIS 1) și în Directiva (UE) 2022/2555 (Directivei NIS2), aspect ce implică încălcarea prin textul criticat, a dispozițiilor art.1 alin.(5) din Constituție, dar și a prevederilor constituționale ale art.26 și art.30, Curtea reține că această critică este neîntemeiată, pentru aceleași motive expuse mai sus.

106. Referitor la criticile de neconstituționalitate formulate cu privire la dispozițiile art.48 din legea analizată, Curtea reține că acestea sunt neîntemeiate pentru următoarele motive:

107. Cu privire la critica conform căreia doar noțiunea de „notificare" este definită legal la art.22 din legea criticată, printr-o normă de trimitere la dispozițiile Capitolului IV Secțiunea a 2-a din Legea nr.362/2018, în timp ce noțiunea de „comunicare completă" nu beneficiază de o definiție legală, motiv pentru care destinatarii legii nu pot cunoaște dacă raportarea unui incident constituie o „notificare" sau o „comunicare completă", Curtea reține că, potrivit prevederilor art.26 din Legea nr.362/2018, notificarea incidentelor de securitate cibernetică conține, în mod obligatoriu, următoarele date și informații: elementele de identificare ale infrastructurii și operatorului sau furnizorului în cauză; descrierea incidentului; perioada de desfăşurare a incidentului; impactul estimat al incidentului; măsuri

preliminare adoptate; lista de autorităţi ale statului afectate de incident; întinderea geografică potenţială a incidentului; date despre efecte potenţial transfrontaliere ale incidentului.

108. În aplicarea dispozițiilor Legii 362/2018, notificarea către autoritățile competente, respectiv către Directoratul Național de Securitate Cibernetică, a incidentelor de securitate cibernetică, poate fi urmată de o comunicare ulterioară a unor date suplimentare privind incidentul, această procedură implicând utilizarea unor cadre general utilizate - spre exemplu Structured Threat Information eXpression (STIX) - pentru obținerea de date și informații suplimentare tehnice privind respectivele incidente de securitate cibernetică. Conform Structured Threat Information eXpression (STIX) pot fi necesare următoarele date și informații suplimentare: calea de atac utilizată de către atacatorii cibernetici (Attack Pattern); campania de atac cibernetic (Campaign) sau setul de activități malițioase ori de atacuri cibernetice cu care incidentul este asociat; tipul de acțiuni și contramăsuri a fi luate in considerare (Course of Action); indicatorii de compromitere (IoC Indicator of compromise); infrastructura atacatorilor - descriere a sistemelor, serviciilor software și infrastructurilor TIC fizice sau virtuale folosite de atacatori ca parte a unui atac ce a produs un incident cibernetic; locația geografică în care atacul cibernetic a fost detectat sau în care incidentul a produs efecte; malware - tipul de cod/program malițios implicat; actorul implicat în amenințarea cibernetică (Threat Actor); instrumente precum aplicații, platforme, soluții software folosite pentru executarea atacului cibernetic; vulnerabilitățile implicate, etc.

109. Procedura de notificare a incidentelor cibernetice, cu toate componentele sale, este reglementată detaliat, la Capitolului IV Secțiunea a 2-a din Legeanr.362/2018, care prevede cu claritate, precizie și previzibilitate etapele și operațiunile pe care persoanele fizice și persoanele juridice care au obligația de a notifica incidentele de securitate cibernetică trebuie să le realizeze.

110. În aceste condiții, elementul material al contravenției prevăzute la art.48 alin.(1) lit.a) din legea criticată are în vedere un număr determinat și limitat de fapte, expres prevăzute de lege, motiv pentru care potențialul subiect activ al contravențiilor reglementate prin textul criticat poate să prevadă cu claritate care sunt faptele care constituie contravenție și să își adapteze conduita la exigențele legii.

111. Referitor la elementul constitutiv al contravenției prevăzute la art.48 alin.(1) lit.b) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, acesta constă în faptele de necomunicare de către persoanele fizice și juridice prevăzute la art.3 alin.(1) lit.b) și c) din lege, a incidentelor de securitate cibernetică, potrivit dispozițiilor aceleiași legi, respectiv prin intermediul Platformei naționale pentru raportarea incidentelor de securitate cibernetică (PNRISC) și în termenul prevăzut la art.21 alin.(2) și la art.22 din aceeși lege. Totodată, conform normei analizate, comunicarea trebuie să fie „completă”. Cum legislația în vigoare nu definește sintagma „comunicare completă a incidentelor de securitate cibernetică”, rezultă că aceasta are înțelesul ce rezultă din sensul uzual al termenilor care o compun, acela de comunicare integrală a acestor incidente.

112. Cu privire la elementul constitutiv al contravenției prevăzute la art.48 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, acesta constă în faptele de nerespectare de către furnizorii de servicii de securitate cibernetică a obligației de a pune la dispoziția autorităților prevăzute la art.10 din aceeași lege, a datelor și informațiilor privind incidente, amenințări, riscuri sau vulnerabilități a căror manifestare poate afecta o rețea sau sistem informatic al deținătorului sau al unor terți, în condițiile prevăzute de lege și cu respectarea termenului reglementat la art.25 alin.(1) din actul normativ criticat. Referitor la contravenția anterior menționată, Curtea constată că actul de punere la dispoziție a datelor și informațiilor prevăzute în ipoteza normei ce reglementează această contravenție se realizează, pe de-o parte, în condițiile art.25 alin.(1) din legea criticată - în ceea ce privește termenele de notificare a incidentelor și, respectiv, de comunicare a amenințărilor, a riscurilor și a vulnerabilităților - iar, pe de altă parte, în condițiile art.52 alin.(5) din aceeași lege - dispoziție ce face trimitere la hotărârea Guvernului care urmează să prevadă normele metodologice privind solicitarea și comunicarea datelor și informațiilor prevăzute la art.25 alin.(1) din legea criticată. Așadar, conduita sancționată prin dispozițiile art.48 alin.(1) lit.c) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative constă în necomunicarea, respectiv nepunerea la dispoziția autorităților prevăzute la art.10 din legea criticată, a incidentelor și, respectiv, a amenințărilor, riscurilor și vulnerabilităților, în termenele prevăzute la art.25 alin.(1) din legea analizată, în condițiile ce vor fi prevăzute prin hotărâre a Guvernului.

113. Curtea reține, totodată, că mecanismele de notificare a incidentelor de securitate cibernetică și cele de comunicare a riscurilor, amenințărilor și vulnerabilităților de securitate cibernetică asigură, în fiecare caz în parte, termene/intervale de timp determinate, cuprinse între momentul notificării incidentului și cel al comunicării datelor și informațiilor suplimentare referitoare la respectivul incident, termene care sunt stabilite astfel încât să permită oricărui subiect de drept vizat să aibă

capacitatea din punct de vedere fizic, tehnic și operațional, de a transmite autorităților competente, informațiile în cauză. Așadar, cu toate că natura unor astfel de incidente impune semnalarea lor de urgență, legea criticată prevede termene acoperitoare în scopul asigurării proporționalității între obligațiile reglementate în sarcina destinatarilor legii care intră în domeniul său de aplicare, pe de-o parte, și posibilitățile reale de notificare/comunicare a datelor și a informațiilor arătate în ipotezele normelor ce prevăd contravențiile reglementate la art.48 din legea criticată, pe de altă parte.

114. Pentru aceste considerente, Curtea reține că dispozițiile art.48 alin.(1) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative sunt clare, precise și previzibile, fiind, așadar, în acord cu exigențele ce rezultă din prevederile art.1 alin.(5) din Constituție.

115. În ceea ce privește aspectul reglementării procedurii de comunicare, respectiv de punere la dispoziție a datelor și informațiilor la care fac referire prevederile art.48 din legea analizată, printr-o hotărâre a Guvernului, ca act secundar și nu primar de legiferare, acest mod de reglementare constituie o aplicație a dispozițiilor constituționale ale art.108, ce reglementează actele Guvernului. De altfel, cele două aspecte (procedura de comunicare, respectiv de punere la dispoziție a datelor și informațiilor) reflectă o măsură cu caracter organizatoric, administrativ, iar nu substanțial. În jurisprudența sa, Curtea a statuat că „organizarea executării legii are un sens mai larg decât cea privind aplicarea legii, şi anume prin hotărâri ale Guvernului pot fi dispuse măsuri organizatorice, financiare, instituţionale sau sancţionatorii în vederea stabilirii cadrului necesar pentru ducerea la îndeplinire a dispoziţiilor legii. Aşadar, legiuitorul nu mai stabileşte întotdeauna direct, prin lege, contravenţii şi sancţiuni, ci, chiar în sensul textului constituţional invocat, această competenţă revine autorităţii publice însărcinate cu organizarea executării legii.” (a se vedea Decizia nr.107 din 22 februarie 2005, publicată în Monitorul Oficial, Partea I nr.334 din 20 aprilie 2005).

116. Referitor la criticile de neconstituționalitate formulate cu privire la dispozițiile art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, Curtea reține că acestea sunt neîntemeiate pentru următoarele considerente:

117. În ceea ce privește critica conform căreia introducerea tuturor rețelelor şi sistemelor informatice în sistemul de protecție a securităţii naţionale, mai exact în sectorul cibernetic al securităţii naţionale încalcă dreptul la viață intimă, familială și privată, precum și libertatea de exprimare, Curtea constată că soluția legislativă analizată nu vizează rețelele și sistemele informatice, în materialitatea lor, ci obiectul de interes al securității naționale îl reprezintă efectele negative produse de atacurile și amenințările cibernetice, precum și de amenințările de tip hibrid din spațiul cibernetic, care afectează capacitatea de reziliență a statului, respectiv campaniile de propagandă și dezinformare din spațiul cibernetic ce afectează ordinea constituțională. Or, cu privire la aceasta, Curtea Constituțională a statuat în jurisprudența sa că, în materia stabilirii tipurilor de amenințări la adresa securității naționale, revine legiuitorului primar sarcina de a stabili aceste amenințări, aspect care constituie o opțiune de politică de securitate națională a statului român (a se vedea Decizia nr.91 din 28 februarie 2018, paragraful 69).

118. De asemenea, printr-o jurisprudență constantă, Curtea Constituțională a reținut că „nu intră în competența sa posibilitatea de a se pronunța asupra aprecierilor, dintre care unele neavând caracter juridic, referitoare la faptul dacă legea supusă controlului de constituționalitate își poate atinge scopul pentru care a fost inițiată și adoptată, și aceasta, și chiar dacă, eventual, asemenea aprecieri ar fi îndreptățite. Curtea Constituțională nu decide dacă o lege este sau nu este bună, dacă este sau nu este eficientă sau dacă este sau nu este oportună.” (a se vedea Decizia nr.203 din 29 noiembrie 1999, publicată în Monitorul Oficial al României, Partea I, nr.603 din 9 decembrie 1999).

119. Având în vedere aceste aspecte, principalele categorii de actori care generează amenințări în spațiul cibernetic sunt prezentate în Strategia de Securitate Cibernetică a României 2022 – 2027 adoptată prin Hotărârea de Guvern nr.1321 din 30 decembrie 2021, publicată în Monitorul Oficial al României, Partea I, nr.2 din data de 3 ianuarie 2022, care face trimitere la persoane sau grupări de criminalitate organizată care exploatează vulnerabilitățile spațiului cibernetic în scopul obținerii de avantaje patrimoniale sau nepatrimoniale; la teroriști sau extremiști care utilizează spațiul cibernetic pentru desfășurarea și coordonarea unor atacuri teroriste, activități de comunicare, propagandă, recrutare și instruire, colectare de fonduri, etc., în scopuri teroriste; la state sau actori non-statali care inițiază sau derulează operațiuni în spațiul cibernetic, în scopul culegerii de informații din domeniile guvernamental, militar, economic ori al materializării altor amenințări la adresa securității naționale.

120. În considerare acestor realități și în scopul armonizării cadrului normativ incident, prin dispozițiile art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, Legiuitorul primar a introdus modificări corelative

completând lista amenințărilor la adresa securității naționale prevăzute la art.3 din Legea nr.51/1991 cu următoarele tipuri de amenințări / atacuri introduse la noile litere n) – p) ale art.3:

121. ***Art.3 lit.n) - „amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice şi de comunicații de interes național”.*** Norma introdusă la lit.n) a art.3 din Legea nr.51/1991 conține noțiuni și concepte definite în cuprinsul legii criticate sau în legislația incidentă. Astfel, noțiunea de „amenințare cibernetică” este definită la art.2 lit.b) din legea criticată, prin trimitere la dispozițiile art.2 lit.f) din Ordonanța de urgență a Guvernului nr.104/2021, iar cea de „atac cibernetic” la art.2 lit.c) din aceeași lege, ca fiind o „acțiune ostilă (de rea-credință) desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică”. La rândul său, sintagma „infrastructură informatică și de comunicații de interes național” este definită de art.2 lit.d) din Legea nr.163/2021, ca reprezentând infrastructura informatică și de comunicații esențială pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărei perturbare sau distrugere are un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții.

122. *Art.3 lit.o) - acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului român în raport cu riscurile și amenințările de tip hibrid*. În mod similar, noua prevedere de la lit.o) conține noțiuni și concepte identificate în legea criticată sau în alte legi incidente. Astfel, conceptul de „reziliență” este amplu definit în mai multe acte normative naționale, pe baza definiției „rezilienței în spațiul cibernetic”, prevăzute la art.2 lit.v) din legea criticată, conceptul fiind dezvoltat prin Hotărârea Parlamentului nr.22/2020 privind aprobarea Strategiei naționale de apărare a țării pentru perioada 2020-2024, prin Hotărârea Guvernului nr.1321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, prin dispozițiile Ordonanţei de urgenţă a Guvernului nr.155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă și prin Ordonanţa de urgenţă a Guvernului nr.124/2021 privind stabilirea cadrului instituţional şi financiar pentru gestionarea fondurilor europene alocate României prin Mecanismul de redresare şi rezilienţă, precum şi pentru modificarea şi completarea Ordonanţei de urgenţă a Guvernului nr.155/2020 privind unele măsuri pentru elaborarea Planului naţional de redresare şi rezilienţă necesar României pentru accesarea de fonduri externe rambursabile şi nerambursabile în cadrul Mecanismului de redresare şi rezilienţă.

123. Totodată, riscurile și amenințările de tip hibrid la adresa securității cibernetice sunt definite ca fiind acele riscuri și amenințări definite la art.2 lit.b) și w) din legea criticată, care se manifestă sub formă hibridă. Noțiunea de „forma hibridă a amenințărilor și riscurilor de securitate cibernetică” este conceptualizată prin Strategia națională de apărare a țării pentru perioada 2020-2024, aprobată prin Hotărârea Parlamentului nr.22/2020, mai sus citată, paragrafele 6, 8, 21, 49, 61, 71, 75, 82, 91, 92, 93, 104, 154, 158, 177, 170, 203. Totodată, amenințările militare de tip hibrid sunt descrise și enumerate în cuprinsul Hotărârii Guvernului nr.832/2021 pentru aprobarea Strategiei militare a României, la Capitolul I, lit.A și B, Capitolul II, lit.A și B, Capitolul IV și Capitolul V.

124. *Art.3 lit.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*. Autorii sesizărilor de neconstituționalitate consideră că sintagma prevăzută la art.50 din legea supusă controlului de constituționalitate cu referire la art.3 lit.p) din Legea nr.51/1991 („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”) încalcă dispozițiile art.1 alin.(5) din Constituție, fiind lipsită de claritate, precizie și previzibilitate.

125. La fel ca în cazul argumentelor aduse împotriva sintagmei reglementate de art.3 alin.(1) lit.c) analizate anterior, și în cazul acestor critici, problema de drept invocată nu vizează de fapt imprecizia, neclaritatea sau impredictibilitatea normei, ci sfera prea largă de întindere a reglementării. Or, imprecizia, neclaritatea și impredictibilitatea unei norme sau noțiuni juridice nu poate fi confundată cu sfera de întindere a respectivei noțiuni juridice. De altfel, autorul obiecției (Avocatul Poporului) precizează în sesizarea sa faptul că sfera de aplicare a dispoziției este atât de largă, încât față de orice persoană se poate reține exercitarea unei acțiuni care constituie amenințare la adresa securității naționale. Or, tocmai acest lucru denotă faptul că, în realitate, sintagma criticată nu este neclară sau imprecisă, ci faptul că, în opinia autorului sesizării de neconstituționalitate, aceasta este prea largă.

126. Pentru a lămuri semnificația sintagmei/noțiunilor supuse controlului de constituționalitate trebuie realizată deopotrivă o interpretare textualistă și una sistematică, având în vedere decelarea scopului urmărit de legiuitor.

127. În primul rând, prin interpretarea textualistă, semnificațiile noțiunilor de „propagandă” și „dezinformare” sunt cele avute în vedere prin definițiile din Dicționarul Explicativ al Limbii Române - DEX. Astfel, propaganda reprezintă pe de o parte, acțiunea desfășurată sistematic în vederea răspândirii unei doctrine politice, religioase etc., a unor teorii, opinii, pentru a le face cunoscute și acceptate, pentru a câștiga adepți, iar pe de altă parte poate consta în acțiunea de răspândire a unor idei care prezintă și susțin o teorie, o concepție, un partid politic etc, cu scopul de a convinge și de a câștiga adepți. Noțiunea de dezinformare este acțiunea de informare greșită (în mod tendențios), acțiunea de a dezinforma și rezultatul ei care semnifică a informa greșit, în mod intenționat, tendențios, a induce în eroare cu o informație falsă.

128. În al doilea rând, Curtea observă din modul de redactare a normei că nu orice campanie de propagandă sau dezinformare în spațiul cibernetic este avută în vedere de legiuitor, ci doar acele campanii de propagandă sau dezinformare de natură să afecteze ordinea constituțională. Tipul de amenințare introdus la art.3 lit.p) poate viza exclusiv acele campanii de propagandă sau dezinformare care promovează incitarea la război, la ură pe criterii de rasă, religie, naționalitate etc., la separatism teritorial sau la violenţă publică, dar și la schimbarea regimului democratic constituțional sau la desființarea unor instituții de rang constituțional. Calificarea unei acțiuni în sfera amenințărilor reglementate la lit.p) presupune întrunirea unui număr de patru condiții. Astfel, o primă condiție pentru ca o amenințare la adresa securității naționale a României să poată fi încadrată la art.3 lit.p) din Legea nr.51/1991 este aceea ca amenințarea să vină de la un stat străin sau o organizație străină sau națională; a doua condiție este aceea ca acțiunile să se deruleze sub forma unor campanii, adică a unei succesiuni organizate de acțiuni, caracterizate prin intenție, organizare și frecvență; cea de-a treia condiție impune ca acțiunile să se desfășoare în spațiul cibernetic, adică prin rețele sociale și de comunicații funcționale prin intermediul unor sisteme și rețele informatice; cea de-a patra condiție este ca acțiunile să fie de natură să afecteze ordinea constituțională.

129. În ceea ce privește noțiunea de „propagandă”, aceasta este consacrată legislativ în cuprinsul art.405 din Codul penal care incriminează propaganda pentru război, sensul acesteia fiind explicat în doctrina de drept penal, care a reținut că norma de incriminare anterior menționată are în vedere două modalități alternative de realizare a variantei tip, respectiv: propaganda pentru război și distinct, răspândirea de ştiri tendenţioase sau inventate. Astfel, *propaganda pentru război de agresiune* constă în răspândirea, în public, de idei și concepții în favoarea unui asemenea război. Potrivit art.1 din Rezoluția Adunării Generale a ONU nr.3314 din 14 decembrie 1974, prin război de agresiune se înțelege folosirea forțelor armate de către un stat sau un grup de state împotriva suveranității, integrității teritoriale sau independenței politice a altui stat sau în orice alt mod incompatibil cu Carta Națiunilor Unite. În cazul *răspândirii de ştiri tendențioase sau inventate,* suntem în prezența unei modalități de manipulare a populației în scopul creării unei psihoze a declanșării unui război de agresiune. Acestea sunt alternative şi pot apărea în practică în multe forme, de la discursuri publice sau manifestări, precum cele prilejuite de diferite competiţii sportive, la articole apărute în presa scrisă, emisiuni realizate la posturile de radio sau de televiziune. Putem întâlni, de asemenea, promovarea (...) prin mijloacele de comunicare mai moderne, precum internetul, unde reţelele de socializare reprezintă o platformă foarte potrivită pentru propagarea unor astfel de mesaje. În cazul răspândirii de ştiri tendențioase sau inventate, este necesar ca informaţiile să fie inventate, complet sau parţial, sau interpretate într-o formă diferită faţă de realitate. Mesajul (...) are o firească şi necesară dimensiune publică, propaganda fiind prin esenţa sa destinată a atinge mase mari de oameni, a influenţa comportamentul acestora, a genera reacţii puternice, a modifica sau crea tendinţe la nivel social, credinţe, opinii.

130. De asemenea, noțiunea de „propagandă” este definită legal la art.4 pct.9 din Legea nr.535/2004 privind prevenirea şi combaterea terorismului, cu modificările și completările ulterioare, ca semnificând „răspândirea în mod sistematic sau apologia unor idei, concepţii ori doctrine, cu intenţia de a convinge şi de a atrage noi adepţi”. Totodată, protejarea normelor de rang constituțional de acte de propagandă este asigurată și prin dispozițiile Legii partidelor politice nr.14/2003 care, la art.3 alin.(2) interzice absolut „partidele politice care, prin statutul, programele, propaganda de idei ori prin alte activităţi pe care le organizează, încalcă prevederile art.30 alin.(7), art.40 alin.(2) sau (4) din Constituţia României, republicată”, sancțiunea prevăzută pentru cazul constatării actelor de propagandă fiind dizolvarea partidului politic.

131. Nu în ultimul rând, noțiunea de „propagandă” se regăsește, cu sensul mai sus arătat, în cuprinsul următoarelor dispoziții legale: la art.28 din Legea nr.80/1995 privind statutul cadrelor militare, la art.53 alin.(3) și art.64 din Legea nr.47/1992, la art.45 lit.a) din Legea nr.360/2002, la art.18 alin.(2) din Legea nr.17/1990 privind regimul juridic al apelor maritime interioare, al mării teritoriale, al zonei contigue şi al zonei economice exclusive ale României și la art.15 din Legea nr.1/1998 privind organizarea și funcționarea Serviciului de Informații Externe.

132. În ceea ce privește noțiunea de „dezinformare”, aceasta a fost definită în cuprinsul documentului european denumit Comunicarea comună către Parlamentul European, Consiliul European, Consiliu, Comitetul Economic şi Social European şi Comitetul Regiunilor. Plan de acţiune împotriva dezinformării, 5 decembrie 2018. Potrivit actului european anterior menționat, prin „dezinformare” se înţelege crearea, prezentarea şi diseminarea de informaţii false sau înşelătoare, în scopul obţinerii unui câştig economic sau pentru a induce publicul în eroare în mod deliberat şi care pot provoca un prejudiciu public. Prejudiciul public include ameninţări legate de procesele democratice, precum şi de bunurile publice cum ar fi sănătatea, mediul sau securitatea cetăţenilor.

133. Totodată, noțiunea de „dezinformare” este utilizată în cuprinsul mai multor acte normative de rang primar, secundar și terțiar, respectiv la art.3 lit.c), art.8 alin.(3) și art.14 alin.(4) din Legea nr.122/2011 privind regimul armelor, dispozitivelor militare şi muniţiilor deținute de Ministerul Apărării, în cuprinsul Hotărârii Guvernului nr.548/2008 privind aprobarea Strategiei naţionale de comunicare şi informare publică pentru situaţii de urgenţă, la pct.IV și VIII ale Strategiei naţionale de comunicare şi informare publică, la art.4, art.13, art.34, art.42 și art.43 din Ordinul nr.150/138/2021 pentru modificarea şi completarea Regulamentului privind gestionarea situaţiilor de urgenţă specifice riscului nuclear sau radiologic, aprobat prin Ordinul ministrului afacerilor interne şi al preşedintelui Comisiei Naţionale pentru Controlul Activităţilor Nucleare nr.61/113/2018.

134. Nu în ultimul rând, noțiunea de „dezinformare” este definită în Codul de Practică a Uniunii Europene împotriva dezinformării, actualizat în 2022 (2022 – Strengthened Code of Practice on Disinformation), precum și în Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor privind Planul de acțiune pentru democrația europeană . Conform acesteia din urmă, „este important să se facă distincția între diferitele fenomene care sunt denumite în mod obișnuit „dezinformare” pentru a permite elaborarea unor răspunsuri politice adecvate: informarea greșită este conținut fals sau înșelător partajat fără intenție dăunătoare, deși efectele pot fi totuși dăunătoare, de ex. când oamenii împărtășesc informații false prietenilor și familiei cu bună credință; dezinformarea este conținut fals sau înșelător care este răspândit cu intenția de a înșela sau de a asigura un câștig economic sau politic și care poate cauza prejudicii publice. Operația de influență a informațiilor se referă la eforturile coordonate ale actorilor autohtoni sau străini de a influența un public țintă folosind o serie de mijloace înșelătoare, inclusiv suprimarea surselor independente de informații în combinație cu dezinformarea. Interferența străină în spațiul informațional, adesea efectuată ca parte a unei operațiuni hibride mai ample, poate fi înțeleasă ca eforturi coercitive și înșelătoare de a perturba formarea și exprimarea liberă a voinței politice a indivizilor de către un actor de stat străin sau agentul acestuia”.

135. Cu privire sensul noțiunii de „știri false”, aceasta nu este definită legal, aspect ce indică intenția legiuitorului de a-i fi conferit expresiei anterior menționate înțelesul ce rezultă din sensul uzual al cuvintelor care o compun, respectiv acela de date sau informații cu caracter de noutate care nu corespund adevărului. Același sens rezultă și din interpretarea gramaticală și teleologică a normelor juridice în cuprinsul cărora este utilizată sintagma analizată, respectiv din interpretarea dispozițiilor art.272 și art.272[1] din Legea societăților nr.31/1990, a dispozițiilor Anexei nr.1 la Hotărârea nr.539/2021 privind aprobarea Strategiei naționale pentru prevenirea şi combaterea antisemitismului, xenofobiei, radicalizării şi discursului instigator la ură, aferentă perioadei 2021-2023, şi a Planului de acţiune al Strategiei naţionale pentru prevenirea şi combaterea antisemitismului, xenofobiei, radicalizării şi discursului instigator la ură, aferentă perioadei 2021-2023, a Considerațiilor finale ale Hotărârii Guvernului nr.28/2021 pentru aprobarea Cartei albe a apărării, precum și a Hotărârii Parlamentului nr.22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024.

136. În ceea ce privește noțiunea de „ordinea constituțională”, aceasta desemnează un concept amplu descris și dezvoltat în jurisprudența Curții Constituționale, jurisprudență din care rezultă, cu claritate, precizie și previzibilitate caracteristicile, conținutul și limitele acesteia. Astfel, prin Decizia nr.611 din 3 octombrie 2017, publicată în Monitorul Oficial al României, Partea I, nr.877 din 7 noiembrie 2017, paragraful 107, Curtea a constatat că „respectarea statului de drept nu se limitează la această componentă, ci implică, din partea autorităților publice, comportamente și practici constituționale, care își au sorgintea în ordinea normativă constituțională, privită ca ansamblu de principii care fundamentează raporturile sociale, politice, juridice ale unei societăți. Altfel spus, această ordine normativă constituțională are o semnificație mai amplă decât normele pozitive edictate de legiuitor, constituind cultura constituțională specifică unei comunități naționale. Prin urmare, colaborarea loială presupune, dincolo de respectul față de lege, respectul reciproc al autorităților/instituțiilor statului, ca expresie a unor valori constituționale asimilate, asumate și promovate, în scopul asigurării echilibrului între puterile statului. Loialitatea constituțională poate fi caracterizată, deci, ca fiind o valoare-principiu intrinsecă Legii fundamentale, în vreme ce colaborarea loială între autoritățile/instituțiile statului are un rol definitoriu în implementarea Constituției”. Prin aceeași decizie, anterior citată, la paragraful 108,

Curtea a mai reținut că ordinea constituțională vizează și „respectul pentru Constituţie” care „nu poate fi limitat la executarea literală a dispoziţiilor sale operaţionale. Constituţia prin însăşi natura sa, în plus faţă de garantarea drepturilor omului, oferă un cadru pentru instituţiile statului, stabileşte atribuţiile şi obligaţiile acestora. Scopul acestor dispoziţii este de a permite buna funcţionare a instituţiilor, în baza cooperării loiale dintre acestea. Şeful statului, Parlamentul, Guvernul, sistemul judiciar, toate servesc scopului comun de a promova interesele ţării ca un întreg, nu interesele înguste ale unei singure instituţii sau ale unui partid politic care a desemnat titularul funcţiei. Chiar dacă o instituţie este într-o situaţie de putere, atunci când este în măsură să influenţeze alte instituţii ale statului, trebuie să facă acest lucru având în vedere interesul statului ca un întreg, inclusiv, ca o consecinţă, interesele celorlalte instituţii şi cele ale minorităţii parlamentare (*Avizul Comisiei de la Veneţia, precitat, paragraful 87 – s.n. Avizul privind compatibilitatea cu principiile constituţionale şi statul de drept a acţiunilor Guvernului României cu privire la alte instituţii ale statului şi Ordonanţa de urgenţă a Guvernului de modificare a Legii nr.47/1992 privind organizarea şi funcţionarea Curţii Constituţionale şi Ordonanţa de urgenţă a Guvernului de modificare şi completare a Legii nr.3/2000 privind organizarea şi desfăşurarea referendumului în România, aviz adoptat de la cea de-a 93-a Sesiune Plenară/Veneţia, 14-15 decembrie 2012*).”

137. Totodată, noțiunea de „ordine constituțională” este folosită de legiuitor și în cuprinsul normei ce reglementează infracțiunea de acțiuni împotriva ordinii constituționale prevăzute la art.397 din Codul penal. Conform doctrinei de drept penal , prin „ordine constituțională” se înțelege ordinea izvorâtă din normele și principiile constituționale de instituire a organelor statului și a modului de funcționare și de îndeplinire a atribuțiilor acestora, în scopul funcționării statului de drept și respectării și garantării drepturilor și libertăților fundamentale.Acțiunea armată și acțiunile violente desfășurate în mod clasic (în spațiu terestru, aerian sau maritim) sau mai nou, în spațiul cibernetic, dacă sunt exercitate în scopul schimbării ordinii constituționale, prezintă un pericol deosebit pentru securitatea națională, inclusiv pentru atributele fundamentale ale statului. Infracțiunea prevăzută la art.397 din Codul penal are o structură formată dintr-o variantă tip și o variantă atenuată. Astfel, *schimbarea ordinii constituționale* reprezintă orice modificare a atributelor fundamentale ale statului român (caracterul național, suveran, independent, unitar și indivizibil al statului, forma de guvernământ ori democrația constituțională. În cea de-a doua modalitate, respectiv *îngreunarea exercitării puterii de stat* presupune prin generarea unor dificultăți reale în îndeplinirea de către autoritățile statului a atribuțiilor și sarcinilor ce le revin, iar *împiedicarea exercitării puterii de stat* reprezintă punerea organelor de stat în imposibilitatea de a-și realiza atribuțiile legale și sarcinile ce le revin. Astfel, atât timp cât legea recunoaște deja ordinea constituțională ca valoare supremă ce trebuie apărată prin norme de drept penal, este firesc și logic ca și securitatea națională - care urmărește, în esență, tot apărarea ordinii constituționale prin mijloace de culegere, prelucrare, evaluare și comunicare a informațiilor - să dispună de pârghiile legale pentru a-și putea exercita această misiune.

138. În ceea ce privește noțiunea de „spațiul cibernetic”, aceasta este definită la art.2 lit.z) din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, ca fiind *„mediul virtual generat de rețelele și sistemele informatice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta”*. De asemenea, art.2 lit.c) din Ordonanța de urgență a Guvernului nr.104/2021, definește spațiul cibernetic ca *„mediul virtual, astfel cum este definit în Strategia de securitate cibernetică a României și Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, aprobat prin Hotărârea Guvernului nr.271/2013”*, în condițiile în care Strategia de securitate cibernetică a României, adoptată prin Hotărârea Guvernului nr.271/2013 descrie spațiul cibernetic ca fiind *„mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta”.*

139. Referitor la sensul verbului „a afecta”, Curtea Constituțională a reținut, în jurisprudența sa, spre exemplu, prin Decizia nr.650 din 15 decembrie 2022, publicată în Monitorul Oficial al României, Partea I, nr.1262 din 28 decembrie 2022, paragraful 49, că acesta este susceptibil de interpretări diferite, aşa cum rezultă din unele dicţionare. Din punctul de vedere al Curţii, aceasta urmează să reţină numai sensul juridic al noţiunii, sub diferite nuanţe, cum ar fi: «a suprima», «a aduce atingere», «a prejudicia», «a vătăma», «a leza», «a antrena consecinţe negative»” (a se vedea în același sens și Decizia nr.1189 din 6 noiembrie 2008, publicată în Monitorul Oficial al României, Partea I, nr.787 din 25 noiembrie 2008).

140. Cu privire la sensul sintagmei „securitate națională” din cuprinsul art.50 din legea criticată, Curtea reține că, prin Decizia nr.872 din 25 iunie 2010, Curtea a statuat că „noţiunea de securitate naţională este un concept constituţional şi că un element al acesteia îl constituie starea de echilibru şi de stabilitate economică. Prin aceeași decizie, Curtea a reținut că securitatea națională nu implică numai securitatea militară, deci domeniul *manu militari*, ci are și o componentă socială și economică,

dar și că „posibilitatea restrângerii exercițiului unor drepturi sau libertăți prevăzută de art.53 din Constituție este o prerogativă constituțională distinctă de instituirea unor măsuri excepționale (starea de urgență sau de asediu) reglementate de prevederile art.93 din Constituție (astfel, restrângerea exercițiului unor drepturi se poate dispune și în afara situațiilor reglementate la art.93 din Constituție)". De asemenea, prin Decizia nr.91 din 28 februarie 2018, Curtea a reținut că termenul de „securitate națională" este unul plurivalent și că, din perspectiva art.53, alin.(1) din Constituție, se poate vorbi de securitate militară, economică, financiară, informatică sau socială a țării. Totodată, prin Decizia nr.455 din 4 iulie 2018, paragraful 63, Curtea a constatat că securitatea rețelelor și sistemelor informatice este o chestiune care ține de securitatea națională.

141. În concluzie, prevederile art.50 din legea criticată, inclusiv sintagma criticată punctual de „campanie de propagandă sau dezinformare" nu pot fi analizate exclusiv în abstract, fără să se țină cont de elementele care determină limitele sale de interpretare. Autorii sesizărilor de neconstituționalitate identifică doi termeni din ansamblul legislativ și îi analizează în abstract, independent de elementele determinante care clarifică, prin limitare, întinderea semnificației juridice a sintagmei criticate. În considerarea acestui raționament pur abstract, autorul criticii trage concluzia inerentă că semnificația termenilor este prea largă, deci imprecisă, neclară și impredictibilă. O asemenea metodă de interpretare, care valorifică exclusiv „în abstract" o sintagmă cuprinsă într-o lege ar conduce inevitabil la concluzia că acestea sunt imprecise, neclare și impredictibile.

142. Or, Curtea Constituțională a precizat în jurisprudența sa, faptul că „analiza existenței amenințărilor la adresa securității naționale a României, în cazul dispoziției de lege criticate, trebuie să se realizeze prin corelarea formei/modalității de manifestare a activităților prevăzute de art.3 lit.f) din Legea nr.51/1991 cu scopul urmărit/valoarea lezată prin acea activitate". În cazul criticilor aduse prevederilor art.50, Curtea reține că trebuie urmată aceeași logică de interpretare trebuie si ori de câte ori se urmărește identificarea semnificației unei amenințări la adresa securității naționale. În cazul dedus judecății, sintagma „campanii de propagandă sau dezinformare" trebuie să fie corelată atât cu forma/modalitatea/condițiile de manifestare prevăzute de normă, cât și cu scopul urmărit prin lege și cu valoarea lezată prin aceste activități care este ordinea constituțională, element component al suveranității statului.

143. Așadar, nu orice campanie de propagandă sau dezinformare este avută în vedere de legiuitor, ci doar acele campanii de propagandă sau de dezinformare de o gravitate extremă, de natură să reprezinte o amenințare la adresa securității naționale, prin îndeplinirea cumulativă a condițiilor prevăzute expres de legiuitor, enunțate mai sus.

144. Ca atare, o sintagmă neclară, imprecisă și impredictibilă prin analiza sa „în abstract", independent de elementele determinate și de scopul avut în vedere, devine clară, precisă și predictibilă prin analiza elementelor care îi determină conținutul normativ, în interpretarea sistematică a acestora.

145. Având în vedere toate aceste considerente, Curtea reține că dispozițiile art.50 din legea criticată sunt clare, precise și previzibile, fiind în acord cu prevederile constituționale ale art.1 alin.(5) referitoare la calitatea legii.

146. În ceea ce privește critica invocată de autorii deputați ai sesizării de neconstituționalitate privind încălcarea dreptului la viață intimă, familială și privată prin extinderea realizată de dispozițiile art.50 din legea criticată, a sferei de aplicare a prevederilor art.3 din Legea nr.51/1991, Curtea Constituțională observă că prin conținutul normativ în vigoare al art.3 raportat la prevederile art.1 și art.2 din Legea nr.51/1991, legiuitorul nu a reglementat activități sau competențe specifice din domeniul culegerii de informații care presupun restrângerea exercițiului unor drepturi sau libertăți fundamentale ale omului. Astfel, art.1 din Legea nr.51/1991 reglementează conținutul conceptului de securitate națională a României, enumerând valorile expres ocrotite potrivit principiilor și normelor democratice statornicite prin Constituție, prin mijloacele menționate la art.2 alin.(1) – respectiv prin cunoașterea, prevenirea și înlăturarea amenințărilor interne și externe ce pot aduce atingere valorilor sus menționate. Dispozițiile art.3 în vigoare [lit.a) – m)] enumeră tipurile de amenințări la adresa securității naționale a României, asupra cărora Curtea s-a mai pronunțat în jurisprudența sa, prin Decizia nr.91/2018 și Decizia nr.802/2018. Prevederile art.3 din Legea nr.51/1991 au fost completate prin dispozițiile art.50 din legea ce fac obiectul prezentului control de constituționalitate în sensul introducerii la literele noi n) – p) a următoarelor tipuri de amenințări: *lit.n) - „amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național*"; *lit.o) - „acțiuni, inacțiuni sau stări de fapt cu consecințe la nivel național, regional sau global care afectează reziliența statului român în raport cu riscurile și amenințările de tip hibrid*"*; lit.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.* "

147. Curtea constată că în raport de argumentele invocate, critica privind afectarea unor drepturi și libertăți fundamentale nu este întemeiată întrucât legiuitorul nu a introdus la art.3 lit.n) – p)

măsuri, competențe sau activități specifice culegerii de informații care presupun restrângerea unor drepturi sau libertăți fundamentale ale omului, acestea fiind expres și limitativ reglementate la art.14 din Legea nr.51/1991. Stabilirea sferei amenințărilor la adresa securității naționale cu luarea în considerare a modului în care acestea au evoluat, s-au transformat și s-au diversificat, nu presupune în mod implicit și necesar măsuri de restrângere a exercițiului unor drepturi fundamentale. Doar măsurile prevăzute expres la art.14 restrâng drepturi si libertăți și în aceste cazuri limitativ prevăzute, legiuitorul a reglementat deopotrivă garanțiile legale prevăzute la art.15 si următoarele din Legea nr.51/19991. Astfel, reținem că art.14-24 din Legea nr.51/1991 prevăd proceduri *ex ante* și *a posteriori* care garantează evitarea oricărei ingerințe ilegale sau neautorizate în viața privată a cetățenilor, regim de protecție aplicabil în cazul oricărui tip de amenințare la adresa securității naționale, prevăzută de art.3, astfel cum a fost completat prin dispozițiile legii criticate.

148. Simpla enumerare a amenințărilor interne sau externe la adresa securității naționale nu poate afecta prin restrângere, drepturi sau libertăți fundamentale. Legiuitorul nu modifică regimul juridic al amenințărilor la adresa securității naționale, nici nu suprimă garanțiile prevăzute în vederea asigurării respectării drepturilor și libertăților fundamentale, ci doar actualizează sfera amenințărilor la realitățile actuale ale societății, urmărind ca, prin reglementarea protecției oferite de mecanismele de securitate națională să asigure, în final, funcționarea statului român și exercitarea neîngrădită a drepturilor și libertăților fundamentale ale cetățenilor.

149. Așadar, Curtea constată că stabilirea amenințărilor la adresa securității naționale prevăzute la art.3 lit.n)-p) din Legea nr.51/1991, se încadrează în marja de apreciere a statului român, noile amenințări au un scop legitim, fiind instituite ca urmare a realităților care guvernează spațiul cibernetic, realități care în lipsa unei protecții legale adecvate pot aduce atingere funcționării statului, ordinii constituționale, infrastructurilor cibernetice critice și, implicit, exercițiului drepturilor și libertăților fundamentale de către cetățenii acestuia, acestea fiind, totodată, proporționale cu scopul legii criticate, acela de asigurare a securității și apărării cibernetice a României.

150. Autorii sesizărilor de neconstituționalitate critică dispozițiile art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative și pentru motivul că aceste norme ar permite calificarea ca infracțiune de comunicare de informații false, a faptelor de exprimare a unor opinii neobediente prin raportare la acțiunile statale, a faptelor de adresare a unor întrebări incomode, a celor de formulare a unor opinii contrare politicii oficiale a statului sau a unor poziții publice contrare politicii oficiale a statului. Critica nu poate fi reținută, întrucât infracțiunea prevăzută la art.404 din Codul penal are ca element material al laturii obiective acțiunile de comunicare și de răspândire de știri, de date sau de informații false ori de documente falsificate, în condițiile în care subiectul activ al infracțiuni cunoaște caracterul fals al acestora, consecința faptelor sale trebuind să constea în punerea în pericol a securității naționale. Spre deosebire de vechea reglementare, noul Cod penal stabilește cerința ca făptuitorul să cunoască la momentul săvârșirii faptei, caracterul fals al știrilor, datelor sau informațiilor ori a documentelor falsificate pe care le comunică sau răspândește, fiind înlăturat pericolul unei răspunderi obiective, prin urmare, forma de vinovăție cu care acționează subiectul activ al infracțiunii reglementate la art.404 din Codul penal este intenția. În privința elementului material, infracțiunea prevăzută de art.404 se realizează printr-o acțiune de comunicare sau răspândire de știri, date, informații ori de documente. Comunicarea constă în prezentarea, informarea, înștiințarea uneia sau mai multor persoane asupra conținutului anumitor date, informații ori documente, iar răspândirea presupune acțiunea prin care sunt împrăștiate, difuzate, propagate știri, date, informații, cu dorința ca acestea să ajungă la cunoștința publicului. Pentru întregirea elementului material, trebuie îndeplinite două cerințe esențiale: pe de o parte, e necesar ca știrile, datele, informațiile sau documentele să fie false ori falsificate, iar făptuitorul să cunoască aceste aspecte. Pe de altă parte, se cere ca acțiunea de comunicare sau de răspândire a unor știri, date, informații false ori documente falsificate să pună în pericol securitatea națională. Așadar, știrile, datele și informațiile, precum și documente falsificate la care face referire norma de incriminare invocată de autorii sesizării sunt, în mod obiectiv false, caracter care trebuie probat pentru ca faptele avute în vedere să poată fi încadrate conform art.404 anterior menționat.

151. În considerarea argumentelor expuse mai sus, Curtea reține că faptele reglementate prin dispozițiile art.50 din Legea privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative, nu constituie, *de plano*, elementul material al laturii obiective a infracțiunii de comunicare de informații false prevăzute de art.art.404 din Codul penal, motiv pentru care dispozițiile legale criticate sunt în acord cu prevederile art.1 alin.(5) din Constituție, critica fiind neîntemeiată.

152. Pentru considerentele arătate, în temeiul art.146 lit.a) şi al art.147 alin.(4) din Constituţie, precum şi al art.11 alin.(1) lit.A.a), al art.15 alin.(1) şi al art.18 alin.(2) din Legea nr.47/1992, cu majoritate de voturi,

CURTEA CONSTITUŢIONALĂ
În numele legii
DECIDE:

Respinge, ca neîntemeiate, obiecţiile de neconstituţionalitate formulate de un număr de 57 de deputați, aparținând grupului parlamentar al USR și deputați neafiliați și, respectiv, de Avocatul Poporului şi constată că dispoziţiile art.3 alin.(1) lit.c), art.21 alin.(1), art.22, art.25, art.41, art.48 și art.50 din Legea privind securitatea și apărare cibernetică a României precum și pentru modificare și completarea unor acte normative sunt constituționale în raport cu criticile formulate.

Definitivă şi general obligatorie.

Decizia se comunică Preşedintelui României şi se publică în Monitorul Oficial al României, Partea I.

Pronunţată în şedinţa din data de 28 februarie 2023.

OPINIE SEPARATĂ

În dezacord cu opinia majoritară, considerăm că obiecțiile de neconstituționalitate referitoare la Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative trebuiau admise şi constatată neconstituţionalitatea dispozițiilor criticate pentru argumentele ce urmează a fi expuse:

I. Examinând obiecțiile de neconstituționalitate, reținem că o primă critică de neconstituționalitate se referă la lipsa de claritate și previzibilitate a dispozițiilor 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, cu următorul conținut: *„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)”.*

Cu titlu general, reținem că instanța de contencios constituțional a constatat că orice act normativ trebuie să îndeplinească anumite condiţii calitative, printre acestea numărându-se previzibilitatea, ceea ce presupune că acesta trebuie să fie suficient de precis şi clar pentru a putea fi aplicat (a se vedea, în acest sens, spre exemplu, Decizia nr.189 din 2 martie 2006, publicată în Monitorul Oficial al României, Partea I, nr.307 din 5 aprilie 2006, Decizia nr.903 din 6 iulie 2010, publicată în Monitorul Oficial al României, Partea I, nr.584 din 17 august 2010, sau Decizia nr.26 din 18 ianuarie 2012, publicată în Monitorul Oficial al României, Partea I, nr.116 din 15 februarie 2012). 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 (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).

De aceea, o lege îndeplineşte condiţiile calitative impuse atât de Constituţie, cât şi de Convenţie, numai dacă norma este enunţată cu suficientă precizie pentru a permite cetăţeanului să îşi adapteze conduita în funcţie de aceasta, astfel încât, apelând la nevoie la consiliere de specialitate în materie, el să fie capabil să prevadă, într-o măsură rezonabilă, faţă de circumstanţele speţei, consecinţele care ar putea rezulta dintr-o anumită faptă şi să îşi corecteze conduita.

Curtea, având în vedere principiul generalităţii legilor, a reţinut că poate să fie dificil să se redacteze legi de o precizie totală şi o anumită supleţe poate chiar să se dovedească de dorit, supleţe care nu trebuie să afecteze, însă, previzibilitatea legii (a se vedea, în acest sens, Decizia Curţii Constituţionale nr.903 din 6 iulie 2010, publicată în Monitorul Oficial al României, Partea I, nr.584 din 17 august 2010, şi Decizia Curţii Constituţionale nr.743 din 2 iunie 2011, publicată în Monitorul Oficial al României, Partea I, nr.579 din 16 august 2011, precum şi jurisprudenţa Curţii Europene a Drepturilor Omului cu privire la care se reţin, spre exemplu, Hotărârea din 15 noiembrie 1996, pronunţată în Cauza Cantoni împotriva Franţei, paragraful 29, Hotărârea din 25 noiembrie 1996, pronunţată în Cauza Wingrove împotriva Regatului Unit, paragraful 40, Hotărârea din 4 mai 2000, pronunţată în Cauza

Rotaru împotriva României, paragraful 55, Hotărârea din 9 noiembrie 2006, pronunţată în Cauza Leempoel & S.A. ED. Cine Revue împotriva Belgiei, paragraful 59).

Totodată, Curtea a reținut că, potrivit art.8 alin.(4) din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, „forma şi estetica exprimării nu trebuie să prejudicieze stilul juridic, precizia şi claritatea dispoziţiilor", iar, potrivit art.36 alin.(1) din acelaşi act normativ, „actele normative trebuie redactate într-un limbaj şi stil juridic specific normativ, concis, sobru, clar şi precis, care să excludă orice echivoc, cu respectarea strictă a regulilor gramaticale şi de ortografie". Curtea a constatat că, în elaborarea actelor normative, organul legislativ trebuie să se asigure că folosirea termenilor se realizează într-un mod riguros, într-un limbaj şi stil juridic, care este prin excelenţă un limbaj specializat şi instituţionalizat. În doctrină s-a arătat că precizia şi claritatea limbajului folosit în domeniul juridic se obţin din analizarea şi utilizarea cât mai adecvată a termenilor şi expresiilor, ţinând seama de semnificaţia lor în mod curent, precum şi de respectarea cerinţelor gramaticale şi de ortografie, realizându-se asigurarea unităţii terminologice a stilului juridic. Astfel, Curtea a reţinut că, deşi legiuitorul în cadrul procedurii de legiferare poate opera cu termeni de drept comun, aceştia trebuie folosiţi adecvat domeniului respectiv, numai în acest mod putându-se ajunge la respectarea unei unităţi terminologice a stilului juridic (Decizia nr.405 din 15 iunie 2016, publicată în Monitorul Oficial al României, Partea I, nr.517 din 8 iulie 2016, paragraful 47).

Având în vedere aceste considerente de principiu, urmează să analizăm în ce măsură dispozițiile criticate respectă standardul de claritate şi predictibilitate cerut de Legea fundamentală şi de Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale.

Așa fiind, reținem că din economia dispozițiilor art.3 rezultă că, în ceea ce privește securitatea cibernetică, legea criticată se adresează următorilor destinatari:

- autorităţile şi instituţiile publice din domeniul apărării, ordinii publice, securităţii naţionale, justiţiei, situaţiilor de urgenţă, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat care deţin, organizează, administrează, utilizează sau au în competenţă reţele şi sisteme informatice;
- persoanele fizice şi juridice de drept privat care dețin și utilizează reţele şi sisteme informatice în vederea furnizării de servicii de comunicaţii electronice către autorităţile şi instituţiile administraţiei publice centrale şi locale;
- autorităţile şi instituţiile administraţiei publice centrale şi locale (cu excepția celor din domeniul apărării, ordinii publice, securităţii naţionale, justiţiei, situaţiilor de urgenţă, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat) care deţin, organizează, administrează sau utilizează reţele şi sisteme informatice;
- persoanele fizice şi juridice care deţin, organizează, administrează sau utilizează reţele şi sisteme informatice și care furnizează servicii publice ori de interes public (cu excepția acelor persoane fizice/juridice care furnizează servicii de comunicaţii electronice către autorităţile şi instituţiile administraţiei publice centrale şi locale).

Reținem că autorii sesizării apreciază că în ceea ce privește această ultimă categorie, legiuitorul a reglementat o normă cu o sferă de cuprindere foarte largă, care determină încălcarea prevederilor art.1 alin.(5) din Constituție.

Pentru început, reținem că dispoziția criticată se referă la „persoane fizice şi juridice". Potrivit art.25 din Codul civil, *„subiectele de drept civil sunt persoanele fizice şi persoanele juridice"*, *„persoana fizică este omul, privit individual, ca titular de drepturi şi de obligaţii civile"*, *„persoana juridică este orice formă de organizare care, întrunind condiţiile cerute de lege, este titulară de drepturi şi de obligaţii civile"*. Referitor la persoana fizică, reținem că în Capitolul I al Titlului II din Codul civil este reglemntată capacitatea civilă a persoanei fizice. De asemenea, în ceea ce privește persoana juridică, observăm că dispozițiile incidente sunt cuprinse în Titlul IV din Codul civil. Astfel, potrivit art.188 din Codul civil *„sunt persoane juridice entităţile prevăzute de lege, precum şi orice alte organizaţii legal înfiinţate care, deşi nu sunt declarate de lege persoane juridice, îndeplinesc toate condiţiile prevăzute la art.187"*, iar dispozițiile art.187 din același act normativ prevăd că *„orice persoană juridică trebuie să aibă o organizare de sine stătătoare şi un patrimoniu propriu, afectat realizării unui anumit scop licit şi moral, în acord cu interesul general"*. Potrivit art.189 din Codul civil *„persoanele juridice sunt de drept public sau de drept privat"*.

Persoanele juridice de drept privat se pot constitui, în mod liber, în una dintre formele prevăzute de lege (potrivit art.190 din Codul civil). Pe de altă parte, potrivit art.191 alin.(1) din același act normativ, persoanele juridice de drept public se înființează prin lege, iar, potrivit alin.(2) al aceluiași articol, prin excepţie, în cazurile anume prevăzute de lege, persoanele juridice de drept public se pot înființa prin acte ale autorităţilor administraţiei publice centrale sau locale ori prin alte moduri prevăzute de lege.

În acest context, reținem că dispozițiile art.3 lit.c) teza finală din legea criticată nu fac distincţie din perspectiva destinatarilor normei între persoanele juridice de drept public sau persoanele juridice de drept privat. Or, observăm că, potrivit principiului *ubi lex non distinguit, nec nos distinguere debemus*,

atunci când legiuitorul nu face el singur distincţia între anumite elemente avute în vedere în momentul legiferării, interpretul nu poate realiza această distincţie (în acelaşi sens, Decizia nr.355 din 4 aprilie 2007, publicată în Monitorul Oficial al României, Partea I, nr.318 din 11 mai 2007; Decizia nr.305 din 12 mai 2016, publicată în Monitorul Oficial al României, Partea I, nr.485 din 29 iunie 2016). Principiul general de drept anterior menţionat este aplicabil indiferent de caracterul normei supuse interpretării sau de materia în care aceasta a fost adoptată. În acest sens, în practica judiciară s-a reţinut că „acolo unde legea nu distinge, nici interpretul nu trebuie să distingă (...), chiar dacă este în discuţie o zonă normativă specială (...). Astfel (...), formulării generale a textului îi corespunde o aplicare în aceeaşi măsură generală, neputând fi introduse distincţii dacă legea nu le încorporează" (Decizia nr.10 din 18 iunie 2012, pronunţată de Înalta Curte de Casaţie şi Justiţie - Completul competent să judece recursul în interesul legii, publicată în Monitorul Oficial al României, Partea I, nr.495 din 19 iulie 2012). În sensul celor anterior menționate, a se vedea și Decizia Curții Constituționale nr.564 din 18 septembrie 2018, publicată în Monitorul Oficial al României, Partea I, nr.66 din 28 ianuarie 2019, paragraful 25.

Așa fiind, din modalitatea de reglementare a dispozițiilor criticate reiese că legiuitorul a înțeles să includă în categoria destinatarilor legii supuse examinării toate persoanele fizice, toate persoanele juridice de drept public, precum și toate persoanele juridice de drept privat care deţin, organizează, administrează sau utilizează reţele şi sisteme informatice și care furnizează servicii publice ori de interes public.

Mai mult, se observă că legiuitorul nu a distins între modalitățile și formele de constituire ale persoanelor juridice de drept privat, astfel că, aplicând același principiu (*ubi lex non distinguit, nec nos distinguere debemus)* rezultă că acesta a avut în vedere orice formă de asociere care permite desfășurarea unor activități economice, potrivit Legii societăților nr.31/1990, republicată în Monitorul Oficial al României, Partea I, nr.1066 din 17 noiembrie 2004, sau Ordonanţei de urgenţă a Guvernului nr.44/2008 privind desfăşurarea activităţilor economice de către persoanele fizice autorizate, întreprinderile individuale şi întreprinderile familiale, publicată în Monitorul Oficial al României, Partea I, nr.328 din 25 aprilie 2008.

Cu alte cuvinte, textul criticat se adresează tuturor persoanelor fizice, persoanelor juridice de drept public, societăților în nume colectiv, societăților în comandită simplă, societăților pe acţiuni, societăților în comandită pe acţiuni, societăților cu răspundere limitată, persoanelor fizice autorizate, întreprinderilor individuale, întreprinderilor familiale.

Un alt argument în sensul celor afirmate este modalitatea de reglementare a sancțiunilor contravenționale în cazul nerespectării obligațiilor impuse prin actul normativ criticat. Astfel, potrivit art.48 alin.(1) lit.a) și b), (2), (5) și (6) din actul normativ criticat: *„(1) Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate infracțiuni potrivit legii:*

a) *nerespectarea de către persoanele prevăzute la art.3 alin.(1) lit.b) și c) a obligației de notificare a incidentelor de securitate cibernetică, prin intermediul PNRISC, în termenul prevăzut la art.21 alin.(1);*

b) *nerespectarea de către persoanele prevăzute la art.3 alin.(1) lit.b) și c) a obligației de comunicare completă a incidentelor de securitate cibernetică, prin intermediul PNRISC, în termenul și condițiile prevăzute la art.21 alin.(2) și art.22:*

(2) Prin derogare de la dispozițiile art.8 alin.(2) lit.a) din Ordonanța Guvernului nr.2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr.180/2002, cu modificările și completările ulterioare, contravențiile prevăzute la alin.(1) se sancționează astfel:

a) *cu amendă de la 5.000 lei la 50.000 lei, iar în cazul săvârșirii unei noi contravenții în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 200.000 lei;*

b) *pentru operatorii economici cu o cifră de afaceri netă de peste 1.000.000 lei, cu amendă în cuantum de până la 1% din cifra de afaceri netă, iar, în cazul săvârșirii unei noi contravenții, în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 3% din cifra de afaceri netă.*

(5) Pentru persoanele fizice autorizate, întreprinderile individuale și întreprinderile familiale, cifrei de afaceri prevăzute la alin.(2) lit.b) îi corespunde totalitatea veniturilor realizate de respectivii operatori economici în exercițiul financiar anterior sancționării.

(6) Pentru persoanele juridice nou-înființate și pentru persoanele juridice care nu au înregistrat cifra de afaceri în exercițiul financiar anterior sancționării, amenda prevăzută la alin.(2) se stabilește în cuantum de minimum unu și maximum 25 de salarii minime brute pe economie."

Întrucât textul de lege criticat prevede ca destinatari ai normei acele persoane fizice și juridice care furnizează servicii publice ori de interes public, apreciem ca fiind esențial stabilirea înțelesului noțiunilor „serviciu public" și „serviciu de interes public".

În ceea ce privește noțiunea de „serviciu public", observăm că, potrivit art.5 lit.kk) din Ordonanţa de urgenţă a Guvernului nr.57/2019 privind Codul administrativ, publicată în Monitorul Oficial al

României, Partea I, nr.555 din 5 iulie 2019, aceasta este definită ca *„activitatea sau ansamblul de activităţi organizate de o autoritate a administraţiei publice ori de o instituţie publică sau autorizată/autorizate ori delegată de aceasta, în scopul satisfacerii unei nevoi cu caracter general sau a unui interes public, în mod regulat şi continuu”*.

Potrivit art.586 din același act normativ, *„caracterul de serviciu public al unei activităţi sau al unui ansamblu de activităţi se recunoaşte prin acte normative”.* Totodată, potrivit art.589, *„autorităţile administraţiei publice centrale, prin acte normative, au competenţa de înfiinţare/organizare a structurilor responsabile pentru prestarea serviciilor publice de interes naţional”,* iar *„autorităţile administraţiei publice locale, prin acte administrative, au competenţa de înfiinţare/organizare a structurilor responsabile pentru prestarea serviciilor care răspund în principal nevoilor specifice colectivităţii locale”.*

În continuare, actul normativ precitat, reglementează la art.590 modalitățile de gestiune ale unui serviciu public, gestiunea putând fi directă sau delegată. Potrivit art.591 din Ordonanţa de urgenţă a Guvernului nr.57/2019 privind Codul administrativ, gestiunea directă este modalitatea de gestiune prin care o autoritate a administraţiei publice îşi asumă/exercită nemijlocit competenţa care îi revine cu privire la prestarea unui serviciu public potrivit legii sau actului de reglementare a serviciului public. Aceasta se poate realiza de către o autoritate a administraţiei publice, de către structurile cu sau fără personalitate juridică ale acesteia, de către societăţile reglementate de Legea societăţilor nr.31/1990, republicată, cu modificările şi completările ulterioare, cu capital social integral al statului sau al unităţii administrativ-teritoriale înfiinţate de autorităţile administraţiei publice sau alte persoane juridice de drept privat, după caz, cu respectarea prevederilor legale.

Referitor la gestiunea delegată, dispozițiile art.592 din același act normativ dispun în sensul că aceasta este modalitatea de gestiune prin care prestarea serviciului public se realizează în baza unui act de delegare şi/sau a unei autorizări din partea autorităţii administraţiei publice competente, cu respectarea prevederilor din legislaţia privind achiziţiile publice, achiziţiile sectoriale şi concesionarea de servicii, de către organismele prestatoare de servicii publice, altele decât cele prevăzute la art.591 alin.(2). Gestiunea delegată poate implica dreptul organismului prestator de servicii publice de a utiliza infrastructura aferentă serviciului delegat, printr-una dintre modalităţile prevăzute de legislaţia aplicabilă fiecărui tip de serviciu.

În continuare, în ceea ce privește înțelesul noțiunii de „serviciu de interes public”, observăm că aceasta nu beneficiază de o definiție legală nici la nivelul legii criticate, nici în cuprinsul altui act normativ. Totodată, legislația în vigoare nu impune obligația existenței unui act normativ care să definească o anumită activitate ca fiind „serviciu de interes public” și nici criteriile ce trebuie analizate pentru a ajunge la concluzia că observatorul se află în fața unui „serviciu de interes public”. Pe de altă parte, utilizarea de către legiuitor, în cuprinsul aceluiași act normativ, a celor două noțiuni – serviciu public/serviciu de interes public – denotă abordarea dihotomică a acestora. Din această perspectivă, noțiunea de „serviciu de interes public” nu poate fi privită decât ca fiind diferită de cea de „serviciu public”. Chiar dacă împrumută anumite caracteristici ale „serviciului public” sau, chiar dacă pentru a stabili înțelesul noțiunii, interpretul va face apel la reglementarea noțiunii de „serviciului public”, aceste elemente nu determină echivalența absolută a noțiunilor precizate („serviciu de interes public”/„serviciu public”).

În acest context, observăm că în unele cazuri legiuitorul a reglementat expres caracterul de serviciu de interes public al unei activități. Spre exemplu, art.3 alin.(1) din Legea nr.36/1995 a notarilor publici şi a activităţii notariale, republicată în Monitorul Oficial al României, Partea I, nr.237 din 19 martie 2018 dispune în sensul că: *„Notarul public este învestit să îndeplinească un serviciu de interes public şi are statutul unei funcţii autonome”*. Dispozițiile art.2 alin.(1) din Legea nr.188/2000 privind executorii judecătoreşti, republicată în Monitorul Oficial al României, Partea I, nr.738 din 20 octombrie 2011, prevăd că *„Executorii judecătoreşti sunt învestiţi să îndeplinească un serviciu de interes public”*. De asemenea, potrivit art.2 lit.b) din Legea nr.62/2019 privind activitatea consulară, publicată în Monitorul Oficial al României, Partea I, nr.299 din 18 aprilie 2019, serviciul consular este *„serviciul de interes public prin care, potrivit legii, misiunile diplomatice şi oficiile consulare eliberează sau procură documente oficiale ori prestează anumite formalităţi în acest scop”*. Totodată, prevederile art.10 alin.(1) din Legea nr.1/2011 a educaţiei naţionale, publicată în Monitorul Oficial al României, Partea I, nr.18 din 10 ianuarie 2011, *„În România, învăţământul este serviciu de interes public şi se desfăşoară, în condiţiile prezentei legi, în limba română, precum şi în limbile minorităţilor naţionale şi în limbi de circulaţie internaţională”.*

În ceea ce privește jurisprudența Curții Constituționale, reținem că aceasta a constatat că art.191 alin.(1) din Codul civil se referă la autorităţile şi instituţiile statului [înfiinţarea Guvernului, ministerelor, autorităţilor administrative autonome (spre exemplu, Consiliul Concurenţei), Consiliul Legislativ, Curtea Constituţională etc.], la unităţile administrativ-teritoriale, toate acestea exercitând prerogativele puterii publice, în timp ce alin.(2) al aceluiaşi text legal se referă la *operatorii economici, partidele politice etc., respectiv la persoane juridice care sunt calificate de drept public prin prisma*

scopului şi obiectului lor de activitate, prestând, spre exemplu, un serviciu de interes public/general, administrând bunuri proprietate publică etc. (a se vedea în acest sens Decizia nr.249 din 19 aprilie 2018, publicată în Monitorul Oficial al României, Partea I, nr.456 din 31 mai 2018, paragraful 55, Decizia nr.531 din 18 iulie 2018, publicată în Monitorul Oficial al României, Partea I, nr.674 din 2 august 2018, paragraful 62).

Curtea Constituțională a reținut, de asemenea, că „*registrul comerţului desfăşoară o activitate de interes public*, încredinţată Oficiului Naţional al Registrului Comerţului şi oficiilor registrului comerţului, ca autorităţi publice, la dispoziţia persoanelor interesate de situaţia economico-financiară a comercianţilor (Decizia nr.212 din 15 mai 2003, publicată în Monitorul Oficial al României, Partea I, nr.471 din 1 iulie 2003).

Totodată, instanța de contencios constitutional a reținut că dispozițiile din Legea nr.101/2006 a serviciului de salubrizare a localităţilor „au menirea de a asigura realizarea efectivă a *salubrizării localităţilor*, dincolo de voinţa fiecărui individ. Fiind un *serviciu de interes public*, ar fi inadmisibil ca acesta să fie lăsat la libera apreciere a individului, care [...] pot fi de acord sau nu ca prestarea acestui serviciu să fie realizată de un anumit operator, punând astfel în pericol sănătatea publică, valoare ocrotită la nivel constituţional de art.35” (Decizia nr.612 din 28 aprilie 2009, publicată în Monitorul Oficial al României, Partea I, nr.391 din 10 iunie 2009).

În continuare, reținem că expresia „*serviciu de interes public”* este utilizată și în materie penală, respectiv în dispozițiile art.175 alin.(2) din Codul penal. Acest text de lege asimilează funcţionarului public (în sens penal) şi persoana care exercită un serviciu de interes public pentru care a fost învestită de autorităţile publice sau care este supusă controlului ori supravegherii acestuia cu privire la îndeplinirea respectivului serviciu public. Aşadar, pentru ca o persoană să facă parte din această categorie este necesară întrunirea, în mod cumulativ, a două cerinţe obligatorii: (1) să exercite un serviciu de interes public şi (2) să fie învestită cu îndeplinirea respectivului serviciu public de către o autoritate publică sau să exercite serviciul de interes public sub controlul ori supravegherea unei autorităţi publice.

În acest context, incidentă în cauza dedusă controlului de constituționalitate este analiza efectuată în ceea ce privește prima condiție impusă de dispozițiile anterior menționate, aceea a *exercitării unui serviciu de interes public,* cu mențiunea faptului că noţiunea de „funcţionar public” în sensul legii penale are un caracter autonom.

Referitor la acest aspect, reținem că Înalta Curte de Casație și Justiție a constatat că „Analiza îndeplinirii primei cerinţe, care vizează sfera atribuţiilor persoanei, se face ţinând seama de definiţia dată serviciului de interes public în doctrina de drept administrativ. Altfel spus, trebuie observat dacă, prin realizarea serviciului, se urmăreşte satisfacerea unor nevoi de interes general şi dacă se relevă, în mod direct sau indirect, o autoritate publică. [...] sunt asimilaţi funcţionarilor publici şi persoanele fizice care exercită o profesie de interes public pentru care este necesară o abilitare specială a autorităţilor publice, aşa-numitele profesii liberale. În acest sens se constată că profesiile liberale se organizează şi se exercită numai în condiţiile legii, ale statutului profesiei şi codului deontologic şi au statutul unor funcţii autonome, care se exercită în birouri sau cabinete ori în cadrul asociaţiilor profesionale înfiinţate potrivit legii. Îndeplinirea condiţiilor prevăzute de art.175 alin.(2) din Codul penal trebuie analizată pentru fiecare categorie profesională în concret, pornind de la normele speciale ce îi reglementează statutul. În aceste condiţii se constată că *expertul tehnic judiciar* face parte din categoria funcţionarilor publici asimilaţi, reglementată de dispoziţiile art.175 alin.(2) teza întâi din Codul penal, întrucât *exercită un serviciu de interes public*-întocmirea de expertize în vederea aflării adevărului şi soluţionării cauzelor aflate pe rolul instanţelor judecătoreşti sau instrumentate de către organele de urmărire penală -, serviciu pentru care a fost învestit de către o autoritate publică (Ministerul Justiţiei) (Decizia nr.20 din 29 septembrie 2014, pronunțată de Înalta Curte de Casaţie şi Justiţie - Completul pentru dezlegarea unor chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr.766 din 22 octombrie 2014).

Totodată, Înalta Curte de Casație și Justiție a reținut că „baza naturii activităţii desfăşurate, se desprinde concluzia că *banca (instituţia de credit) cu capital integral privat reprezintă o persoană juridică abilitată să exercite un serviciu de interes public*” (Decizia nr.18 din 30 mai 2017, pronunțată de Înalta Curte de Casaţie şi Justiţie - Completul pentru dezlegarea unor chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr.545 din 11 iulie 2017)

De asemenea, Înalta Curte de Casație și Justiție a constatat că „*în cazul în care întreprinzătorul titular al unei întreprinderi individuale exercită un serviciu de interes public* care este supus controlului ori supravegherii autorităţilor publice cu privire la îndeplinirea respectivului serviciu public, acesta are calitatea de funcţionar public în accepţiunea dispoziţiilor art.175 alin.(2) din Codul penal (Decizia nr.13 din 7 mai 2020, pronunțată de Înalta Curte de Casaţie şi Justiţie - Completul pentru dezlegarea unor

chestiuni de drept în materie penală, publicată în Monitorul Oficial al României, Partea I, nr.721 din 11 august 2020).

Totodată, reținem că instanța de contencios constituțional a apreciat că „*din categoria serviciilor de interes public fac parte acele entităţi care, prin activitatea pe care o desfăşoară, sunt chemate să satisfacă anumite interese generale ale membrilor societăţii*" (Decizia nr.243 din 4 iunie 2020, publicată în Monitorul Oficial al României, Partea I, nr.718 din 10 august 2020, paragraful 16, Decizia nr.790 din 15 decembrie 2016, publicată în Monitorul Oficial al României, Partea I, nr.168 din 8 martie 2017, paragraful 16).

Așa fiind, cu excepția acelor situații calificate expres de legiuitor ca intrând în categoria unor servicii de interes public, în oricare altă situație revine destinatarului normei obligația de a analiza dacă persoana fizică sau cea juridică de drept public/privat exercită/furnizează sau nu un serviciu de interes public. Or, calificare unei activități ca fiind un „serviciu de interes public" determină automat respectarea tuturor obligațiilor prevăzute de actul normativ criticat și, implicit, sancționarea contravențională a acelor persoane care nu le respectă. Mai mult, în unele cazuri, apare ca fiind deloc facilă calificarea unei activități ca fiind un „serviciu de interes public".

Plecând de la premisa că analiza existenței „serviciului de interes public" nu comportă aspecte dificile, observăm că stabilirea destinatarilor actului normativ, potrivit art.3 lit.c) teza finală, nu a fost realizată de către legiuitor în corelaţie cu o anumită amploare a activității/serviciilor prestate/furnizate de către aceștia, a căror afectare (în sensul apariției unui incident de securitate cibernetică) să aibă vreo relevanță la nivel naţional.

Un argument în acest sens, este modalitatea de reglementare a sancțiunilor contravenționale în cazul nerespectării obligațiilor impuse prin actul normativ criticat, potrivit art.48 alin.(2) lit.b) și (5), anterior redat, care face referire la operatorii economici cu o cifră de afaceri netă de peste 1.000.000 lei, dar și la persoane fizice autorizate. Or, nu se poate afirma că activitatea tuturor persoanelor fizice, societăților în nume colectiv, societăților în comandită simplă, societăților pe acţiuni, societăților în comandită pe acţiuni, societăților cu răspundere limitată, persoanelor fizice autorizate, întreprinderilor individuale, întreprinderilor familiale, chiar calificată ca fiind un serviciu de interes public, se desfășoară întotdeauna cu o asemenea amploare încât un eventual incident de securitate cibernetică care afectează reţelele şi sistemele informatice deținute de acestea echivalează cu existența unor situaţii de pericol cu privire la infrastructuri de interes naţional.

Astfel, cu titlu exemplificativ ne vom referi la activitatea unei persoane care exercită profesia de medic veterinar. Aceasta este reglementată prin Legea nr.160/1998 pentru organizarea şi exercitarea profesiunii de medic veterinar, republicată în Monitorul Oficial al României, Partea I, nr.209 din 24 martie 2014, și este definită ca fiind o profesie liberală şi independentă, cu organizare autonomă reglementată. Potrivit art.3 alin.(1) din actul normativ precitat dispune că „profesiunea de medic veterinar are ca obiective apărarea sănătăţii animalelor, sănătăţii publice, protecţia consumatorului şi a mediului înconjurător, în scopul ameliorării efectivelor de animale, al asigurării securităţii alimentare a populaţiei, al facilitării relaţiilor comerciale şi al păstrării echilibrului ecologic". Potrivit art.7, „Profesiunea de medic veterinar se exercită în cadrul următoarelor structuri profesionale: a) reţeaua veterinară de stat; b) serviciile medicale veterinare particulare, autorizate legal; c) instituţiile de învăţământ veterinar autorizate şi acreditate sau autorizate să funcţioneze provizoriu; d) alte instituţii publice şi private". Formele de exercitare a profesiei de medic veterinar sunt reglementate în art.27 alin.(1) și 28 din Legea nr.160/1998. Potrivit acestor prevederi legale, medicii veterinari cu drept de liberă practică îşi pot desfăşura activitatea independent, atât ca persoane fizice autorizate, cât şi ca persoane juridice. Totodată, medicii veterinari de liberă practică îşi pot desfăşura activitatea fie în cabinete medicale veterinare, fie în societăţi reglementate de Legea societăţilor nr.31/1990, republicată în Monitorul Oficial al României, Partea I, nr.1066 din 17 noiembrie 2004, al căror obiect principal de activitate îl reprezintă activităţile veterinare. Totodată, prin art.31 din Legea nr.160/1998 se stabileşte că unităţile medical-veterinare cu personalitate juridică ce se înfiinţează potrivit Legii nr.31/1990 vor putea funcţiona dacă au ca obiect de activitate principal activităţile veterinare şi dacă sunt înregistrate în Registrul unic al cabinetelor medical-veterinare. Aşadar, cerinţa înregistrării în Registrul unic al cabinetelor medicale veterinară este stipulată chiar prin Legea nr.160/1998.

Referitor la exercitarea acestei profesii, Curtea Constituțională a reținut, prin Decizia nr.511 din 4 iulie 2017, publicată în Monitorul Oficial al României, Partea I, nr.788 din 4 octombrie 2017, că „animalele pot fi privite ca o parte constitutivă a unui mediu înconjurător durabil şi echilibrat ecologic, protecţia acestora fiind încorporată în cadrul mai larg al asigurării condiţiilor pentru menţinerea unei naturi sănătoase, de care să beneficieze atât generaţiile prezente, cât şi cele viitoare. Totodată, mediul înconjurător de calitate implică şi o faună sănătoasă, problemele animalelor putând afecta, în acelaşi timp, sănătatea şi siguranţa oamenilor. Grija pentru sănătatea animalelor apare, aşadar, ca o reflexie a dreptului oamenilor la ocrotirea sănătăţii, garantat la nivel constituţional prin prevederile art.34, care

instituie în sarcina statului obligaţia de a lua măsuri pentru asigurarea igienei şi a sănătăţii publice. Tratarea necorespunzătoare a unor boli ale animalelor transmisibile oamenilor sau potenţialele probleme de sănătate ale populaţiei pe care consumul de produse provenind din animale bolnave ori cărora li s-au administrat în mod iraţional anumite medicamente sunt doar câteva dintre riscurile pe care comercializarea cu amănuntul doar de către medicii veterinari a produselor menţionate în textul de lege criticat le poate evita. Activităţile pe care legiuitorul le dă în competenţa exclusivă a medicilor veterinari prezintă o importanţă deosebită, având un impact direct asupra sănătăţii animalelor şi indirect asupra celei a oamenilor. În considerarea acestor valori ce se urmăreşte a fi protejate, desfăşurarea activităţilor date de lege în competenţa medicilor veterinari necesită o pregătire teoretică şi practică specială, pe care doar persoanele care au obţinut diplomă de medic veterinar eliberată de o instituţie de învăţământ superior o pot dovedi".

Așa fiind, deși nu este definită expres, din cele anterior menționate se poate trage concluzia că un medic veteriar, care își desfășoară activitatea potrivit legislației în vigoare, furnizează servicii de interes public. Totodată, se observă că, potrivit art.27 alin.(1) din Legea nr.160/1998, medicul veterinar îşi poate desfăşura activitatea independent, ca persoană fizică autorizată (care, potrivit art.17 alin.(1) din Ordonanța de urgență a Guvernului nr.44/2008, precitată, poate desfăşura activităţile pentru care este autorizată, singură sau împreună cu cel mult 3 persoane, angajate de aceasta). Totodată, menționăm definiția dată de legiuitor reţelei şi sistemului informatic, în sensul că acestea pot fi (1) orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic sau (2) datele digitale stocate, prelucrate, recuperate sau transmise de elementele prevăzute la pct.1 şi 2 din art.3 lit.l) din Legea nr.362/2018 în vederea funcţionării, utilizării, protejării şi întreţinerii lor.

Plecând de la aceste premise, se poate observa că, un medic veterinar care îşi desfăşoară activitatea independent, ca persoană fizică autorizată (singur, fără a avea alți angajați), în mediu rural (sat/comună) și care deține un dispozitiv care asigură prelucrarea automată a datelor cu ajutorul unui program informatic (cu alte cuvinte, un calculator pe care este instalat un program informatic cu ajutorul căruia se ține evidența cazurilor) intră în categoria destinatarilor prevăzuți de dispozițiile art.3 lit.c) teza finală din actul normativ criticat.

Având în vedere aceste aspecte, apreciem că metoda de reglementare a destinatarilor actului normativ criticat este realizată într-o modalitate deficitară, prin instituirea unei sfere extrem de largi de aplicare a textului de lege criticat, ceea ce contravine art.1 alin.(5) din Constituție, care consacră principiul legalităţii.

Or, destinatarii legii trebuie să aibă o reprezentare clară, precisă şi corectă a normelor juridice aplicabile, astfel încât să îşi adapteze conduita şi să prevadă consecinţele ce decurg din nerespectarea acestora, lipsa unei reglementări predictibile în acest sens constituind premisa unei aplicări neunitare, discreţionare, în activitatea de securizare cibernetică a României (Decizia nr.17 din 21 ianuaire 2015, publicată în Monitorul Oficial al României, Partea I, nr.79 din 30 ianuarie 2015, paragraful 56).

Așa fiind, apreciem că noţiunile juridice cu care operează legea nu delimitează în mod neechivoc sfera de incidenţă a normelor cuprinse în actul supus controlului de constituţionalitate, acesta neavând un caracter precis şi previzibil, şi, prin urmare, dispoziţiile art.3 lit.c) teza finală contravin art.1 alin.(5) din Legea fundamentală.

II. O a doua critică de neconstituționalitate se referă la faptul că, 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.

În legătură cu acest aspect, observăm că, potrivit art.52 alin.(1) din actul normativ criticat, *„categoriile de persoane prevăzute la art.3 alin.(1) lit.c) se stabilesc prin hotărâre a Guvernului, inițiată de MCID, adoptată în maximum 60 de zile de la data intrării în vigoare a prezentei legi"*.

Reținem că, analizând constituționalitatea Legii privind securitatea cibernetică a României (PLX263/2014; L580/2014), prin Decizia nr.17 din 21 ianuarie 2015, precitată, paragrafele 66 – 68, Curtea a constatat că modalitatea prin care se stabilesc criteriile în funcţie de care se realizează selecţia infrastructurilor cibernetice de interes naţional şi, implicit, a deţinătorilor ICIN nu respectă cerinţele de previzibilitate, certitudine şi transparenţă.

În acest context, Curtea a constatat că „trimiterea la o legislaţie infralegală, respectiv hotărâri de Guvern, acte normative caracterizate printr-un grad sporit de instabilitate, pentru reglementarea criteriilor în funcţie de care devin incidente obligaţii în materia securităţii naţionale încalcă principiul constituţional al legalităţii, consacrat de art.1 alin.(5) din Constituţie. Opţiunea pentru o atare modalitate de reglementare apare cu atât mai nejustificată cu cât într-o materie similară, cea a identificării infrastructurilor critice naţionale, Ordonanţa de urgenţă a Guvernului nr.98/2010 stabileşte în chiar conţinutul său criteriile intersectoriale de identificare a ICN. Mai mult, prin anexa la actul normativ se

aprobă lista sectoarelor, subsectoarelor infrastructurii critice naţionale/infrastructurii critice europene (ICN/IGE) şi autorităţilor publice responsabile (energetic, tehnologia informaţiei şi comunicaţii, alimentare cu apă, alimentaţie, sănătate, securitate naţională, administraţie, transporturi, industria chimică şi nucleară, spaţiu şi cercetare). Or, în cazul Legii privind securitatea cibernetică, dispoziţiile art.19 fac trimitere la acte normative cu forţă juridică inferioară legii, identificarea ICIN realizându-se pe baza unei metodologii elaborate de Serviciul Român de Informaţii şi de Ministerul pentru Societatea Informaţională, în baza unei proceduri neprevăzute de lege, netransparente, şi deci, susceptibilă dea fi calificată arbitrară. Prin urmare, Curtea a reţinut că atât criteriile în funcţie de care se realizează selecţia infrastructurilor cibernetice de Interes naţional, cât şi modalitatea prin care se stabilesc acestea trebuie prevăzute de lege, iar actul normativ de reglementare primară trebuie să conţină o listă cât mai completă a domeniilor în care sunt incidente prevederile legale".

Având în vedere cele anterior expuse, apreciem că cele reținute de Curtea Constituțională în Decizia nr.17 din 21 ianuarie 2015, precitată, sunt aplicabile *mutatis mutandis* și în ceea ce privește cauza dedusă în prezent controlului de constituționalitate.

Astfel cum s-a demonstrat la pct.I, 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, prin care se reglementează una dintre categoriile destinatarilor actului normativ criticat nu respectă cerinţele de previzibilitate, certitudine şi transparenţă. Or, în aceste condiții, reglementarea prin art.52 alin.(1) din actul criticat a competenței Guvernului de a stabili, printr-o legislaţie infralegală - respectiv hotărâri de Guvern - categoriile de persoane prevăzute la art.3 alin.(1) lit.c) din același act normativ încalcă principiul constituţional al legalităţii, consacrat de art.1 alin.(5) din Constituţie.

În concluzie, apreciem că dispoziţiile art.52 alin.(1) din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normativ încalcă prevederile constituţionale cuprinse în art.1 alin.(5) care consacră principiul clarității și previzibilității legii.

III. O a treia critică de neconstituționalitate se referă la faptul că actul normativ criticat - art.21 alin.(1), art.22, art.24, art.29, art.37 și art.41 - 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.

Referitor la această critică, reținem că dispozițiile art.21 alin.(1), art.24, art.29 și art.37 din actul normativ criticat impun diverse obligații în sarcina persoanelor prevăzute la art.3 lit.c) teza finală din legea criticată. Astfel, aceștia 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.21 alin.(1)].

De asemenea, au obligația de a asigura reziliența în spaţiul cibernetic prin implementarea de măsuri proactive şi reactive [art.24]; *măsuri proactive* precum: (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; *măsuri reactive* precum (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.

De asemenea, potrivit art.29, 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.(1) din actul normativ criticat, iar, la declararea stărilor de alertă cibernetică, persoanele prevăzute la art.3 pun în aplicare măsurile din aceste planuri.

Totodată, 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, seminalii, precum şi alte tipuri de activităţi [potrivit art.37]. Dispozițiile art.41 dispun în sensul că, persoanele prevăzute la art.3 implementează procesele de management al riscurilor de securitate cibernetică specifice lanțului de aprovizionare. Mai mult, art.42 prevede că persoanele prevăzute la art.3 desemnează responsabili de securitate cibernetică, iar art.43 reglementează în sensul că persoanele prevăzute la art.3 dispun măsurile necesare pentru organizarea de cursuri de instruire în domeniul managementului riscurilor de securitate cibernetică specifice lanțului de aprovizionare, respectiv introducerea de teme noi în cadrul cursurilor și programelor de instruire existente.

Având în vedere analiza realizată la pct.I din prezenta opinie separată, rezultă că toate aceste obligații incumbă tuturor persoanelor prevăzute de art.3 lit.c) teza finală, adică chiar și acelor forme de asociere care au chiar un singur angajat sau care își desfășoară activitatea la o scară teritorială care nu implică nicio relevanță în ceea ce privește securitatea națională/interesul național. În concret, referindu-ne la exemplul anterior dezvoltat, rezultă că un medic veterinar care îşi desfăşoară activitatea independent, ca persoană fizică autorizată (singur, fără a avea alți angajați), în mediu rural (sat/comună) și care deține un dispozitiv care asigură prelucrarea automată a datelor cu ajutorul unui program informatic (cu alte cuvinte, un calculator pe care este instalat un program informatic cu ajutorul căruia se ține evidența cazurilor) are toate obligațiile prevăzute de dispozițiile art.21 alin.(1), art.22, art.24, art.29, art.37 și art.41 din actul normativ criticat, în cazul nerespectării acestora fiind pasibil de aplicarea unei amenzi contravenționale.

Or, Curtea a constatat anterior, prin Decizia nr.17 din 21 ianuarie 2015, precitată, paragraful 69, că „obligaţiile ce decurg din Legea securităţii cibernetice a României trebuie să fie aplicabile în exclusivitate persoanelor juridice de drept public sau privat deţinătoare sau care au în responsabilitate infrastructuri cibernetice de interes național (care includ, în baza legii, şi administraţiile publice), întrucât numai situaţiile de pericol cu privire la o infrastructură de interes naţional pot avea implicaţii asupra securităţii României, prin dimensiunea, dispersia și accesibilitatea unei astfel de infrastructuri, prin efectele economice, evaluate în funcţie de importanţa pierderilor economice şi/sau a degradării produselor sau serviciilor, prin efectele asupra populaţiei, evaluate în funcţie de impactul asupra încrederii acesteia sau perturbarea vieţii cotidiene, inclusiv prin pierderea unor servicii esenţiale. Or, dispoziţiile legale în forma supusă controlului de constituţionalitate prezintă un grad mare de generalitate, obligaţiile vizând totalitatea deţinătorilor de infrastructuri cibernetice, constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice, indiferent de importanţa acestora care poată viza interesul naţional sau doar un interes de grup ori chiar particular. Pentru a evita impunerea unei sarcini disproporţionate asupra micilor operatori, cerinţele trebuie să fie proporţionale cu riscurile la care sunt expuse reţeaua sau sistemul informatic în cauză şi nu trebuie aplicat deţinătorilor de infrastructuri cibernetice cu importanţă nesemnificativă din punctul de vedere al interesului general. Prin urmare, riscurile vor trebui identificate la nivelul entităţilor care activează în domenii esenţiale/vitale pentru buna desfăşurare a serviciilor publice naţionale, care vor decide ce măsuri trebuie adoptate pentru a atenua riscurile respective”.

Apreciem că cele statuate de către Curtea Constituțională în precedent sunt aplicabile *mutatis mutandis* și în prezenta cauză, în condițiile în care obligațiile impuse de actul normativ criticat se aplică tuturor persoanelor prevăzute de art.3 lit.c) teza finală, indiferent de dimensiunea, dispersia şi accesibilitatea rețelei și sistemului informatic deținut, organizat, administrat sau utilizat de acestea.

Așa fiind, textele criticate impun sarcini disproporţionate asupra micilor operatori, fără ca cerinţele să fie proporţionale cu riscurile la care sunt expuse reţeaua sau sistemul informatic în cauză fiind aplicate inclusiv acelor rețele și sisteme informatice cu importanţă nesemnificativă din punctul de vedere al interesului general.

Pentru motivele expuse mai sus apreciem că dispoziţiile art.21 alin.(1), art.22, art.24, art.29, art.37 și art.41 din actul normativ criticat încalcă prevederile art.1 alin.(5) din Constituţie, întrucât nu respectă cerinţele de previzibilitate, stabilitate şi certitudine.

IV. În continuare, reținem că autorii obiecțiilor formulează critici de neconstituționalitate și în ceea ce privește completarea, prin actul normativ criticat, a art.3 din Legea nr.51/1991 privind securitatea națională a României. Așa fiind, o primă critică de neconstituționalitate se referă la introducerea, în cuprinsul articolului menționat, a literei n), cu următorul conținut: *„amenințări cibernetice sau atacuri cibernetice asupra infrastructurilor informatice și de comunicații de interes național”*.

În acest context, observăm că în ceea ce privește înțelesul unor termeni și expresii legiuitorul primar a ales fie să reglementeze acest înțeles în chiar cuprinsul actului normativ criticat, fie să adopte norme de trimitere la alte acte normative.

Așa fiind, în ceea ce privește termenii și expresiile regăsite în conținutul dispoziției literei n), care completează art.3 din Legea nr.51/1991, se observă că expresia *atac cibernetic* își găsește înțelesul/definiția în chiar cuprinsul actului normativ criticat, în sensul că, potrivit art.1 lit.c), acesta reprezintă o acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică. Pe de altă parte, în ceea ce privește înțelesul/semnificația expresiei *amenințare cibernetică*, legiuitorul a ales să utilizeze o normă de trimitere, aceasta urmând să fie definită conform art.2 lit.f) din Ordonanța de urgență a Guvernului nr.104/2021 privind înființarea Directoratului Naţional de Securitate Cibernetică, publicată în Monitorul Oficial al României, Partea I, nr.918 din 24 septembrie 2021. Astfel, *amenințare cibernetică* reprezintă orice circumstanţă, eveniment sau acţiune potenţială care ar putea cauza daune sau perturbări la nivelul reţelelor şi al sistemelor informatice, precum şi la nivelul utilizatorilor unor astfel de sisteme şi al altor persoane sau care poate avea un alt fel de impact negativ asupra acestora.

În schimb, în ceea ce privește sintagma *„infrastructuri informatice și de comunicații de interes național”,* observăm că legiuitorul nu a apelat la niciuna dintre modalitățile de configurare a înțelesului termenilor utilizați (definirea în cuprinsul actului criticat/adoptarea unei norme de trimitere). Într-adevăr, se observă că o definiție a sintagmei *infrastructură informatică şi de comunicaţii de interes naţional* se poate regăsi în art.2 lit.d) din Legea nr.163/2021 privind adoptarea unor măsuri referitoare la infrastructuri informatice şi de comunicaţii de interes naţional şi condiţiile implementării reţelelor 5G, publicată în Monitorul Oficial al României, Partea I, nr.590 din 11 iunie 2021, în sensul că aceasta se referă la infrastructura informatică şi de comunicaţii esenţială pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, siguranţei, securităţii, bunăstării sociale ori economice a persoanelor şi a cărei perturbare sau distrugere are un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii.

Cu toate acestea, din modalitatea de reglementare a actului normativ criticat transpare cu evidență opțiunea legiuitorului fie de a da termenilor și expresiilor utilizate definiții/înțelesuri proprii, fie de a face trimitere expresă la cele regăsite în alte acte normative. Or, în ceea ce privește sintagma *„infrastructuri informatice și de comunicații de interes național”* se observă că legiuitorul nu a apelat la niciuna dintre cel două modalități de reglementare. Mai mult, în cuprinsul actului normativ criticat nu se face nicio trimitere la dispozițiile Legii nr.163/2021, nici punctual în cadrul vreunui articol, nici în mod general prin reglementarea unei dispoziții finale care să determine completarea prevederilor Legii privind securitatea şi apărarea cibernetică a României cu cele ale Legii nr.163/2021. În acest context, amintim că dispozițiile art.16 alin.(1) din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative dispun în sensul că *„[...] Pentru sublinierea unor conexiuni legislative se utilizează norma de trimitere”*, iar cele ale art.50 alin.(2) din același act normativ prevăd că *„dacă norma la care se face trimitere este cuprinsă în alt act normativ, este obligatorie indicarea titlului acestuia, a numărului şi a celorlalte elemente de identificare”*.

În egală măsură, se poate observa că, potrivit art.1 din Legea nr.163/2021, scopul acesteia este adoptarea *unor măsuri referitoare la autorizarea producătorilor de tehnologii, echipamente şi programe software utilizate în cadrul infrastructurilor informatice şi de comunicaţii de interes naţional, precum şi în reţelele de comunicaţii electronice prin intermediul cărora se asigură servicii de comunicaţii electronice de tip 5G*, denumite în continuare *reţele 5G*, în vederea prevenirii, contracarării şi eliminării riscurilor, ameninţărilor şi vulnerabilităţilor la adresa securităţii naţionale şi apărării ţării. Pe de altă parte, potrivit art.1 alin.(1) din actul normativ criticat, acesta *stabilește cadrul juridic şi instituţional privind organizarea şi desfăşurarea activităţilor din domeniile securitate şi apărare cibernetică, mecanismele de cooperare şi responsabilităţile instituţiilor cu atribuţii în domeniile menţionate.*

Așa fiind, rațiunea reglementării celor două acte normative este diferit, Legea nr.163/2021 axându-se pe adoptarea măsurilor aplicabile autorizării anumitor producători a căror sferă de activitate se circumscrie actului normativ precitat, pe când actul normativ criticat se axează pe organizarea şi desfăşurarea activităţilor din domeniile securitate şi apărare cibernetică, mecanismele de cooperare şi responsabilităţile instituţiilor cu atribuţii în domeniile menţionate.

Astfel, într-o interpretare comparativă, sistematică şi teleologică, rezultă că cele două acte normative au finalități diferite, care se reflectă şi în modalitatea de interpretare și aplicare a prevederilor legilor amintite, inclusiv în ceea ce privește înțelesul termenilor și expresiilor utilizate.

Un alt argument în sensul celor anterior menționate decurge tot din modalitatea diferită de reglementare și scopul diferit al celor două acte normative anterior menționate. Astfel, apreciem că Legea nr.163/2021 nu poate fi calificată ca fiind dreptul comun în materia securității şi apărării cibernetice a României pentru a putea fi aplicată chiar și în lipsa reglementării exprese a unei dispoziții de trimitere.

În egală măsură, raportul dintre cele două reglementări - Legea nr.163/2021 și actul normativ criticat – nu poate fi calificat nici ca fiind unul de tip lege generală – lege specială, situație care ar determina aplicarea legii generale (Legea nr.163/2021) în cazul în care legea specială (actul normativ criticat) nu reglementează un anumit aspect.

Așa fiind, în contextul în care expresiei *infrastructură informatică şi de comunicaţii de interes naţional* nu i se poate atribui înțelesul stabilit prin Legea nr.163/2021, aceasta nebeneficiind nici la nivelul actului normativ criticat de o definiție legală astfel încât să aibă un înţeles specific sferei de reglementare a acestuia, rezultă că intenţia legiuitorului a fost de a-i atribui, în contextul reglementării, înţelesul ce rezultă din sensul comun al termenilor care o compun (a se vedea, *mutatis mutandis*, Decizia nr.315 din 9 iunie 2020, publicată în Monitorul Oficial al României, Partea I, nr.1130 din 24 noiembrie 2020).

În sens comun, prin *infrastructură* se înțelege acel ansamblu de metode, dispozitive, obiecte, etc., utilizate împreună pentru a fi posibilă furnizarea unui serviciu. Astfel, infrastructura informatică și de comunicații reprezintă acel ansamblu care înglobează diverse aplicații (software/hardware), dispozitive (spre exemplu, servere, routere, etc.), linii de comunicaţii (fibră optică, linii satelitare) utilizate pentru a furniza servicii informatice.

În continuare, reținem că expresia *„infrastructură informatică”* este folosită de legiuitor şi în alte acte normative, de exemplu: art.9 alin.(3), (7) și (9) și art.17 alin.(3) din Legea nr.242/2022 privind schimbul de date între sisteme informatice şi crearea Platformei naţionale de interoperabilitate, publicată în Monitorul Oficial al României, Partea I, nr.752 din 27 iulie 2022; art.9 din Legea nr.135/2020 privind stabilirea datei alegerilor pentru autorităţile administraţiei publice locale din anul 2020, precum şi a unor măsuri pentru buna organizare şi desfăşurare a acestora, publicată în Monitorul Oficial al României, Partea I, nr.626 din 16 iulie 2020; art.114 alin.(3) din Legea nr.115/2015 pentru alegerea autorităţilor administraţiei publice locale, pentru modificarea Legii administraţiei publice locale nr.215/2001, precum şi pentru modificarea şi completarea Legii nr.393/2004 privind Statutul aleşilor locali, publicată în Monitorul Oficial al României, Partea I, nr.349 din 20 mai 2015; art.110 alin.(3) din Legea nr.208/2015 privind alegerea Senatului şi a Camerei Deputaţilor, precum şi pentru organizarea şi funcţionarea Autorităţii Electorale Permanente, publicată în Monitorul Oficial al României, Partea I, nr.553 din 24 iulie 2015.

Or, analizând aceste dispoziții de lege rezultă că expresia *infrastructură informatică* are în vedere atât infrastructuri cu relevanță la nivel național, cât și infrastructuri cu relevanță la nivel local sau de unitate. Astfel, în categoria *infrastructură informatică* sunt cuprinse toate acele ansambluri care au caracteristicile unei infrastructuri informatice indiferent de deținătorul acestora și de relevanța lor. Spre exemplu, art.9 alin.(3) din Legea nr.242/2022 dispune că *„Suportul tehnic al Platformei naţionale de interoperabilitate este asigurat de o infrastructură informatică dedicată, care oferă mecanisme de acces automat la toate registrele de bază sau la sistemul informatic al instituţiei sau autorităţii care deţine în administrare/gestionare registrul de bază şi care permite schimbul de date între autorităţile şi instituţiile publice sau între acestea şi persoanele juridice de drept privat, respectiv persoanele care exercită profesii liberale reglementate, în vederea asigurării interoperabilităţii sistemelor informatice pentru furnizarea serviciilor publice”;* art.17 alin.(3) din același act normativ dispune că *„Autorităţile şi instituţiile publice vor putea folosi infrastructuri informatice private în vederea conectării la Platforma Naţională de Interoperabilitate atunci când propria infrastructură nu le permite acest lucru conform standardelor de calitate stabilite prin NRRI”;* art.114 alin.(3) din Legea nr.115/2015 prevăd că *„Pentru implementarea şi funcţionarea pe durata alegerilor a Sistemului informatic de monitorizare a prezenţei la vot şi de prevenire a votului ilegal se va utiliza, de regulă, infrastructura informatică deţinută de autorităţile administraţiei publice centrale şi locale, precum şi de unităţile de învăţământ, sub coordonarea Serviciului de Telecomunicaţii Speciale”;* art.110 alin.(3) din Legea nr.208/2015 prevede că *„Pentru implementarea şi funcţionarea pe durata alegerilor a Sistemului informatic de monitorizare a prezenţei la vot şi de prevenire a votului ilegal se va utiliza, de regulă, infrastructura informatică deţinută de autorităţile administraţiei publice centrale şi locale, precum şi de unităţile de învăţământ, sub coordonarea Serviciului de Telecomunicaţii Speciale”.*

Așa fiind, având în vedere toate aceste aspecte, apreciem că expresia *infrastructură informatică* utilizată de textul de lege criticat se referă la toate infrastructurile informatice indiferent de mărimea, relevanța sau deținătorul acestora.

În ceea ce privește expresia *interes național*, reținem că aceasta nu este definită în legislație, Curtea Constituțională constatând că legiuitorul constituant a utilizat-o, Legea fundamentală făcând referire la acest concept în conținutul prevederilor art.87 alin.(1), art.90, art.135 alin.(2) lit.b) şi d), art.136 alin.(3). Curtea a constatat că noţiunea de „interes naţional” reprezintă el însuşi un concept plurivalent, care nu comportă o definiţie abstractă, ci se determină prin circumstanţierea elementelor ce îl compun. Curtea a constatat că legiuitorul trebuie să reglementeze cu atenţie sfera elementelor a căror

afectare determină existenţa unei ameninţări la adresa securităţii naţionale. Acestea, în condiţiile imposibilităţii definirii obiective, trebuie să poată fi cel puţin determinabile prin stabilirea concretă a elementelor componente. Pe de altă parte, Curtea a constatat că noţiunea de „securitate naţională" este indisolubil legată de elementele prevăzute de art.3 din Legea nr.51/1991, sfera de cuprindere a acestei noţiuni fiind determinată şi de acestea. Or, Curtea a constatat că sfera de cuprindere a noţiunii de „interese ale ţării", noțiune echivalentă din punct de vedere semantic şi cu aceeaşi sferă de cuprindere ca și cea de „ *interes național",* necesită ea însăşi identificarea elementelor ce o compun (Decizia nr.802 din 6 decembrie 2018, publicată în Monitorul Oficial al României, Partea I, nr.218 din 20 martie 2019, paragrafele 72 și 73).

Cu alte cuvinte, utilizarea de către legiuitor a noțiunii de „interes național" determină în sarcina acestuia obligația reglementării elementelor la care cel chemat să interpreteze și să aplice legea trebuie să se raporteze pentru a determina sfera de cuprindere a acestei noţiuni.

Or, în ceea ce privește dispoziția de lege criticată, pe de-o parte, astfel cum anterior s-a arătat, expresia *infrastructură informatică* se referă la toate infrastructurile informatice indiferent de mărimea, relevanța sau deținătorul acestora, iar, pe de altă parte, legiuitorul nu a reglementat elementele necesare determinării sferei de cuprindere a noțiunii de interes național în materia analizată.

Mai mult, cum anterior s-a demonstrat, determinarea conţinutului unei astfel de noțiuni nu poate fi realizată nici prin coroborarea anumitor dispoziţii legislative. Astfel, conţinutul şi limitele sintagmei *„infrastructurilor informatice și de comunicații de interes național"* rămân la libera apreciere a organului abilitat să aplice legea, în/din această categorie putând fi, astfel, introduse sau excluse elemente, care nu pot fi cunoscute de destinatarul normei. Caracterul larg 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.

Aşadar, apreciem că dispoziţiile criticate nu instituie reguli clare pentru a oferi destinatarilor normei o indicaţie adecvată cu privire la circumstanţele şi condiţiile care determină existența unei amenințări la adresa securității naționale.

În concluzie, apreciem că dispoziţiile art.50 din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normativ, cu referire la introducerea literei n) în articolul 3 din Legea nr.51/1991 privind securitatea naţională a României, încalcă prevederile constituţionale cuprinse în art.1 alin.(5) care consacră principiul clarității și previzibilității legii.

V. O a doua critică de neconstituționalitate în ceea ce privește completarea art.3 din Legea nr.51/1991 privind securitatea națională a României, se referă la introducerea, în cuprinsul articolului menționat, a literei o), cu următorul conținut: *„acţiuni, inacţiuni sau stări de fapt cu consecinţe la nivel naţional, regional sau global care afectează reziliența statului în raport cu riscurile şi ameninţările de tip hibrid".* Referitor la expresia *„reziliența statului",* observăm că termenul „reziliență" provine din cuvântul francez *résilience,* care, potrivit Dicționarului Larousse (www.larousse.fr) are, printre altele, înțelesul comun de „capacitate a unui sistem de a continua să funcționeze chiar și în cazul unei defecțiuni".

Pe de altă parte, art.2 lit.w) din actul normativ criticat dispune că *reziliența în spaţiul cibernetic* reprezintă capacitatea unei reţele sau sistem informatic de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate de dinaintea incidentului sau atacului cibernetic. Așa fiind, rezultă că *reziliența statului* reprezintă capacitatea acestuia de a rezista unui incident de o anumită natură, de a funcționa pe durata incidentului și ulterior acestuia și de a reveni la starea de dinaintea incidentului.

În ceea ce privește expresia *„ameninţările de tip hibrid",* reținem că aceasta nu beneficiază de o definiție în cuprinsul textului de lege criticat, nefiind regăsită, de altfel, vreo definiție nici în alt act normativ. Într-adevăr, se observă că în Hotărârea Guvernului nr.832/2021 pentru aprobarea Strategiei militare a României, publicată în Monitorul Oficial al României, Partea I, nr.781 din 13 august 2021, precum și în Hotărârea Parlamentului nr.22/2020 privind aprobarea Strategiei Naţionale de Apărare a Ţării pentru perioada 2020-2024, publicată în Monitorul Oficial al României, Partea I, nr.574 din 1 iulie 2020, se fac anumite referiri la termenul „hibrid", fără însă a se putea discerne asupra înțelesului exact al noțiunii în cauză. Astfel, în cele două acte regăsim referiri la „amenințări de tip hibrid", „strategii şi tactici hibride", „strategii şi acţiuni hibride", „operaţii hibride", „amenințări hibride", „mediul hibrid", „provocări de tip hibrid", „caracter hibrid", „instrumentar hibrid", „ofensive cu caracter hibrid", etc.

Așa fiind, în analiza noastră vom porni de la definiția termenului comun „hibrid", regăsită în Dicționarul explicativ al limbii române, potrivit acestuia noțiunea în cauză având semnificația *„provenit din încrucișarea a doi indivizi de specii, de soiuri, de genuri sau de rase diferite; (despre realizări, idei, fapte) alcătuit din elemente disparate; lipsit de armonie".*

Din aplicarea acestei definiții la materia securității și apărării cibernetice și la cea a securității naționale, având în vedere sfera/domeniul de aplicare a reglementărilor adoptate în materiile anterior menționate, rezultă că *„elementele de tip hibrid”* comportă, în mod abstract, aspecte multidimensionale, care pot avea naturi diferite, care îmbină (asociază) acțiuni (măsuri) constrângătoare (opresive) și/sau subversive (perturbatoare/destabilizatoare), și care utilizează atât instrumente și tactici convenționale, cât și unele neconvenționale. Așa fiind, apreciem că *„amenințările de tip hibrid”* sunt definite de aceleași caracteristici abstracte, pe lângă care se adaugă scopul pentru care acestea sunt întreprinse, acela de a destabiliza.

În acest context, observăm că instanța de contencios constituțional a apreciat că există concepte pentru care oferirea unei definiţii abstracte, atotcuprinzătoare este un deziderat imposibil de realizat. Aceasta deoarece, în funcţie de materia în legătură cu care acesta este analizat, elementele luate în considerare vor fi diferite (Decizia nr.551 din 13 iulie 2017, publicată în Monitorul Oficial al României, Partea I, nr.977 din 8 decembrie 2017, paragraful 28). Plecând de la aceste premise, Curtea a constatat că în ceea ce privește acestea concepte, dispozițiile Legii fundamnetale nu vor fi încălcate în măsura în care, deși nu este oferită o definiție, sunt reglementate criterii exprese pe baza cărora se poate determina elementele ce aparțin/nu aparțin acestora și, implicit, se poate stabili sfera de cuprindere a acestora (a se vedea *mutatis mutandis* Decizia nr.104 din 23 februarie 2021, publicată în Monitorul Oficial al României, Partea I, nr.583 din 9 iunie 2021, paragrafele 34 și 35).

Cu alte cuvinte, utilizarea de către legiuitor a unor astfel de concepte naște în sarcina acestuia obligația unei reglementări exprese și cât mai riguroase a criteriilor aplicabile în scopul determinării sferei de cuprindere a noțiunilor/expresiilor folosite.

Având în vedere aceste aspecte, reținem că în ceea ce privește expresia *„amenințările de tip hibrid”* legiuitorul nu a reglementat o definiție a acestui concept. Mai mult, nici în cuprinsul actului normativ criticat și nici în cel al Legii nr.51/1991, act normativ care se dorește a fi completat, nu sunt reglementate nici criterii exprese pe baza cărora destinatarii normei să poată determina acele elemente care capătă caracteristicile unei amenințări de tip hibrid, neputându-se determina nici limita de aplicare a dispoziţiei de lege criticate.

Totodată, apreciem că nici din coroborarea legislaţiei incidente nu se pot desprinde reperele unei astfel de analize, simpla utilizare în diverse acte normative/administrative cu caracter normativ a termenului „hibrid”, fără însă vreo circumstanțiere, nu este suficientă pentru determinarea sferei de incidență a expresiei *„amenințările de tip hibrid”*.

Tocmai gradul sporit de generalitate al conceptului de *„amenințări de tip hibrid”*, multitudinea elementelor care singure sau împreună determină această proprietate „hibridă” a amenințării, precum și caracteristicile diferite/multidimensionale ale acestor elemente determină necesitatea unei reglementări clare din partea legiuitorului. Curtea a statuat că, în primul rând, legiuitorului îi revine obligaţia, ca, în actul de legiferare, indiferent de domeniul în care îşi exercită această competenţă constituţională, să dea dovadă de o atenţie sporită în respectarea principiului clarităţii şi previzibilităţii legii (Decizia nr.405 din 15 iunie 2016, publicată în Monitorul Oficial al României, Partea I, nr.517 din 8 iulie 2016, paragraful 52).

Or, caracterul larg 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.

În concluzie, apreciem că dispoziţiile art.50 din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normativ, cu referire la introducerea literei o) în articolul 3 din Legea nr.51/1991 privind securitatea naţională a României, încalcă prevederile constituţionale cuprinse în art.1 alin.(5) care consacră principiul clarității și previzibilității legii.

VI. O a treia critică de neconstituționalitate în ceea ce privește completarea art.3 din Legea nr.51/1991 privind securitatea națională a României, se referă la introducerea, în cuprinsul articolului menționat, a literei p), cu următorul conținut: *„acţiuni derulate de către o entitate statală sau nonstatală, prin realizarea, în spaţiul cibernetic, a unor campanii de propagandă sau dezinformare, de natură a afecta ordinea constituţională”*.

Pentru început, reținem că singura expresie ce beneficiază de o definiție legală, în chiar cuprinsul actului normativ criticat, este cea de „spațiu cibernetic”, dispozițiile art.2 lit.z) definindu-l ca *„mediul virtual generat de reţelele şi sistemele informatice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta”.* Spre deosebire de aceasta, în cazul expresiilor *„entitate statală”*, *„entitate nonstatală”*, *„campanii de propagandă”* și *„campanii de dezinformare”* legiuitorul nu a reglementat vreo definiție legală, și nici nu a adoptat vreo dispoziție în

legătură cu acestea pe baza căreia să se poată discerne eventuale caracteristici/aspecte care caracterizează termenii/noțiunile utilizate.

În ceea ce privește claritatea și previzibilitatea acestor expresii, reiterăm cele expuse anterior în sensul că legiuitorul nu a apelat nici în acest caz la vreuna dintre modalitățile de configurare a înțelesului termenilor utilizați (definirea în cuprinsul actului criticat/adoptarea unei norme de trimitere). Mai mult, în cuprinsul actului normativ criticat nu se face nicio trimitere la dispoziții ale altor acte normative care ar putea avea relevanță în definirea acestor expresii, nici punctual în cadrul vreunui articol, nici în mod general prin reglementarea unei dispoziții finale care să determine completarea prevederilor Legii privind securitatea şi apărarea cibernetică a României cu dispoziții din alte acte normative.

Așa fiind, din această perspectivă, apreciem că se păstrează și în acest caz viciul de neconstituționalitate în sensul lipsei de claritate și previzibilitate al expresiilor și termenilor utilizați.

Într-adevăr, potrivit jurisprudenței Curții Constituționale, în cazul în care expresia utilizată nu beneficiază de o definiție legală, rezultă că intenţia legiuitorului a fost de a-i atribui, în contextul reglementării, înţelesul ce rezultă din sensul comun al termenilor care o compun (a se vedea, *mutatis mutandis*, Decizia nr.315 din 9 iunie 2020, publicată în Monitorul Oficial al României, Partea I, nr.1130 din 24 noiembrie 2020).

Din această perspectivă, observăm că, potrivit Dicționarului explicativ al limbii române, *propagandă* reprezintă aceea „acțiune desfășurată sistematic în vederea răspândirii unei doctrine politice, religioase etc., a unor teorii, opinii, pentru a le face cunoscute și acceptate, pentru a câștiga adepți”, iar *dezinformare* reprezintă „faptul de a dezinforma”, adică de „a informa (în mod intenționat) greșit”.

Plecând de la premisa că în cazul acestor termeni va fi avut în vedere sensul comun atribuit lor, observăm însă că pentru a constata existența unei propagande sau a unei dezinformări nu este suficientă o simplă constatare formală din partea celui chemat să aplice legea. Din contră, pentru a constata existența unei propagande sau a dezinformării persoana îndrituită va fi obligată să realizeze o analiză de fond a situației, a aspectelor implicate, a corectitudinii informațiilor diseminate, a formei de vinovăție cu care se acționează, a plasării în cadrul constituțional a doctrinelor, teoriilor, opiniilor emise, etc.

Or, deși definirea *in abstracto* a termenilor utilizați se poate realiza prin diverse procedee, inclusiv prin apelarea la sensul comun al acestora, în unele cazuri, în funcție de materia în care aceștia sunt reglementați, acest lucru nu este suficient pentru a respecta exigențele constituționale de claritate și previzibilitate. Astfel, în unele cazuri intervine necesitatea reglementării exprese și riguroase a criteriilor/trăsăturilor care trebuie îndeplinite pentru ca unei anumite acțiuni să i se poată atribui o anumită caracteristică.

Astfel, în cazul supus controlului de constituționalitate, deși termenilor *propagandă* și *dezinformare* li se pot atribui sensul comun, nereglementarea unor criterii/trăsături exprese pe care destinatarul normei să le poată aplica pentru a putea realiza o analiză concretă și corectă/obiectivă a acțiunilor întreprinse în scopul stabilirii existenței propagandei și/sau dezinformării lasă la îndemâna acestuia stabilirea criteriilor/trăsăturilor care trebuie îndeplinite. Or, în acest caz destinatarul normei este acela care va stabili singur criteriile/trăsăturile, de la caz la caz, printr-o apreciere care nu poate fi decât una subiectivă şi, în consecinţă, discreţionară.

În concluzie, apreciem că dispoziţiile art.50 din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normativ, cu referire la introducerea literei p) în articolul 3 din Legea nr.51/1991 privind securitatea naţională a României, încalcă prevederile constituţionale cuprinse în art.1 alin.(5) care consacră principiul clarității și previzibilității legii.

Având în vedere aceste aspecte observăm că, potrivit art.13 lit.f) din Legea nr.51/1991, în situaţiile prevăzute la art.3 din acelaşi act normativ, organele cu atribuţii în domeniul securităţii naţionale pot, în condiţiile legii privind organizarea şi funcţionarea acestora, să efectueze activităţi specifice culegerii de informaţii care presupun restrângerea exerciţiului unor drepturi sau al unor libertăţi fundamentale ale omului, desfăşurate cu respectarea prevederilor legale, inclusiv interceptarea şi înregistrarea comunicaţiilor electronice, efectuate sub orice formă.

Or, având în vedere aceste aspecte şi caracterul intruziv al activităţilor specifice culegerii de informaţii care presupun restrângerea exerciţiului unor drepturi sau al unor libertăţi fundamentale ale omului, Curtea a constatat că este obligatoriu ca acestea să se realizeze într-un cadru normativ clar, precis şi previzibil, atât pentru persoana supusă acestei măsuri, cât şi pentru organele de urmărire penală şi pentru instanţele de judecată. În caz contrar, s-ar ajunge la posibilitatea încălcării într-un mod aleatoriu/abuziv a drepturilor fundamentale, esenţiale într-un stat de drept, privind viaţa intimă, familială şi privată, precum şi secretul corespondenţei. Este îndeobşte admis că drepturile prevăzute la art.26 şi art.28 din Constituţie nu sunt absolute, însă limitarea lor trebuie să se facă cu respectarea dispoziţiilor

art.1 alin.(5) din Legea fundamentală, iar gradul de precizie a termenilor şi noţiunilor folosite trebuie să fie unul ridicat, dată fiind natura măsurilor intruzive reglementate (a se vedea, în acelaşi sens, Decizia nr.51 din 16 februarie 2016, precitată, paragraful 48).

În concluzie, apreciem că instanța de contencios constituțional trebuia să admită obiecțiile de neconstituționalitate și să constate că dispozițiile art.50 din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative sunt neconstituționale.

Având în vedere toate argumentele expuse, apreciem că instanța de contencios constituțional trebuia să admită obiecțiile de neconstituționalitate și să constate că dispozițiile art.3 lit.c) teza finală, art.21 alin.(1), art.22, art.24, art.29, art.37, art.41, art.50 și art.52 alin.(1) din Legea privind securitatea şi apărarea cibernetică a României precum şi pentru modificarea şi completarea unor acte normative sunt neconstituționale.

JUDECĂTORI,

GHEORGHE STAN
ATTILA VARGA