

DECIZIA nr.17
din 21 ianuarie 2015

**asupra obiecției de neconstituționalitate a dispozițiilor Legii privind
securitatea cibernetică a României**

Augustin Zegrean	- președinte
Valer Dorneanu	- judecător
Toni Greblă	- judecător
Petre Lăzăroiu	- judecător
Mircea Ștefan Minea	- judecător
Daniel Marius Morar	- judecător
Mona-Maria Pivniceru	- judecător
Puskás Valentin Zoltán	- judecător
Tudorel Toader	- judecător
Mihaela Senia Costinescu	- magistrat-asistent șef

1. Pe rol se află pronunțarea asupra obiecției de neconstituționalitate a dispozițiilor Legii privind securitatea cibernetică a României, obiecție formulată de un număr de 69 de deputați aparținând Grupului parlamentar al Partidului Național Liberal din Camera Deputaților.

2. Cu Adresa nr.2/6103 din 23 decembrie 2014, Secretarul general al Camerei Deputaților a transmis Curții Constituționale sesizarea de neconstituționalitate, care a fost înregistrată la Curtea Constituțională sub nr.6188 din 23 decembrie 2014 și constituie obiectul Dosarului nr.1419A/2014. La sesizare a fost anexată, în copie, Legea privind securitatea cibernetică a României.

3. **În motivarea obiecției de neconstituționalitate**, autorii susțin că dispozițiile legale sunt contrare art.1 alin.(3) și (4) referitor la statul de drept și obligația respectării Constituției și a legilor. Se apreciază că legea criticată introduce multe confuzii și condiționări pentru deținătorii de infrastructuri cibernetică care sunt de natură a genera restrângeri ale drepturilor și libertăților fundamentale ale cetățenilor. Prevederile legale nu respectă dispozițiile art.6 din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea

actelor normative și încalcă, astfel, principiul legalității, care este fundamental pentru buna funcționare a statului de drept. La art.1 din lege se prevăd doar obligații pentru deținătorii de infrastructuri cibernetice fără a se stabili și drepturile acestora. Enumerarea cuprinsă în art.2 a persoanelor/entităților cărora li se aplică legea nu este una precisă, omițând să prevadă situația intermediarilor de infrastructuri cibernetice, a infrastructurilor neoperaționale, a acționarilor unor persoane juridice sau cea a fondatorilor unor asociații sau fundații care dețin astfel de infrastructuri.

4. Autorii sesizării susțin că legea are probleme fundamentale de concepție, propunând o serie de măsuri cu efect limitativ asupra dreptului prevăzut de art.26 alin.(1) din Constituție privind viața intimă, familială și privată, și încalcă în mod evident reglementările europene aflate în dezbatere referitoare la securitatea informației în domeniul digital.

5. În temeiul legii criticate, autorii obiecției de neconstituționalitate susțin că se restrâng drepturi și libertăți ale cetățenilor prin permiterea accesului la o infrastructură cibernetică și la datele conținute de aceasta în urma unei simple solicitări motivate a instituțiilor nominalizate de lege, comunicate deținătorilor de infrastructuri, fără aprobarea prealabilă a unui judecător, așa cum prevede Codul de procedură penală sau jurisprudența Curții Constituționale, în Deciziile nr.440/2014 și nr.461/2014, fapt ce determină încălcarea prevederilor constituționale cuprinse în art.23 alin.(1) referitor la inviolabilitatea libertății individuale și a siguranței persoanei și în art.28 privind secretul corespondenței.

6. Pe de altă parte, se arată că prin dispozițiile art.10 din lege Serviciul Român de Informații este desemnat autoritate națională în domeniul securității cibernetice, calitate în care asigură coordonarea tehnică, organizarea și executarea activităților ce privesc securitatea cibernetică a României. În vreme ce Uniunea Europeană propune în proiectul de Directivă NIS (Network and Information System) ca instituțiile care se ocupă de domeniul securității cibernetice să fie „organisme civile, care să funcționeze integral pe baza

controlului democratic, și nu ar trebui să desfășoare activități în domeniul informațiilor”, Parlamentul României acordă acces nelimitat și nesupravegheat la toate datele informatice deținute de persoane de drept public și privat unor instituții care nu îndeplinesc niciuna din condițiile de mai sus. Faptul că în jurisprudența recentă a Curții Constituționale, aceasta a declarat neconstituționalitatea a două legi care, în esență, încălcau aceleași drepturi ca și legea supusă în prezent controlului, constituie un motiv serios pentru o dezbatere reală a implicațiilor Legii securității cibernetice și, într-un cadru mai larg, a echilibrului dintre drepturile individuale și securitatea națională pe care România trebuie să îl asigure prin sistemul său legal. Autorii sesizării susțin că posibilitatea accesării fără mandat judecătoresc a datelor electronice provenind de la orice computer, indiferent de proprietarul său, este o ingerință nejustificată în dreptul la protecția corespondenței, adică în dreptul la viață privată, drept garantat de art. 26 și 28 din Constituție. O astfel de ingerință nu numai că nu este necesară într-o societate democratică, dar ea are tocmai efectul contrar: subminează esența societății democratice. Astfel, sub pretextul protecției împotriva atacurilor cibernetice, orice fel de date pot fi accesate la bunul plac al puterii executive, fără existența vreunui control al societății civile.

7. În sesizarea de neconstituționalitate, se arată că art.148 alin.(2) din Constituție este, de asemenea, încălcat prin netranspunerea corectă a reglementărilor comunitare în materie. Astfel, prevederile art.17 alin.(1) lit.a) nu sunt conforme cu jurisprudența Curții de Justiție a Uniunii Europene, întrucât nu precizează exact ce date sunt necesare a fi deținute, iar cadrul în care se solicită aceste date nu prezintă suficiente garanții procesuale. Pentru îndeplinirea acestei obligații este necesară o monitorizare perpetuă a tuturor persoanelor, aspect ce creează o sarcină disproporționată pentru subiecții vizați și implică totodată încălcarea drepturilor persoanelor monitorizate fără să existe în legătură cu acestea o suspiciune relativă la comiterea vreunei infracțiuni. Se mai arată că legea contravine din multe puncte de vedere și propunerii de Directivă NIS (Network & Information Security) care are ca scop protecția datelor personale

ale cetățenilor, iar nu crearea de noi atribuții pentru serviciile secrete. „În timp ce Directiva NIS are drept scop protejarea sistemelor informatice și a datelor informatice ale cetățenilor, legea, în forma adoptată, reprezintă un cec în alb care poate fi folosit de serviciile de informații pentru a controla orice persoană de drept privat (S.R.L., S.A., P.F.A., O.N.G.) care deține un sistem informatic (adică orice calculator sau smart-phone). Potențialul pentru abuzuri este, astfel, enorm. Acesta decurge din nenumăratele ambiguități prezente în lege, începând de la definirea vagă a deținătorilor de sisteme informatice și continuând cu obligațiile ce le revin celor care cad sub incidența legii.”

8. În concluzie, autorii obiecției de neconstituționalitate apreciază că „întreaga arhitectură a actului normativ este de natură a permite încălcarea drepturilor fundamentale ale omului, fără a exista un remediu eficient împotriva unor astfel de încălcări”. Deși într-o societate democratică limitele protecției drepturilor fundamentale pot fi reduse în cazul unor pericole deosebite (terorism, infracțiuni transfrontaliere), probele obținute prin aceste proceduri nu pot fi folosite în cazurile de drept comun (cele care nu implică protecția siguranței naționale, așa cum este ea definită prin lege), acolo unde garanțiile procedurale trebuie să fie strict respectate. Or, „legea atacată nu instituie nicio interdicție de utilizare a datelor în orice alt mod decât cel necesar pentru protecția în fața atacurilor cibernetice, situație ce poate submina garanția unui proces echitabil”.

9. În conformitate cu dispozițiile art.16 alin.(2) din Legea nr.47/1992 privind organizarea și funcționarea Curții Constituționale, sesizarea a fost comunicată președinților celor două Camere ale Parlamentului, precum și Guvernului, pentru a comunica punctul lor de vedere.

10. **Președintele Camerei Deputaților** a transmis cu Adresa nr.2/51/7 ianuarie 2015, înregistrată la Curtea Constituțională sub nr.99 din 7 ianuarie 2015, punctul său de vedere, în care se apreciază că sesizarea de neconstituționalitate este neîntemeiată.

11. În argumentare se arată că prevederile art. 1 din legea criticată se referă nu numai la obligații pentru cei în drept, ci vizează soluții legislative care

acoperă întreaga problematică a relațiilor sociale ce reprezintă obiectul de reglementare al acestei legi. Astfel, legea pornește de la premisa că măsurile privind securitatea cibernetică trebuie să asigure un mediu virtual sigur, care să constituie un real suport pentru maximizarea beneficiilor cetățenilor, mediului de afaceri și societății românești, în ansamblul ei. Toți deținătorii și utilizatorii de infrastructuri cibernetice, indiferent că sunt intermediari sau nu, trebuie să întreprindă măsurile necesare pentru securitatea infrastructurilor proprii și să nu afecteze securitatea celorlalți deținători sau utilizatori.

12. Pe de altă parte, se arată că, întrucât dispozițiile acestei legi se aplică numai persoanelor juridice de drept public sau privat, deținătoare de infrastructuri cibernetice, nu și persoanelor fizice, dispozițiile art. 26 alin. (1) din Constituție nu au incidență.

13. În ceea ce privește criticile aduse art.17 din lege referitoare la accesul la date, Președintele Camerei Deputaților susține că legea vizează datele relevante luării măsurilor proactive și reactive la nivelul infrastructurilor cibernetice, și nicidecum datele de trafic, astfel încât nu se aduce atingere drepturilor prevăzute la art. 23 și 28 din Legea fundamentală. Mai mult decât atât, dispozițiile art.12 și 14 din legea criticată prevăd că autoritățile și instituțiile publice cu atribuții în aplicarea acestei legi asigură securitatea infrastructurilor cibernetice potrivit legii și competențelor legale. Aceste entități sunt așadar obligate și limitate strict de respectarea cadrului legal.

14. Cu privire la desemnarea Serviciului Român de Informații ca autoritate națională în domeniul securității cibernetice, se arată, pe de o parte, că Directiva NIS nu impune statelor membre ale Uniunii Europene desemnarea unei autorități civile, și, pe de altă parte, că, potrivit art.1 din Legea nr.14/1992 privind organizarea și funcționarea Serviciului Român de Informații, activitatea acestei instituții este supusă controlului parlamentar efectuat prin intermediul Comisiei comune permanente a Camerei Deputaților și a Senatului.

15. **Guvernul** a transmis punctul său de vedere prin Adresa nr.5/7033/2014 înregistrată la Curtea Constituțională sub nr.146 din 13 ianuarie

2015, în care se arată că scopul Legii privind securitatea cibernetică este de a asigura un cadru coerent de reglementare a relațiilor sociale desfășurate în mediul virtual, care să asigure realizarea securității cibernetice a acestora, ca parte componentă a securității naționale a României.

16. Cu privire la criticile de neconstituționalitate formulate, Guvernul apreciază că „citirea atentă a legii demonstrează că aceste aspecte nu sunt reale, ci se bazează pe o interpretare tendențioasă a art.17 din lege, respectiv nu se ia în considerare contextul general de asigurare a securității cibernetice”. Se arată că autoritățile competente la care face referire articolul vor avea acces la date relevante ale deținătorilor de infrastructuri cibernetice pentru realizarea securității cibernetice, nu la mesaje ori alte date de conținut stocate, procesate sau transmise de sistemul informatic. Datele vizate de această lege sunt jurnalele sistemelor de stocare, prelucrare și transmitere a datelor (log-uri), date tehnice sau date de configurare ale sistemelor informatice, și nu includ mesaje ori alte date de conținut. În situația în care în urma analizei preliminare se constată că se impun investigații aprofundate asupra datelor de conținut, accesul la acestea și orice alte activități care vizează restrângerea unor drepturi și libertăți se realizează cu respectarea prevederilor legale în vigoare, respectiv în baza unui act de autorizare eliberat de judecător. În condițiile în care atacurile informatice se derulează foarte repede, pot provoca pagube materiale cetățenilor, pot afecta Infrastructurile Cibernetice de Interes National (ICIN-uri) sau chiar securitatea națională, este inefficient ca autoritățile competente să aștepte un aviz întocmit de un procuror și analizat și aprobat de un judecător pentru a obține acces la date tehnice care nu lezează în vreun fel drepturile și libertățile constituționale. Este fizic imposibil ca fiecare dintre aceste incidente să fie investigate, de aceea autoritățile competente se concentrează doar asupra celor care pot produce efecte negative semnificative, inclusiv în planul securității naționale. Guvernul susține că „astfel de clarificări vor fi introduse, însă, în normele de aplicare a legii, în actul normativ prevederea fiind nominalizată doar la nivel conceptual”.

17. Cu privire la critica potrivit căreia legea nu reglementează și „situațiile în care apar intermediari ce pun la dispoziție astfel de infrastructuri”, Guvernul menționează că în cazurile în care apar astfel de intermediari în fluxul infrastructurilor cibernetice, aceștia se circumscriu calității de deținători de astfel de infrastructuri, așa cum sunt definiți la art.2 din lege.

18. În consecință, pentru considerentele prezentate, Guvernul apreciază că sesizarea de neconstituționalitate a Legii privind securitatea cibernetică a României este neîntemeiată.

19. **Președintele Senatului** nu a comunicat punctul său de vedere asupra obiecției de neconstituționalitate.

CURTEA,

examinând obiecția de neconstituționalitate, raportul judecătorului-raportor, punctele de vedere ale Președintelui Camerei Deputaților și Guvernului, dispozițiile Legii privind securitatea cibernetică a României, precum și prevederile Constituției, reține următoarele:

20. Curtea a fost legal sesizată și este competentă, potrivit dispozițiilor art.146 lit. a) din Constituție și ale art.1, art.10, art.15, art.16 și art.18 din Legea nr.47/1992, să se pronunțe asupra constituționalității prevederilor legale criticate.

21. Obiectul controlului de constituționalitate, astfel cum rezultă din sesizarea formulată, îl constituie dispozițiile Legii privind securitatea cibernetică a României.

22. Dispozițiile constituționale pretins a fi încălcate sunt cele ale art.1 alin.(3) și (5) referitoare la statul de drept și obligația respectării legii și a supremației Constituției, art.23 alin.(1) referitor la inviolabilitatea libertății individuale și a siguranței persoanei, art.26 privind viața intimă, familială și privată, art.28 privind secretul corespondenței, precum și cele ale art.148 referitor la integrarea în Uniunea Europeană.

23. Examinând obiecția de neconstituționalitate, Curtea reține că Legea privind securitatea cibernetică a României, care are ca scop completarea cadrului

legislativ în materia securității naționale, a fost inițiată de Guvernul României și, ulterior, adoptată de Parlament în data de 19 decembrie 2015. În „Expunerea de motive” care însoțește legea, Guvernul afirmă că, „prin adoptarea acestuia act normativ, România va continua să transmită semnale puternice de racordare la realitățile internaționale, fiind pe deplin conștientă de necesitatea armonizării cu demersurile similare ale statelor europene”, în lipsa unei atare reglementări, „țara noastră nu-și va putea armoniza demersurile pe dimensiunea securității cibernetice cu cele ale partenerilor săi din Uniunea Europeană și NATO, demersuri necesare unei abordări coerente și suficiente a provocărilor și oportunităților spațiului cibernetic”.

24. Cu privire la aspectele invocate, Curtea ia act de faptul că, la nivel european, în temeiul art.114 din Tratatul privind funcționarea Uniunii Europene, a fost inițiată procedura legislativă ordinară de adoptare a unei directive privind măsuri de asigurare a unui nivel comun ridicat de securitate a rețelelor și a informației în Uniune – Directiva NIS (Network and Information Security). Inițiativa aparține Comisiei Europene, care la data de 7 februarie 2013 a transmis propunerea de directivă Consiliului și Parlamentului European. ***Propunerea de directivă a parcurs procedura primei lecturi în Parlamentul European, unde a fost adoptată cu modificări, la data de 13 martie 2014.*** La 10 iunie 2014, Comisia Europeană a exprimat un acord parțial cu privire la modificările Parlamentului. *Prin urmare, la data soluționării cauzei deduse judecării Curții Constituționale, nu există la nivelul Uniunii Europene un act normativ în vigoare cu privire la securitatea cibernetică.*

25. Cu toate acestea, **Curtea apreciază relevante pentru domeniul de reglementare câteva aspecte reținute la nivelul instituțiilor Uniunii cu privire la domeniul cercetat.** Astfel, potrivit „Expunerii de motive” a directivei, necesitatea adoptării actului normativ european constă, pe de o parte, *în asigurarea rezilienței și stabilității rețelelor și a sistemelor informatice, care sunt esențiale pentru definitivarea pieței digitale unice și pentru buna funcționare a pieței interne* și, pe de altă parte, în asigurarea unei capacități și a

unei pregătiri similare la nivelul statelor membre de natură să ofere o securitate globală a rețelelor și a informației în cadrul sistemelor interconectate. Directiva propusă vizează următoarele obiective: în primul rând, *solicită tuturor statelor membre să se asigure că este instituit un nivel minim de capacități naționale prin înființarea autorităților competente în materie de rețele și sisteme informatice*, să creeze echipe de intervenție în caz de urgență informatică (*Computer Emergency Response Teams - CERT*) și să adopte strategii naționale privind securitatea cibernetică și planurile naționale de cooperare în domeniul vizat; în al doilea rând, *autoritățile naționale competente trebuie să coopereze în cadrul unei rețele* care să permită o coordonare sigură și eficientă, inclusiv schimbul coordonat de informații la nivelul U.E., pentru a contracara amenințările și incidentele în materie de securitate cibernetică, pe baza planului european de cooperare în domeniu; în al treilea rând, conform modelului Directivei-cadru privind comunicațiile electronice, propunerea urmărește să asigure dezvoltarea unei culturi a gestionării riscurilor și partajarea informațiilor de către sectoarele public și privat.

26. De asemenea, Curtea reține considerentul 41 al preambulului directivei care prevede că „*Prezenta directivă respectă drepturile fundamentale și principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene, în special dreptul la respectarea vieții private și a secretului comunicațiilor, dreptul la protecția datelor cu caracter personal, libertatea de a desfășura o activitate comercială, dreptul de proprietate, dreptul la o cale de atac eficientă în fața unei instanțe judecătorești și dreptul de a fi ascultat. Prezenta directivă trebuie pusă în aplicare în conformitate cu aceste drepturi și principii.*”

27. Propunerea de directivă, în forma adoptată de Parlamentul European, conține mai multe dispoziții cu caracter obligatoriu pentru statele membre, dispoziții care ar urma să fie transpuse în legislația națională a fiecărui stat. Astfel, preambulul directivei NIS (considerentul 10) prevede că autoritățile competente și punctele unice de contact ar trebui să fie *organisme civile*, care să

*funcționeze integral pe baza controlului democratic, și care **nu ar trebui să desfășoare activități în domeniul informațiilor**, al aplicării legii sau al apărării și nici să fie legate organizațional în vreun fel de organisme active în aceste domenii. Astfel, dispozițiile art.6 din directivă, în forma modificată de PE, prevăd că „(1) **Fiecare stat membru desemnează una sau mai multe autorități naționale civile** competente în domeniul securității rețelelor și a sistemelor informatice.”*

28. În propunerea de Directivă NIS **nu se prevede dreptul autorităților desemnate de a accesa, la solicitarea motivată, datele stocate în rețelele și sistemele informatice**, așa cum prevede art.17 alin.(1) lit.a) din legea supusă controlului de constituționalitate, ci doar obligația de notificare a riscurilor și incidentelor cibernetice (art.14) și de a se supune auditării pentru deținătorii de infrastructuri critice (art.15). Astfel, în cazurile în care notificările conțin date cu caracter personal, acestea sunt comunicate doar destinatarilor din cadrul autorităților competente care trebuie să prelucreze aceste date pentru a-și îndeplini sarcinile în conformitate cu un temei juridic adecvat, iar datele comunicate se limitează la ceea ce este necesar pentru îndeplinirea sarcinilor acestor destinatari - art.14 alin.(2a), în vreme ce autoritățile competente sunt împuternicite să solicite operatorilor de piață furnizarea de „dovezi privind aplicarea efectivă a politicilor de securitate, precum **rezultatele auditului de securitate efectuat de auditori interni, de un organism calificat independent sau de o autoritate națională**, și să transmită dovezile autorității competente sau punctului unic de contact” - art.15 alin.(2) din directivă.

29. De asemenea, art.3 din propunerea de directivă definește noțiunea de **operator de piață**, ca fiind „un operator al unei infrastructuri care este esențială pentru menținerea activităților economice și societale vitale în domeniile energiei, transporturilor, serviciilor bancare, piețelor financiare, IXP (Internet Exchange points), lanțurilor de aprovizionare alimentară și sănătății, activități a căror denaturare sau distrugere ar avea un impact important într-un stat membru; o listă neexhaustivă a acestor operatori este prevăzută în anexa II,

în măsura în care rețeaua și sistemele informatice vizate sunt legate de serviciile esențiale.” Anexa II la propunerea de directivă - Lista operatorilor de piață, vizează, pe de o parte, *platforme de comerț electronic*, procesatori de plăți online, rețele de socializare, motoare de căutare, servicii de cloud computing, magazine de aplicații online, și, pe de altă parte, *domeniile referitoare la serviciile esențiale*, precum energie, transporturi, bănci, infrastructuri ale pieței financiare și sectorul sănătății. De asemenea, sub incidența proiectului de Directivă și, deci, a prevederilor privind securitatea cibernetică intră și *domeniul administrațiilor publice* (pct.26 din Preambul și Capitolul IV din propunerea de Directivă).

30. Potrivit „Expunerii de motive” la Directivă, se va solicita întreprinderilor din sectoarele critice și administrațiilor publice să evalueze riscurile cu care se confruntă și să adopte măsuri adecvate și proporționate de asigurare a securității cibernetice. Aceste entități vor trebui să raporteze autorităților competente orice *incidente* care afectează grav rețelele și sistemele lor informatice și *care au un impact semnificativ asupra continuității serviciilor critice și a aprovizionării cu bunuri*. Pentru a evita impunerea unei sarcini disproporționate asupra micilor operatori, în special asupra IMM-urilor, cerințele sunt proporționale cu riscurile la care sunt expuse rețeaua sau sistemul informatic în cauză și nu se aplică microîntreprinderilor, ci vizează numai entitățile critice și impun măsuri proporționale cu riscurile. Astfel, art.14 alin.(8) din propunerea de Directivă NIS stabilește că ***microîntreprinderile nu intră sub incidența directivei cu excepția situației în care acestea acționează în calitate de filială a unui operator de piață.***

31. În fine, potrivit art.15 alin.(6) din propunerea de Directivă, „***Statele membre se asigură că orice obligații impuse operatorilor de piață [...] pot fi supuse controlului jurisdicțional.***”

32. La momentul efectuării controlului de constituționalitate, Curtea reține că, în legislația națională în domeniul securității, există deja în vigoare o serie de reglementări, acte normative cu caracter primar sau secundar. Astfel,

Ordonanța de urgență a Guvernului nr.98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I, nr.757 din 12 noiembrie 2010, aprobată prin Legea nr.18/2011, publicată în Monitorul Oficial al României, Partea I, nr.183 din 16 martie 2011, stabilește cadrul legal privind identificarea, desemnarea infrastructurilor critice naționale/europene și evaluarea necesității de a îmbunătăți protecția acestora, în scopul creșterii capacității de asigurare a stabilității, securității și siguranței sistemelor economico-sociale și protecției persoanelor. Ordonanța transpune prevederile Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L 345 din 23 decembrie 2008. Actul normativ *definește infrastructura critică națională*, denumită ICN ca fiind un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții. Actul normativ *stabilește criteriile intersectoriale de identificare a ICN*: criteriul privind victimele, evaluat în funcție de numărul posibil de decese sau vătămări; criteriul privind efectele economice, evaluat în funcție de importanța pierderilor economice și/sau a degradării produselor sau serviciilor, inclusiv eventualele efecte asupra mediului; criteriul privind efectul asupra populației, evaluat în funcție de impactul asupra încrederii acesteia, suferința fizică sau perturbarea vieții cotidiene, inclusiv pierderea de servicii esențiale. În conformitate cu procedura prevăzută de ordonanța de urgență, autoritățile publice responsabile identifică potențialele ICN care corespund criteriilor sectoriale și intersectoriale. *Actul normativ conține 3 anexe*: Anexa nr.1 - Lista sectoarelor, subsectoarelor infrastructurii critice naționale/infrastructurii critice europene (ICN/ICE) și autorităților publice

responsabile; Anexa nr.2 - Procedura de identificare de către autoritățile publice responsabile de infrastructuri critice care pot fi desemnate drept infrastructuri critice naționale/infrastructuri critice europene (ICN/ICE) și Anexa nr.3 - Procedura privind planul de securitate pentru operator.

33. În aplicarea ordonanței de urgență, Guvernul a emis **Hotărârea nr.718/2011**, publicată în Monitorul Oficial al României, Partea I, nr.555 din 4 august 2011, prin care aprobă *Strategia națională privind protecția infrastructurilor critice*.

34. **Hotărârea Guvernului nr.494/2011**, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, *reglementează înființarea* ca instituție publică cu personalitate juridică, în coordonarea Ministerului Comunicațiilor și Societății Informaționale, a *Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, structură independentă de expertiză și cercetare-dezvoltare în domeniul protecției infrastructurilor cibernetice*. Centrul este condus de un director general și de un director general adjunct, sprijiniți de Comitetul de coordonare, din care fac parte reprezentanți ai MCSI, Ministerului Apărării Naționale, Ministerului Administrației și Internelor, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, Oficiului Registrului Național al Informațiilor Secrete de Stat și ai Autorității Naționale pentru Administrare și Reglementare în Comunicații. Hotărârea de Guvern *definieste termeni și expresii precum infrastructură cibernetică, spațiu cibernetic, securitate cibernetică, atac cibernetic, incident cibernetic etc.*, și stabilește atribuțiile CERT-RO.

35. Un alt act normativ emis în domeniul securității naționale îl constituie **Hotărârea Guvernului nr. 271/2013**, publicată în Monitorul Oficial al României, Partea I, nr. 296 din 23 mai 2013, pentru aprobarea *Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică*.

36. Strategia de securitate cibernetică prezintă obiectivele, principiile și direcțiile majore de acțiune pentru cunoașterea, prevenirea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetică a României și pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic. În acest sens, stabilește semnificația termenilor și expresiilor utilizați în domeniu, prevede *înființarea Sistemului național de securitate cibernetică (SNSC)* care reprezintă cadrul general de cooperare care reunește autorități și instituții publice, cu responsabilități și capacități în domeniu, în vederea coordonării acțiunilor la nivel național pentru asigurarea securității spațiului cibernetic, inclusiv prin cooperarea cu mediul academic și cel de afaceri, asociațiile profesionale și organizațiile neguvernamentale. De asemenea, prevede că *Consiliul operativ de securitate cibernetică (COSC)* reprezintă organismul prin care se realizează coordonarea unitară a SNSC. Din COSC fac parte, în calitate de membri permanenți, reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Telecomunicații Speciale, Serviciului de Informații Externe, Serviciului de Protecție și Pază, Oficiului Registrului Național pentru Informații Secrete de Stat, precum și secretarul Consiliului Suprem de Apărare a Țării. Conducerea COSC este asigurată de un președinte (consilierul prezidențial pe probleme de securitate națională) și un vicepreședinte (consilierul prim-ministrului pe probleme de securitate națională). Coordonatorul tehnic al COSC este Serviciul Român de Informații, în condițiile legii.

37. *Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică* este conținut în Anexa nr.2 la Hotărâre și este un document clasificat.

38. La data de 27 mai 2014, Guvernul României inițiază proiectul de lege privind securitatea cibernetică a României, care are ca scop completarea cadrului legislativ în materia securității naționale, apreciind că problematica securității cibernetică, ca parte a securității naționale, reprezintă o prioritate care

impune adoptarea de măsuri necesare dezvoltării mecanismelor de apărare cibernetică. Motivul emiterii actului normativ, așa cum reiese din „Expunerea de motive” care îl însoțește, îl constituie „evoluția recentă a atacurilor cibernetice din țara noastră” care determină aprecierea că „România este cu certitudine vizată de entități ostile în mediul virtual, nivelul de securitate cibernetică fiind, în prezent, insuficient pentru a face față unor atacuri de nivel ridicat ori cu intenții distructive.” Legea vizează stabilirea cadrului general de reglementare a activităților în domeniul securității cibernetice, definirea obligațiilor ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice, precum și asigurarea cadrului general de cooperare pentru realizarea securității cibernetice, prin constituirea Sistemului Național de Securitate Cibernetică.

39. Proiectul de lege a fost adoptat, la data de 17 septembrie 2014, de Camera Deputaților, în calitate de primă Cameră sesizată, în temeiul art.75 alin.(2) teza a treia din Constituție – ca urmare a depășirii termenului de 45 de zile, iar la data de 19 decembrie 2014, Senatul României, în calitate de Cameră decizională, a adoptat Legea privind securitatea cibernetică a României. Legea a fost trimisă Președintelui României pentru promulgare, iar în termenul prevăzut de lege, un număr de 69 de deputați a formulat cererea de sesizare a Curții Constituționale, care face obiectul prezentului dosar.

40. Din analiza documentului elaborat de inițiatorul legii intitulat „Expunere de motive”, Secțiunea a 6-a - Consultări efectuate în vederea elaborării proiectului de act normativ, la rubrica Informații privind avizarea de către autoritățile competente, Curtea constată că Guvernul menționează doar avizul Consiliului Legislativ.

41. Potrivit dispozițiilor art.1 din legea criticată, aceasta stabilește cadrul general de reglementare a activităților în domeniul securității cibernetice și obligațiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice, iar dispozițiile art.3 alin.(1) din lege stabilesc că „securitatea cibernetică este componentă a securității naționale a

României”. Cu privire la domeniul de reglementare a actului normativ supus controlului de constituționalitate, Curtea reține că, în temeiul prevederilor art.119 din Legea fundamentală, „Consiliul Suprem de Apărare a Țării organizează și coordonează unitar activitățile care privesc apărarea țării și securitatea națională, participarea la menținerea securității internaționale și la apărarea colectivă în sistemele de alianță militară, precum și la acțiuni de menținere sau de restabilire a păcii”. În aplicarea acestor prevederi, art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea și funcționarea Consiliului Suprem de Apărare a Țării, prevede, printre atribuțiile *CSAT*, că acesta **„avizează proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională”**. Pe de altă parte, potrivit art.9 alin.(1) din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, „În cazurile prevăzute de lege, în faza de elaborare a proiectelor de acte normative inițiatorul trebuie să solicite avizul autorităților interesate în aplicarea acestora, în funcție de obiectul reglementării”. De asemenea, art.31 alin.(3) din aceeași lege prevede că „Forma finală a instrumentelor de prezentare și motivare a proiectelor de acte normative trebuie să cuprindă referiri la avizul Consiliului Legislativ și, după caz, al Consiliului Suprem de Apărare a Țării, Curții de Conturi sau Consiliului Economic și Social.” Așadar, în temeiul dispozițiilor legale, Guvernul avea obligația de a solicita avizul Consiliului Suprem de Apărare a Țării atunci când a elaborat proiectul Legii privind securitatea cibernetică a României.

42. Pentru argumentele expuse, întrucât în cadrul procedurii legislative, inițiatorul nu a respectat obligația legală, conform căreia Consiliul Suprem de Apărare a Țării avizează proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională, **Curtea constată că actul normativ a fost adoptat cu încălcarea prevederilor constituționale ale art.1 alin.(5) care consacră principiul legalității, și ale art.119 referitoare la atribuțiile Consiliului Suprem de Apărare a Țării.**

43. Examinând conținutul normativ al legii, Curtea reține că aceasta prevede înființarea *Sistemului Național de Securitate Cibernetică*, denumit SNSC, care reunește autoritățile și instituțiile publice cu responsabilități și capacități în domeniu (art.6). Coordonarea unitară a activităților SNSC se realizează de către *Consiliul Operativ de Securitate Cibernetică*, denumit COSC (art.8). Serviciul Român de Informații este desemnat autoritate națională în domeniul securității cibernetice, calitate în care asigură coordonarea tehnică a COSC, precum și organizarea și executarea activităților care privesc securitatea cibernetică a României. În acest scop, în structura SRI funcționează *Centrul Național de Securitate Cibernetică*, denumit CNSC (art.10 alin.(1)). Sunt desemnate autorități în domeniul securității cibernetice pentru domeniile lor de activitate, asigurând securitatea infrastructurilor cibernetice proprii sau aflate în responsabilitate: Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază. *Centrul Național de Răspuns la Incidente de Securitate*, denumit în continuare CERT-RO, reprezintă un punct național de contact cu structurile de tip CERT care funcționează în cadrul instituțiilor sau autorităților publice ori al altor persoane juridice de drept public sau privat, naționale ori internaționale, cu respectarea competențelor ce revin celorlalte autorități și instituții publice cu atribuții în domeniu, potrivit legii (art.10 alin.(5)). Autoritatea implicată în securitatea infrastructurilor cibernetice deținute sau administrate de furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice destinate publicului este *Autoritatea Națională pentru Administrare și Reglementare în Comunicații*, denumită ANCOM (art.13 alin.(2)), instituție înființată prin Ordonanța de urgență Guvernului nr.22/2009.

44. Un element de noutate adus de legea criticată, prin art.10 alin.(1), îl constituie ***desemnarea Serviciului Român de Informații ca autoritate națională în domeniul securității cibernetice***, calitate în care asigură

organizarea și executarea activităților care privesc securitatea cibernetică a României. În acest scop, *în structura SRI funcționează Centrul Național de Securitate Cibernetică (CNSC), care a fost constituit, organizat și funcționează deja în cadrul SRI, cu personal militar specializat, potrivit unor hotărâri ale Consiliului Suprem de Apărare a Țării.* Autoritățile și instituțiile publice din componența COSC delegă un reprezentant în cadrul CNSC. Potrivit art.11 din lege, principalele atribuții ale CNSC vizează acțiuni în scopul cunoașterii, prevenirii, protecției, reacției și managementului consecințelor amenințărilor și atacurilor cibernetic; asigurarea schimbului de date și informații între autoritățile și instituțiile publice componente ale SNSC; analiza și integrarea datelor și informațiilor obținute de autoritățile și instituțiile publice componente ale SNSC, în scopul stabilirii, întreprinderii sau propunerii măsurilor ce se impun pentru asigurarea securității cibernetic; asigurarea colectării și identificării evenimentelor survenite în spațiul cibernetic; primirea notificărilor făcute de persoanele juridice de drept public care dețin sau administrează infrastructuri cibernetic de interes național (ICIN); în caz de atac cibernetic, asigurarea colectării și evaluarea datelor și informațiilor cu privire la incident, propunerea sau luarea de măsuri reactive de primă urgență pentru asigurarea integrității datelor și remedierea situației de fapt, informarea organelor competente pentru investigare și cercetare, sau, după caz, sesizarea organelor de urmărire penală.

45. De asemenea, art.15 alin.(8) din lege stabilește *obligația tuturor persoanelor juridice de drept public sau privat deținători de ICIN de a transmite cu celeritate datele privind starea de securitate cibernetică la nivelul acestora către CNSC*, conform competențelor prevăzute de lege.

46. Cu privire la desemnarea SRI, recte CNSC, ca autoritate națională în domeniul securității cibernetic, autorii criticilor de neconstituționalitate susțin că legiuitorul acordă acces nelimitat și nesupravegheat la toate datele informatice deținute de persoane de drept public și privat unei instituții care nu

îndeplinește condiția referitoare la un organism civil, supus controlului democratic.

47. În analiza de constituționalitate, Curtea pornește de la premisa că strategia de securitate cibernetică și legea privind securitatea cibernetică au un rol important în asigurarea securității naționale a României, pe de o parte, și a protecției persoanei față de riscurile la adresa vieții private și a protecției datelor cu caracter personal în mediul online, pe de altă parte. Cu privire la aceste aspecte analizate coroborat, prin Hotărârea din 6 septembrie 1978, pronunțată în *Cauza Klass și alții împotriva Germaniei*, Curtea Europeană a Drepturilor Omului a apreciat că „Societățile democratice sunt amenințate în prezent de modalități complexe de spionaj și de terorism, astfel că statul trebuie să fie capabil, pentru a combate eficient aceste amenințări, să supravegheze în mod secret elementele subversive care operează pe teritoriul său” (paragraful 42). Cu toate acestea, Curtea, conștientă de pericolul, inerent măsurilor de supraveghere secretă, „de a submina, chiar de a distruge democrația sub motivul apărării acesteia, afirmă că statele nu pot lua, în numele combaterii spionajului și terorismului, orice măsură pe care acestea o consideră adecvată” (paragraful 49).

48. În această lumină, Curtea Constituțională trebuie să verifice dacă reglementarea domeniului vizat concordă cu respectarea dreptului la viață intimă, familială și privată, cu inviolabilitatea secretului corespondenței, cu dreptul la protecția datelor cu caracter personal, valori fundamentale care ar trebui să reprezinte principii directe ale politicii de securitate cibernetică la nivel național, și să se asigure că legislația adoptată nu conduce la măsuri care ar constitui interferențe neconstituționale cu drepturile menționate. Așa fiind, Curtea apreciază că, pentru asigurarea unui climat de ordine, guvernat de principiile unui stat de drept, democratic, înființarea sau identificarea unui organism responsabil cu coordonarea problemelor de securitate a sistemelor și rețelelor cibernetică, precum și a informației, care să constituie punctul de contact pentru relaționarea cu organismele similare din străinătate (așa cum prevede art.10 alin.(4) din lege), inclusiv al cooperării transfrontaliere la nivelul

Uniunii Europene, trebuie să vizeze *un organism civil, care să funcționeze integral pe baza controlului democratic*, iar nu o autoritate care desfășoară activități în domeniul informațiilor, al aplicării legii sau al apărării ori care să reprezinte o structură a vreunui organism care activează în aceste domenii.

49. În ceea ce privește dispozițiile art.1 alin.(3), teza întâi din Constituție, care consacră principiul statului de drept, Curtea a reținut în jurisprudența sa (a se vedea Decizia nr.70 din 18 aprilie 2000, publicată în Monitorul Oficial al României, Partea I, nr.334 din 19 iulie 2000) că exigențele acestuia privesc scopurile majore ale activității statale, prefigurate în ceea ce îndeobște este numit ca fiind domnia legii, sintagmă ce implică subordonarea statului față de drept, asigurarea acelor mijloace care să permită dreptului să cenzureze opțiunile politice și, în acest cadru, să pondereze eventualele tendințe abuzive, discreționare, ale structurilor etatice. Statul de drept asigură supremația Constituției, corelarea legilor și tuturor actelor normative cu aceasta, existența regimului de separație a puterilor publice, care trebuie să acționeze în limitele legii, și anume în limitele unei legi ce exprimă voința generală. *Statul de drept consacră o serie de garanții, inclusiv jurisdicționale, care să asigure respectarea drepturilor și libertăților cetățenilor prin autolimitarea statului, respectiv încadrarea autorităților publice în coordonatele dreptului.*

50. În analiza Curții, opțiunea pentru desemnarea în calitate de autoritate națională în domeniul securității cibernetice a unui organism civil, iar nu a unei entități militare cu activitate în domeniul informațiilor, se justifică prin necesitatea preîntâmpinării riscului de a deturna scopul legii securității cibernetice în sensul folosirii atribuțiilor conferite prin această lege de către serviciile de informații în scopul obținerii de informații și date cu consecința încălcării drepturilor constituționale la viață intimă, familială și privată și la secretul corespondenței. Or, tocmai acest lucru nu evită legea supusă controlului de constituționalitate prin desemnarea SRI și a structurii sale militarizate CNSC.

51. Astfel, examinând atribuțiile stabilite de actul normativ supus controlului, apare cu evidență intenția legiuitorului de a stabili în competența

CNSC colectarea tuturor datelor privind starea de securitate a infrastructurii, oricare ar fi natura acestora, atât din mediul public, cât și din cel privat. Or, în condițiile în care Centrul Național de Securitate Cibernetică constituie o structură militară, în cadrul unui serviciu de informații, subordonată ierarhic conducerii acestei instituții, deci sub un control direct militar-administrativ, apare cu evidență că *o atare entitate nu îndeplinește condițiile cu privire la garanțiile necesare respectării drepturilor fundamentale referitoare la viață intimă, familială și privată și la secretul corespondenței.*

52. De asemenea, în condițiile în care autoritatea națională desemnată deservește drept punct unic de contact național în domeniul securității rețelelor și al sistemelor informatice, asigurând relaționarea cu organismele similare din cadrul Uniunii Europene, împrejurarea că România desemnează o autoritate care nu ar îndeplini exigențele actului normativ european, aflat în curs de adoptare, pune sub semnul întrebării atât o eventuală concordanță a reglementării naționale cu cea de drept european, cât și cooperarea efectivă între instituții care, deși au același scop, nu se întemeiază pe o structură organizatorică similară și nu funcționează sub un control democratic.

53. Pentru toate aceste argumente, Curtea constată că **dispozițiile art.10 alin.(1) din legea supusă controlului încalcă prevederile constituționale ale art.1 alin.(3) și (5) referitoare la statul de drept și principiul legalității, precum și cele ale art.26 și art.28 privind viață intimă, familială și privată, respectiv secretul corespondenței, din perspectiva lipsei garanțiilor necesare garantării acestor drepturi.**

54. Curtea observă că dispozițiile art.2 prevăd sfera de incidență a legii, sub aspectul destinatarilor săi, arătând că persoanele juridice de drept public sau privat cărora le sunt aplicabile prevederile legale, intitulați generic *deținători de infrastructuri cibernetice*, sunt: proprietarii, administratorii, operatorii sau utilizatorii de infrastructuri cibernetice, definite la art.5 lit.g) ca fiind infrastructuri din domeniul tehnologiei informației și comunicații, constând în

sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice.

55. Definirea expresiei „deținători de infrastructuri cibernetice” este deosebit de importantă, deoarece includerea în această categorie implică pentru persoanele vizate obligația de a respecta prevederile legii, pe de o parte, și justificarea pentru autoritățile desemnate de lege cu competențe în domeniul securității cibernetice de a dispune măsuri speciale în ceea ce le privește.

56. Obligațiile care incumbă destinatarilor legii vizează asigurarea rezilienței infrastructurilor cibernetice, respectiv capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate. Această stare este menținută în urma aplicării unui ansamblu de măsuri proactive și reactive prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a resurselor și serviciilor publice sau private, din spațiul cibernetic. ***Includerea în sfera de incidență a legii a utilizatorilor de infrastructuri cibernetice***, deci a tuturor persoanelor juridice care utilizează rețele și servicii de comunicații electronice, ridică probleme legate de modul în care acestea pot să-și îndeplinească obligațiile și responsabilitățile prevăzute de lege, în condițiile în care nu sunt proprietari, administratori sau operatori ai infrastructurilor cibernetice pe care le utilizează, iar legea face vorbire în cuprinsul art.16, despre *infrastructuri cibernetice proprii sau aflate în responsabilitate*. Mai mult, în măsura în care obligațiile și responsabilitățile cad atât în sarcina proprietarilor, administratorilor sau operatorilor infrastructurilor cibernetice, cât și a utilizatorilor acestor infrastructuri, iar legea nu stabilește sensul noțiunii de utilizator, rezultă că obligațiile și responsabilitățile se exercită în mod concurent la nivelul fiecărui sistem sau fiecărei rețele informatice. Spre exemplu, potrivit art.16 alin.(1) lit.a) și b) din lege, atât proprietarul, cât și utilizatorul sunt obligați să aplice politici de securitate, să identifice și să implementeze măsurile tehnice și organizatorice adecvate pentru a gestiona eficient riscurile de securitate. Însă, există posibilitatea ca, uneori, politicile de

securitate, măsurile tehnice și, mai ales, cele organizatorice, considerate adecvate de cele două entități, să nu coincidă sau să nu fie compatibile, astfel încât finalitatea urmărită de lege să nu fie atinsă. Or, destinatarii legii trebuie să aibă o reprezentare clară și corectă a normelor juridice aplicabile, astfel încât să își adapteze conduita și să prevadă consecințele ce decurg din nerespectarea acestora, lipsa unei reglementări predictibile în acest sens constituind premisa unei aplicări neunitare, discreționare, în activitatea de securizare cibernetică a României.

57. În concluzie, întrucât noțiunile cu care operează legea nu delimitează în mod neechivoc sfera de incidență a normelor cuprinse în actul supus controlului de constituționalitate, Curtea reține că acesta nu are un caracter precis și previzibil, și, prin urmare, **dispozițiile art.2 contravin art.1 alin.(5) din Legea fundamentală.**

58. Curtea reține că tuturor deținătorilor de infrastructuri cibernetică le sunt aplicabile dispozițiile art.16 (care stabilesc obligațiile ce le incumbă), și ale art.17 (care consacră responsabilitățile pe care aceștia trebuie să le îndeplinească). Printre responsabilitățile acestor persoane este și aceea de *acorda sprijinul necesar, la solicitarea motivată* a Serviciului Român de Informații, Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Oficiului Registrului Național al Informațiilor Secrete de Stat, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, CERT-RO și ANCOM, *în îndeplinirea atribuțiilor ce le revin acestora, și „să permită accesul reprezentanților desemnați în acest scop la datele deținute, relevante în contextul solicitării”*. Textul de lege impune o dublă analiză: prima, din perspectiva tipului de date la care se permite accesul, a doua, din perspectiva modalității în care se realizează accesul.

59. Cu privire la primul aspect, deși legislația privind protecția datelor cu caracter personal nu este menționată în mod expres în lege, accesul la datele deținute de persoanele care cad sub incidența legii, nu exclude accesarea, prelucrarea și utilizarea *datelor cu caracter personal*. De asemenea, având în

vedere că infrastructurile cibernetice constau în sisteme informatice, în rețele și servicii de comunicații electronice, care facilitează stocarea și transferul de date, apare ca fiind evident că tipul de date cuprinse în aceste sisteme și rețele sunt inclusiv *date care privesc viața privată* a persoanelor utilizatoare. Prevederea în temeiul căreia accesul se realizează cu privire la „*datele deținute, relevante în contextul solicitării*” permite interpretarea potrivit căreia autorităților desemnate de lege trebuie să li se permită accesul la oricare din datele stocate în aceste infrastructuri cibernetice, dacă autoritățile apreciază că respectivele date prezintă relevanță. Se remarcă, astfel, caracterul nepredictibil al reglementării, atât sub aspectul tipului de date accesate, cât și al evaluării relevanței datelor solicitate, de natură să creeze premisele unor aplicări discreționare de către autoritățile enumerate în ipoteza normei. Astfel, datele la care se poate solicita accesul pot viza, de exemplu, jurnalele sistemelor de stocare, prelucrare și transmitere a datelor, datele tehnice, datele de configurare ale sistemelor informatice, mesajele sau orice alte date de conținut. Lipsa unei reglementări legale precise, care să determine cu exactitate sfera acelor date necesare identificării evenimentelor survenite în spațiul cibernetic (amenințări, atacuri sau incidente cibernetice), deschide posibilitatea unor abuzuri din partea autorităților competente. Or, cadrul normativ într-un domeniu atât de sensibil trebuie să se realizeze într-o manieră clară, previzibilă și lipsită de confuzie, astfel încât să fie îndepărtată, pe cât posibil, eventualitatea arbitrariului sau a abuzului celor chemați să aplice dispozițiile legale.

60. Cu privire la aceste probleme, Curtea deja a decis într-o manieră indubitabilă, prin Decizia nr.440 din 8 iulie 2014, publicată în Monitorul Oficial al României, Partea I, nr.653 din 4 septembrie 2014, statuând că, „datele care fac obiectul reglementării, deși au un caracter predominant tehnic, sunt reținute în scopul furnizării informațiilor cu privire la persoana și viața sa privată. Chiar dacă, potrivit art.1 alin.(3) din lege, aceasta nu se aplică și conținutului comunicării sau informațiilor consultate în timpul utilizării unei rețele de comunicații electronice, celelalte date reținute, având ca scop identificarea

apelantului și a apelatului, respectiv a utilizatorului și a destinatarului unei informații comunicate pe cale electronică, a sursei, destinației, datei, orei și duratei unei comunicări, a tipului de comunicare, a echipamentului de comunicație sau a dispozitivelor folosite de utilizator, a locației echipamentului de comunicații mobile, precum și a altor «date necesare» — nedefinite în lege —, sunt de natură să prejudicieze manifestarea liberă a dreptului la comunicare sau la exprimare. În concret, datele avute în vedere conduc la concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, concluzii ce pot viza obiceiurile din viața cotidiană, locurile de ședere permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele. Or, o atare limitare a exercițiului dreptului la viață intimă, familială și privată și la secretul corespondenței, precum și a libertății de exprimare trebuie să aibă loc într-o manieră clară, previzibilă și lipsită de echivoc, astfel încât să fie îndepărtată, pe cât posibil, eventualitatea arbitrarului sau a abuzului autorităților în acest domeniu”.(paragraful 56)

61. De asemenea, Curtea de Justiție a Uniunii Europene a reținut, prin Hotărârea din 8 aprilie 2014, pronunțată în cauzele conexe C-293/12 — *Digital Rights Ireland Ltd împotriva Minister for Communications, Marine and Natural Resources și alții* — și C-594/12 — *Kärntner Landesregierung și alții*. că datele ce fac obiectul reglementării Directivei 2006/24/CE, invalidate, conduc la concluzii foarte precise privind viața privată a persoanelor ale căror date au fost păstrate, concluzii ce pot viza obiceiurile din viața cotidiană, locurile de ședere permanentă sau temporară, deplasările zilnice sau alte deplasări, activitățile desfășurate, relațiile sociale ale acestor persoane și mediile sociale frecventate de ele (paragraful 27) și că, în aceste condiții, chiar dacă, potrivit art.1 alin.(2) și art.5 alin.(2) din Directiva 2006/24/CE, este interzisă păstrarea conținutului comunicațiilor și al informațiilor consultate prin utilizarea unei rețele de comunicații electronice, păstrarea datelor în cauză poate afecta utilizarea de către abonați sau de către utilizatorii înregistrați a mijloacelor de

comunicare prevăzute de această directivă și, în consecință, libertatea lor de exprimare, garantată prin art.11 din Cartă (paragraful 28).

62. De altfel, *accesul* la date vizează datele unei infrastructuri cibernetice (infrastructură definită de art.5 lit.g) din lege ca fiind un sistem informatic, aplicații aferente, rețele și servicii de comunicații electronice) în sensul legii supusă controlului de constituționalitate se suprapune cu noțiunea de „acces la un sistem informatic”, reglementată de art.138 alin.(1) lit.b) și alin.(3) din Codul de procedură penală, care constă în „pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice, fie direct, fie de la distanță, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe”. De asemenea, în același context, prin *date deținute* se înțelege „datele informatice” reglementate de art.138 alin.(5) din Codul de procedură penală, care sunt „orice reprezentare de fapte, informații sau concepte, sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic”. Or, accesul la un sistem informatic în scopul obținerii acestor date constituie una dintre metodele speciale de supraveghere sau cercetare potrivit art.138 alin.(13) din Codul de procedură penală, măsură care poate fi dispusă doar în condițiile art.140 (de către judecător) sau a art.141 (de către procuror, pentru o durată de maxim 48 de ore). De asemenea, datele relevante pot fi și cele generate sau prelucrate de către furnizorii de rețele publice de comunicații electronice sau furnizorii de servicii de comunicații electronice destinate publicului și reținute de către aceștia, însă și acestea pot fi obținute doar cu autorizarea judecătorului, conform art.152 din Codul de procedură penală.

63. Cu privire la cel de-al doilea aspect, legea criticată se limitează la a preciza care sunt autoritățile care pot solicita accesul la datele deținute pe baza formulării unei solicitări motivate, fără a reglementa modalitatea în care se realizează accesul efectiv la datele deținute, așa încât persoanele ale căror date au fost păstrate să beneficieze de garanții suficiente care să le asigure protecția

împotriva abuzurilor și a oricărui acces sau utilizări ilicite. Astfel, *legea* nu prevede criterii obiective care să limiteze la strictul necesar numărul de persoane care au acces și pot utiliza ulterior datele păstrate, și *nu stabilește că accesul autorităților naționale la datele stocate este condiționat de controlul prealabil efectuat de către o instanță judecătorească*, care să limiteze acest acces și utilizarea lor la ceea ce este strict necesar pentru realizarea obiectivului urmărit. Garanțiile legale privind utilizarea în concret a datelor reținute nu sunt suficiente și adecvate pentru a îndepărta teama că drepturile personale, de natură intimă, sunt violate, așa încât manifestarea acestora să aibă loc într-o manieră acceptabilă (a se vedea în acest sens și Decizia nr.440/2012, paragraful 57).

64. *Solicitățile de acces la datele reținute în vederea utilizării lor în scopul prevăzut de lege, formulate de către organele de stat desemnate autorități în domeniul securității cibernetice pentru domeniile lor de activitate, nu sunt supuse autorizării sau aprobării instanței judecătorești*, lipsind astfel garanția unei protecții eficiente a datelor păstrate împotriva riscurilor de abuz precum și împotriva oricărui acces și a oricărei utilizări ilicite a acestor date. Această împrejurare este de natură a constitui o ingerință în drepturile fundamentale la viață intimă, familială și privată și a secretului corespondenței și, prin urmare, contravine dispozițiilor constituționale care consacră și protejează aceste drepturi. Lipsa unor astfel de autorizări a fost criticată, printre altele, și de către Curtea de Justiție a Uniunii Europene prin Hotărârea din 8 aprilie 2014, această lipsă echivalând cu insuficiența garanțiilor procesuale necesare ocrotirii dreptului la viața privată și a celorlalte drepturi consacrate de art.7 din Carta drepturilor și libertăților fundamentale și a dreptului fundamental la protecția datelor cu caracter personal, consacrat de art.8 din Cartă (paragraful 62).

65. În concluzie, în condițiile în care măsurile adoptate prin legea supusă controlului de constituționalitate nu au un caracter precis și previzibil, ingerința statului în exercitarea drepturilor constituționale la viață intimă, familială și privată și la secretul corespondenței, deși prevăzută de lege, nu este

formulată clar, riguros și exhaustiv pentru a oferi încredere cetățenilor, caracterul strict necesar într-o societate democratică nu este pe deplin justificat, iar proporționalitatea măsurii nu este asigurată prin reglementarea unor garanții corespunzătoare, considerăm că **dispozițiile art.17 alin.(1) lit.a) din Legea privind securitatea cibernetică a României încalcă prevederile art.1 alin.(5), art.26, art.28, și art.53 din Constituție**. Așadar, limitarea exercițiului acestor drepturi personale în considerarea unor drepturi colective și interese publice, ce vizează securitatea cibernetică rupe justul echilibru care ar trebui să existe între interesele și drepturile individuale, pe de o parte, și cele ale societății, pe de altă parte, legea criticată nereglementând garanții suficiente care să permită asigurarea unei protecții eficiente a datelor față de riscurile de abuz, precum și față de orice accesare și utilizare ilicită a datelor cu caracter personal (*ad similibus*, Decizia nr.461/2014, paragraful 44).

66. În continuarea analizei sale, Curtea observă că, din coroborarea dispozițiilor art.2 cu art.19 și art.20 din lege, rezultă că, în cadrul deținătorilor de infrastructuri cibernetice, *se creează o subcategorie – deținătorii de infrastructuri cibernetice de interes național (ICIN)*, care, potrivit art.2 lit.h) din lege, reprezintă infrastructurile cibernetice care susțin servicii publice sau de interes public, ori servicii ale societății informaționale, a căror afectare poate aduce atingere securității naționale, sau prejudicii grave statului român ori cetățenilor acestuia. Aceștia sunt cuprinși în ***Catalogul ICIN***, întocmit de Ministerul pentru Societatea Informațională, cu consultarea COSC, la propunerea CNSC sau, după caz, a CERT-RO, și a ANCOM. Potrivit art.19 alin.(1), catalogul ***este aprobat prin hotărâre a Guvernului. Identificarea ICIN se realizează pe baza criteriilor de selecție cuprinse în metodologia elaborată de Serviciul Român de Informații și Ministerul pentru Societatea Informațională și este aprobată prin hotărâre de Guvern.***

67. Cu privire la aceste aspecte, Curtea apreciază că ***modalitatea prin care se stabilesc criteriile în funcție de care se realizează selecția infrastructurilor cibernetice de interes național și, implicit, a deținătorilor***

ICIN nu respectă cerințele de previzibilitate, certitudine și transparență. Astfel, trimiterea la o legislație infralegală, respectiv hotărâri de Guvern, acte normative caracterizate printr-un grad sporit de instabilitate, pentru reglementarea criteriilor în funcție de care devin incidente obligații în materia securității naționale încalcă principiul constituțional al legalității, consacrat de art.1 alin.(5) din Constituție. Opțiunea pentru o atare modalitate de reglementare apare cu atât mai nejustificată cu cât într-o materie similară, cea a identificării infrastructurilor critice naționale, Ordonanța de urgență a Guvernului nr.98/2010 stabilește în chiar conținutul său criteriile intersectoriale de identificare a ICN. Mai mult, prin Anexa la actul normativ se aprobă lista sectoarelor, subsectoarelor infrastructurii critice naționale/infrastructurii critice europene (ICN/ICE) și autorităților publice responsabile (energetic, tehnologia informației și comunicații, alimentare cu apă, alimentație, sănătate, securitate națională, administrație, transporturi, industria chimică și nucleară, spațiu și cercetare). Or, în cazul Legii privind securitatea cibernetică, dispozițiile art.19 fac trimitere la acte normative cu forță juridică inferioară legii, *identificarea ICIN realizându-se pe baza unei metodologii elaborate de Serviciul Român de Informații și de Ministerul pentru Societatea Informațională, în baza unei proceduri neprevăzute de lege, netransparente, și deci, susceptibilă de a fi calificată arbitrară.*

68. Prin urmare, Curtea reține că atât *criteriile în funcție de care se realizează selecția infrastructurilor cibernetice de interes național, cât și modalitatea prin care se stabilesc acestea trebuie prevăzute de lege, iar actul normativ de reglementare primară trebuie să conțină o listă cât mai completă a domeniilor în care sunt incidente prevederile legale.*

69. Pe de altă parte, Curtea apreciază că *obligațiile ce decurg din Legea securității cibernetice a României trebuie să fie aplicabile în exclusivitate persoanelor juridice de drept public sau privat deținătoare sau care au în responsabilitate ICIN (care includ, în baza legii, și administrațiile publice),* întrucât numai situațiile de pericol cu privire la o infrastructură de

interes național pot avea implicații asupra securității României, prin dimensiunea, dispersia și accesibilitatea unei astfel de infrastructuri, prin efectele economice, evaluate în funcție de importanța pierderilor economice și/sau a degradării produselor sau serviciilor, prin efectele asupra populației, evaluate în funcție de impactul asupra încrederii acesteia sau perturbarea vieții cotidiene, inclusiv prin pierderea unor servicii esențiale. Or, dispozițiile legale în forma supusă controlului de constituționalitate prezintă un grad mare de generalitate, obligațiile vizând totalitatea deținătorilor de infrastructuri cibernetice, constând în sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice, indiferent de importanța acestora care poate viza interesul național sau doar un interes de grup sau chiar particular. Pentru a evita impunerea unei sarcini disproporționate asupra micilor operatori, cerințele trebuie să fie proporționale cu riscurile la care sunt expuse rețeaua sau sistemul informatic în cauză și nu trebuie aplicat deținătorilor de infrastructuri cibernetice cu importanță ne semnificativă din punct de vedere al interesului general. Prin urmare, riscurile vor trebui identificate la nivelul entităților care activează în domenii esențiale/vitale pentru buna desfășurare a serviciilor publice naționale, care vor decide ce măsuri trebuie adoptate pentru a atenua riscurile respective.

70. Pentru motivele expuse mai sus, apreciem că **dispozițiile art.19 alin.(1) și (3) din Legea securității cibernetice a României încalcă prevederile art.1 alin.(5) din Constituție, întrucât nu respectă cerințele de previzibilitate, stabilitate și certitudine.**

71. În continuare, Curtea reține că dispozițiile art.20 și art.21 alin.(2) din legea criticată prevăd *obligațiile care incumbă persoanelor juridice de drept public sau privat care dețin sau au în responsabilitate ICIN*, printre care să efectueze anual auditări de securitate cibernetică sau să permită efectuarea unor astfel de auditări la solicitarea motivată a autorităților competente potrivit prezentei legi, să constituie structuri sau să desemneze persoane responsabile cu prevenirea, identificarea și reacția la incidentele cibernetice, să notifice imediat, după caz, CNSC, CERT-RO, ANCOM sau autoritățile desemnate, în condițiile

legii, în domeniul securității cibernetice cu privire la riscurile și incidentele cibernetice care, prin efectul lor, pot aduce prejudicii de orice natură utilizatorilor sau beneficiarilor serviciilor lor. De asemenea, în cazul în care au fost notificate riscuri sau incidente cibernetice, deținătorii de ICIN au obligația să permită autorităților competente să intervină pentru identificarea și analizarea cauzelor incidentelor cibernetice, respectiv pentru înlăturarea sau reducerea efectelor incidentelor cibernetice, să rețină și să asigure integritatea datelor referitoare la incidentele cibernetice pentru o perioadă de 6 luni de la data notificării.

72. Legea stabilește că *sunt exceptate de la aplicarea acestor dispoziții autoritățile prevăzute la art.10 alin.(1) și (2) din lege*, respectiv Serviciul Român de Informații, Ministerul Apărării Naționale, Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază. Or, *Curtea consideră nejustificată această exceptare în condițiile în care și autoritățile enumerate desfășoară activități în domeniul securității naționale, sunt deținătoare de ICIN sau au în responsabilitate ICIN și sunt susceptibile a face obiectul unor atacuri cibernetice.*

73. Potrivit dispozițiilor art.20 alin.(1) lit.c) din lege, persoanele juridice de drept public sau privat care dețin sau au în responsabilitate ICIN **au obligația să permită efectuarea unor auditări de securitate cibernetică** la solicitarea motivată a autorităților competente. Auditările sunt realizate de SRI sau de către furnizori de servicii de securitate cibernetică. Cu alte cuvinte, întrucât SRI este autoritate națională în domeniul securității cibernetice, deci autoritate competentă, potrivit legii, să solicite persoanelor juridice de drept public sau privat care dețin sau au în responsabilitate ICIN efectuarea unor auditări de securitate cibernetică, există posibilitatea reală ca *această instituție să se afle concomitent în poziția solicitantului auditului, a celui care efectuează auditul, a celui căruia i se comunică rezultatul auditului și, în fine, în poziția celui care constată o eventuală contravenție, potrivit art.28 lit.e) din lege, și*

aplică sancțiunea, potrivit art.30 lit.c) din lege. Or, o atare situație este inacceptabilă într-o societate guvernată de principiile statului de drept. Dispozițiile legale sunt susceptibile de a genera o aplicare discreționară, chiar abuzivă a legii, fiind nepermis ca toate atribuțiile din domeniul reglementat să fie concentrate în sarcina unei singure instituții. Curtea apreciază că auditul trebuie să fie efectuat de auditori interni sau de un organism calificat independent care să verifice conformitatea aplicării politicilor de securitate cibernetică la nivelul infrastructurilor cibernetică și să transmită rezultatul evaluării efectuate autorității competente sau punctului unic de contact.

74. Pornind de la definiția noțiunii de „audit de securitate cibernetică”, prevăzută în art.5 lit.d), care stabilește că aceasta reprezintă o evaluare sistematică, detaliată, măsurabilă și tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetică, precum și emiterea de recomandări pentru minimizarea riscurilor identificate, Curtea reține că, în accepțiunea legii, această auditare presupune doar o evaluare a politicilor de securitate cibernetică și nicidecum accesul la datele stocate în infrastructurile cibernetică.

75. În ceea ce privește norma prevăzută de art.20 alin.(1) lit.h) și anume ***obligăția de a notifica imediat, după caz, CNSC, CERT-RO, ANCOM sau autoritățile desemnate***, în condițiile legii, în domeniul securității cibernetică cu privire la riscurile și incidentele cibernetică, Curtea consideră că aceasta *ar trebui să stabilească cu exactitate circumstanțele în care este necesară notificarea, precum și conținutul notificării, inclusiv tipurile de date cu caracter personal care ar trebui notificate, și, dacă este cazul, în ce măsură notificarea și documentele sale justificative vor include detalii privind datele cu caracter personal afectate de un incident specific de securitate (precum adresele IP).* Este important să se țină seama de faptul că autorităților competente în domeniul securității rețelelor și informației ar trebui să li se permită să colecteze și să prelucreze date cu caracter personal în cadrul unui incident de securitate doar dacă este strict necesar pentru atingerea obiectivelor de interes public urmărite

de lege, cu respectarea principiului proporționalității. De asemenea, legea trebuie să prevadă garanții adecvate pentru a se asigura protecția efectivă a datelor prelucrate de autoritățile competente privind securitatea cibernetică și nu trebuie să excludă obligația de notificare a cazurilor de încălcare a protecției datelor cu caracter personal în temeiul legislației aplicabile în materie, potrivit art. 21 și 22 din Legea nr.477/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date. Analizând, însă, dispozițiile art.20 alin.(2), Curtea constată că *legiuitorul delegă atribuția sa de legiferare Ministerului pentru Societatea Informațională, ANCOM sau autorităților desemnate, în condițiile legii, în domeniul securității cibernetică, care vor stabili „cerințele minime de securitate cibernetică, modalitatea de notificare, precum și datele și informațiile care însoțesc în mod obligatoriu notificarea, care se aprobă prin ordine sau decizii emise în termen de 90 de zile de la intrarea în vigoare a legii, de conducătorii autorităților sau instituțiilor publice respective, publicate în Monitorul Oficial al României, Partea I”*. ***Trimiterea la acte administrative, cu o forță juridică inferioară legii, într-un domeniu critic pentru securitatea națională, cu impact asupra drepturilor și libertăților fundamentale ale cetățenilor, încalcă prevederile constituționale cuprinse în art.1 alin.(5) referitoare la principiul legalității.*** O dispoziție legală trebuie să fie precisă, neechivocă, să instituie norme clare, previzibile, a căror aplicare să nu permită arbitrariul sau abuzul. De asemenea, norma trebuie să reglementeze în mod unitar, uniform, să stabilească cerințe minimale aplicabile tuturor destinatarilor săi. Or, atâta vreme cât ordinele sau deciziile sunt emise de conducătorii autorităților sau instituțiilor publice desemnate de lege, apare cu evidență că *legea relativizează în mod nepermis reglementarea acestui domeniu, lăsând la latitudinea fiecărei entități stabilirea, în mod diferențiat, a unor măsuri esențiale, precum cerințele minime de securitate cibernetică, modalitatea de notificare, precum și datele și informațiile care însoțesc notificarea.* Pe de altă parte, enumerând autoritățile care stabilesc aceste aspecte, legiuitorul omite chiar Consiliul Suprem de Apărare a Țării, care

potrivit art.9 alin.(1) lit.f) din lege, aprobă propunerile COSC privind cerințele minime de securitate cibernetică și politici de securitate cibernetică pentru autoritățile și instituțiile publice prevăzute la art.10 alin. (1) și (2) din lege.

76. În concluzie, Curtea constată că **dispozițiile art.20 alin.(1) lit.c) și lit.h) coroborate cu art.20 alin.(2) sunt neconstituționale, întrucât contravin prevederilor art.1 alin.(3) și (5), art.26 și art.28 din Constituție.**

77. Din analiza legii, Curtea reține că *aceasta omite să reglementeze posibilitatea subiecților cărora le este destinată legea, în sarcina cărora au fost instituite obligații și responsabilități, de a contesta în justiție actele administrative* încheiate cu privire la îndeplinirea acestor obligații și care sunt susceptibile a prejudicia un drept sau un interes legitim.

78. Potrivit art.21 din Constituție, orice persoană se poate adresa justiției pentru apărarea drepturilor, libertăților și intereselor sale legitime. Prin Decizia nr. 1 din 8 februarie 1994, publicată în Monitorul Oficial al României, Partea I, nr. 69 din 16 martie 1994, Curtea Constituțională a statuat că liberul acces la justiție presupune accesul la toate mijloacele procedurale prin care se înlăptuiește actul de justiție. S-a considerat că legiuitorul are competența exclusivă de a stabili regulile de desfășurare a procesului în fața instanțelor judecătorești, astfel cum rezultă din art. 126 alin. (2) din Constituție. Totodată, în jurisprudența sa (Decizia nr.71 din 15 ianuarie 2009, publicată în Monitorul Oficial al României, Partea I, nr. 49 din 27 ianuarie 2009), Curtea a reținut că liberul acces la justiție este pe deplin respectat ori de câte ori partea interesată, în vederea valorificării unui drept sau interes legitim, a putut să se adreseze cel puțin o singură dată unei instanțe naționale.

79. Pe de altă parte, potrivit art.6 paragraful 1 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, orice persoană are dreptul la judecarea în mod echitabil a cauzei sale, de către o instanță independentă și imparțială, care va hotărî asupra încălcării drepturilor și obligațiilor sale cu caracter civil. Curtea Europeană a Drepturilor Omului a statuat în jurisprudența sa, cu titlu general, că art. 6 paragraful 1 din Convenție

garantează oricărei persoane dreptul de a aduce în fața unei instanțe orice pretenție referitoare la drepturi și obligații cu caracter civil (a se vedea Hotărârea din 21 februarie 1975, pronunțată în Cauza Golder împotriva Marii Britanii, paragraful 36, și Hotărârea din 20 decembrie 2011, pronunțată în Cauza Dokic împotriva Serbiei, paragraful 35). De asemenea, în Hotărârea din 26 ianuarie 2006, pronunțată în Cauza Lungoci împotriva României, paragraful 36, publicată în Monitorul Oficial României, Partea I, nr. 588 din 7 iulie 2006, s-a arătat că accesul liber la justiție implică prin natura sa o reglementare din partea statului și poate fi supus unor limitări, atât timp cât nu este atinsă substanța dreptului.

80. România este un stat de drept în care, potrivit art.1 alin.(5) din Constituție, „respectarea Constituției, a supremației sale și a legilor este obligatorie”. În condițiile în care art.20 alin.(1) din Constituție prevede că dispozițiile constituționale privind drepturile și libertățile cetățenilor vor fi interpretate și aplicate în concordanță cu Declarația Universală a Drepturilor Omului, cu pactele și cu celelalte tratate la care România este parte, iar art.21 din Constituție consacră liberul acces la justiție, a cărei exercitare, potrivit alin.(2), nicio lege nu o poate îngreuna, Parlamentul are îndatorirea de a legifera norme corespunzătoare pentru asigurarea reală a respectării acestui drept, în lipsa căruia nu se poate concepe existența statului de drept, prevăzută prin art.1 alin.(3) din Constituție. Fără îndeplinirea acestei îndatoriri, normele constituționale menționate ar avea un caracter pur declarativ, situație inadmisibilă pentru un stat care împărtășește valorile democratice ce fac parte din ordinea publică europeană, așa cum este prefigurată de Convenția Europeană a Drepturilor Omului și de Carta drepturilor fundamentale a Uniunii Europene (în acest sens, este și Decizia Curții Constituționale nr.233 din 15 februarie 2011, publicată în Monitorul Oficial al României, Partea I, nr.340 din 17 mai 2011).

81. Având în vedere aceste considerente de principiu, Curtea constată că **lipsa oricărei prevederi în conținutul legii prin care să se asigure**

posibilitatea persoanei ale cărei drepturi, libertăți sau interese legitime au fost afectate prin acte sau fapte care au ca temei dispozițiile Legii privind securitatea cibernetică a României de a se adresa unei instanțe judecătorești independente și imparțiale contravine prevederilor art.1 alin.(3) și (5), art.21, precum și art.6 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale.

82. Potrivit dispozițiilor art.27 alin.(1), monitorizarea și controlul aplicării prevederilor legii criticate se asigură, potrivit competențelor stabilite prin lege, de către Camera Deputaților și Senat, Administrația Prezidențială, Guvern, CSAT, precum și instituțiile și autoritățile publice prevăzute la art. 10 alin. (1) și (2), pentru infrastructurile cibernetice proprii sau aflate în responsabilitate, Serviciul Român de Informații pentru infrastructurile cibernetice proprii sau aflate în responsabilitate, precum și pentru deținătorii de ICIN persoane juridice de drept public, Ministerul pentru Societatea Informațională, respectiv ANCOM, după caz, pentru deținătorii de ICIN, persoane juridice de drept privat.

83. *Opțiunea legiuitorului de a atribui competențe de monitorizare și control al aplicării prevederilor legale Camerei Deputaților, Senatului, Administrației Prezidențiale, Secretariatul General al Guvernului și CSAT-ului*, în condițiile în care art.10 alin.(1) și (2) stabilește autoritățile competente în domeniul securității cibernetice privind infrastructurile cibernetice proprii sau aflate în responsabilitate, fără a include în această categorie autoritățile enumerate mai sus, acestea regăsindu-se în întregul act normativ în categoria persoane juridice drept public, în sarcina cărora incumbă respectarea obligațiilor prevăzute de lege, *denotă inconsecvență și generează confuzie cu privire la regimul juridic aplicabil acestor instituții*. Din interpretarea coroborată a dispozițiilor art.20 alin.(1) cu cele ale art.21 alin.(1) lit.a), rezultă că, pe de o parte, Parlamentul, Administrația Prezidențială, Secretariatul General al Guvernului și CSAT au obligația, de exemplu, de a permite efectuarea unor auditări de securitate cibernetică efectuate de SRI sau de a notifica CNSC cu

privire la riscurile și incidentele cibernetice, pe de altă parte, *ele vor monitoriza și controla respectarea acestor obligații, iar, în cazul neîndeplinirii dispozițiilor legale, potrivit art.28 coroborat cu art30 lit.c) din lege, autoritățile își vor aplica lor însele sancțiuni, ca urmare a constatării contravențiilor.* Curtea constată, așadar, că legiuitorul eludează principiile de drept potrivit cărora controlul trebuie efectuat de o entitate independentă, exterioară autorității controlate, iar prin normele edictate face iluzorie respectarea obligațiilor referitoare la securitatea cibernetică. Mai mult, dispozițiile în temeiul cărora Parlamentul, Administrația Prezidențială, Secretariatul General al Guvernului și CSAT devin agenți constatatori ai săvârșirii de contravenții și dispun aplicarea de sancțiuni contravenționale vădesc ignorarea principiilor de drept care guvernează un stat democratic, respectiv a **principiului separației puterilor în stat, prevăzut de art.1 alin.(4) din Constituție și a principiului legalității, consacrat de art.1 alin.(5).** Astfel, în virtutea legii criticate, autoritatea legiuitoare, administrația prezidențială, Guvernul sau CSAT, autorității de rang constituțional ale căror atribuții sunt expres prevăzute în Legea fundamentală, *se subrogă în atribuții care, potrivit Ordonanței Guvernului nr.2/2001 privind regimul juridic al contravențiilor (la care legea criticată face, de altfel, trimitere), revin în competența autorităților administrației publice centrale sau locale.*

84. Pe de altă parte, Curtea observă că ***legea supusă controlului nu stabilește competențe de control și monitorizare față de toți deținătorii de infrastructuri cibernetice, dispozițiile art.27 alin.(1) stabilind aceste competențe doar în ceea ce privește persoanele juridice de drept public sau privat, deținătoare de ICIN.*** Or, în condițiile în care legea prevede, la art.15, 16 și 17, obligații și responsabilități pentru toate persoanele juridice de drept public sau privat deținătoare de infrastructuri cibernetice, iar art.28 lit.a), b), c) califică drept contravenții nerespectarea respectivelor obligații, *omisiunea legislativă cu privire la autoritatea competentă să efectueze controlul deținătorilor de infrastructuri care nu sunt calificate ICIN viciază constituționalitatea textului*

legal cuprins în art.27 alin.(1), din perspectiva art.1 alin.(5) din Constituție.

Normele edictate în materie contravențională, atât în ceea ce privește fapta incriminată, cât și procedura de constatare și sancționare a acesteia, trebuie să fie clare, precise, previzibile, astfel încât destinatarul lor să își poată conforma conduita prescripției legale.

85. De asemenea, Curtea reține că dispozițiile **art.30** din lege conțin prevederi referitoare la constatarea contravențiilor și aplicarea sancțiunilor. Curtea face o primă observație cu privire la **confuzia generată de textul legal ca urmare a necorelării cu prevederile art.28** care consacră contravențiile săvârșite prin nerespectarea dispozițiilor legale. Astfel, Curtea identifică: *omisiunea identificării autorității competente să constate și să aplice sancțiunea pentru contravențiile prevăzute de art.28 lit.i) și j) săvârșite de persoane juridice de drept privat; omisiunea identificării autorității competente să constate și să aplice sancțiunea pentru contravențiile prevăzute de art.28 lit.a), i) și j) săvârșite de persoane juridice de drept public; sancționarea contravențională reglementată de art.30 lit.c) pentru nerespectarea unor obligații de către autoritățile și instituțiile publice prevăzute la art.27 alin.(1) lit. a) din lege, cu privire la infrastructurile cibernetice proprii, obligații de la care acestea erau exceptate, potrivit art.20 alin.(1) teza a doua (contravenții prevăzute de art.28 li.e)-h) din lege).*

86. În jurisprudența sa, Curtea Constituțională a reținut în repetate rânduri că orice act normativ trebuie să îndeplinească anumite condiții calitative, printre acestea numărându-se previzibilitatea, ceea ce presupune că acesta *trebuie să fie suficient de precis și clar pentru a putea fi aplicat* (a se vedea, 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 același sens, Curtea Europeană a Drepturilor Omului a statuat că legea trebuie, într-adevăr, să fie

accesibilă justițiabilului și previzibilă în ceea ce privește efectele sale. Pentru ca legea să satisfacă cerința de previzibilitate, ea trebuie să precizeze cu suficientă claritate întinderea și modalitățile de exercitare a puterii de apreciere a autorităților în domeniul respectiv, ținând cont de scopul legitim urmărit, pentru a oferi persoanei o protecție adecvată împotriva arbitrariului. În plus, nu poate fi considerată "lege" decât *o normă enunțată cu suficientă precizie, pentru a permite cetățeanului să își adapteze conduita în funcție de aceasta*; apelând la nevoie la consiliere de specialitate în materie, el trebuie să fie capabil să prevadă, într-o măsură rezonabilă, față de circumstanțele speței, consecințele care ar putea rezulta dintr-o anumită faptă (a se vedea Hotărârea din 4 mai 2000, pronunțată în *Cauza Rotaru împotriva României*, paragraful 52, și Hotărârea din 25 ianuarie 2007, pronunțată în *Cauza Sissanis împotriva României*, paragraful 66).

87. Așa fiind, Curtea apreciază că imprecizia textelor de lege supuse controlului de constituționalitate, constând în *lipsa stabilirii cu suficientă claritate a procedurilor de monitorizare și control, respectiv a celor privind constatarea și sancționarea contravențiilor*, afectează, pe cale de consecință, și garanțiile constituționale și convenționale care caracterizează dreptul la un proces echitabil, inclusiv componenta sa privind dreptul la apărare. De altfel, Curtea Europeană a Drepturilor Omului a reținut, în esență, că nerespectarea garanțiilor fundamentale, care protejează presupușii autori ai unor fapte ilicite, în fața posibilelor abuzuri ale autorităților desemnate să-i urmărească și să-i sancționeze, reprezintă un aspect ce trebuie examinat în temeiul art. 6 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale (a se vedea, spre exemplu, Hotărârea din 4 octombrie 2007, pronunțată în *Cauza Anghel împotriva României*, paragraful 68).

88. Pentru ca dreptul la un proces echitabil să nu rămână teoretic și iluzoriu, normele juridice trebuie să fie clare, precise și explicite, astfel încât să îl poată avertiza în mod neechivoc pe destinatarul acestora asupra gravității consecințelor nerespectării enunțurilor legale pe care le cuprind. În lumina celor

enunțate mai sus, Curtea reține că, în mod evident, prevederile art.27 alin.(1) și 30 din lege, caracterizate printr-o tehnică legislativă deficitară, **nu întrunesc exigențele de claritate, precizie și previzibilitate și sunt astfel incompatibile cu principiul fundamental privind respectarea Constituției, a supremației sale și a legilor, prevăzut de art.1 alin. (5) din Constituție și cu dreptul la un proces echitabil, prevăzut de art.21 alin. (3) din Constituție, precum și de art.6 din Convenția pentru apărarea drepturilor omului și a libertăților fundamentale.**

89. Potrivit dispozițiilor art.27 alin.(2) din lege, în cadrul activității de monitorizare și control, persoanele desemnate de conducătorii autorităților prevăzute la art.27 alin.(1) ***au dreptul să solicite declarații sau orice documente necesare pentru efectuarea controlului, să facă inspecții, inclusiv inopinate, la orice instalație, incintă sau infrastructură, destinate ICIN***, și să primească, la cerere sau la fața locului, informații sau justificări. Norma cuprinsă în art.27 alin.(2) lit.b) care permite autorităților publice prevăzute de art.10 alin.(1) și (2) din lege să facă inspecții la orice instalație, incintă sau infrastructură destinată ICIN, aflată în responsabilitatea lor, presupune accesul la o anumită locație, cu privire la anumite obiecte, sisteme informatice de stocare, prelucrare și transmitere a datelor, inclusiv a celor cu caracter personal, acces care pune în discuție protecția drepturilor constituționale la viață intimă, familială și privată și la secretul corespondenței. Or, în măsura în care noțiunile cu care legea operează (instalații, incinte și infrastructuri) nu sunt în mod predictibil determinate, iar sfera datelor asupra cărora se realizează controlul este incertă, Curtea apreciază că legea criticată nu reglementează garanții care să permită o protecție eficientă împotriva riscurilor de abuz, precum și față de orice accesare și utilizare ilicită a datelor cu caracter personal. În vreme ce noțiunea de infrastructură cibernetică e definită prin lege, noțiunea de *instalație* folosită în textul de art.27 alin.(2) lit.b) poate reprezenta tot un sistem informatic ori o rețea sau serviciu de comunicații electronice, având în vedere domeniul de reglementare al legii și definițiile cuprinse în aceasta, astfel că accesul la aceste

sisteme informatice nu poate fi permis decât cu autorizarea judecătorului. De asemenea, noțiunea de *incintă* poate semnifica și locul unde se găsesc aceste sisteme informatice, caz în care Curtea reține că sunt aplicabile dispozițiile privind percheziția domiciliară prevăzută de art.157-167 din Codul de procedură penală, în sensul că această măsură nu poate fi dispusă decât de un judecător.

90. Față de cele prezentate, trimiterea la „*respectarea prevederilor legale în vigoare*” este una confuză, întrucât nu sunt identificate ca fiind prevederi aplicabile nici dispozițiile Codului de procedură penală, indicate mai sus, și nici prevederile altor acte normative.

91. Prin urmare, considerentele Deciziilor Curții Constituționale nr.440/2014 și nr.461/2014 sunt valabile *mutatis mutandis*, astfel că argumentele expuse în prealabil cu privire la neconstituționalitatea dispozițiilor art.17 alin.(1) lit.a) din Legea privind securitatea cibernetică a României sunt pe deplin sustenabile și în ceea ce privește **dispozițiile art.27 alin.(2) din lege**. Așa fiind, Curtea conchide că acestea **încalcă prevederile art.1 alin.(5), art.26, art.28, și art.53 din Constituție**.

92. Dincolo de aspectele punctuale a căror neconstituționalitate a fost motivată *supra*, Curtea constată că întregul act normativ suferă de deficiențe sub aspectul respectării normelor de tehnică legislativă, a coerenței, a clarității, a previzibilității, **de natură a determina încălcarea principiului legalității, consacrat de art.1 alin.(5) din Constituție**. Astfel, legea face trimiteri în mai multe cazuri la *reglementarea unor aspecte esențiale în economia domeniului reglementat la acte legislative secundare*, precum hotărâri de Guvern, norme metodologice, ordine sau decizii sau „proceduri stabilite de comun acord”. A se vedea în acest sens dispozițiile art.15 alin.(2), art.17 alin.(1) lit.b), art.19 alin.(1) și (3), art.20 alin.(2), art.23 alin.(2), (5) și (6), art.30 lit.d) din lege.

93. De asemenea, cu excepția cazurilor în care trimiterea vizează chiar legea securității cibernetice, situație în care s-a folosit sintagma „prezenta lege”, *legea folosește în repetate rânduri sintagmele „potrivit legii”, „conform competențelor prevăzute de lege” sau „în condițiile legii”, fără a preciza*

*concret la dispozițiile căror legi se face trimiterea. Această situație se regăsește în cuprinsul art.7 alin.(1) lit.d), art.10 alin.(2) și (5), art.11 alin.(1) lit.j), art.15 alin.(8), art.19 alin.(6), art.20 alin.(1) lit.h), art.21 alin.(1), art.21 alin.(2) lit.d), art.27 alin.(1), art.27 alin.(2) lit.b) din lege. Cu privire la aceste aspecte, Curtea menționează că, potrivit art.39 alin.(1) - *Referirea la alt act normativ*, din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, **„referirea într-un act normativ la alt act normativ se face prin precizarea categoriei juridice a acestuia, a numărului său, a titlului și a datei publicării acelu act sau numai a categoriei juridice și a numărului, dacă astfel orice confuzie este exclusă.”***

94. Pe de altă parte, Curtea constată că dispozițiile art.6 alin.(1), art.8 alin.(1) și ale art.10 alin.(1) teza a doua din lege consacră ***organisme/instituții/autorități înființate în baza unor acte normative anterioare, respectiv hotărâri ale Guvernului (SNSC și COSC) sau hotărâri ale Consiliului Suprem de Apărare a Țării (CNSC)***, care au precedat apariția actului de reglementare primară prin care se stabilește cadrul general de reglementare a domeniului securității cibernetice. Astfel, prin adoptarea lor se creează confuzie cu privire la stabilirea datei de la care aceste entități iau ființă și își exercită competențele - data adoptării hotărârii de Guvern/hotărârii CSAT sau data la care va intra în vigoare Legea securității cibernetice în România.

95. În ceea ce privește aspectele referitoare la criteriile de claritate, precizie, previzibilitate și predictibilitate pe care un text de lege trebuie să le îndeplinească, Curtea constată că autoritatea legiuitoare, Parlamentul sau Guvernul, după caz, are obligația de a edicta norme care să respecte trăsăturile mai sus arătate. Potrivit art.8 alin.(4) teza întâi din Legea nr.24/2000, **„textul legislativ trebuie să fie formulat clar, fluent și inteligibil, fără dificultăți sintactice și pasaje obscure sau echivoce”**, iar potrivit art.36 alin.(1) din aceeași lege, **„actele normative trebuie redactate într-un limbaj și stil juridic specific normativ, concis, sobru, clar și precis, care să excludă orice echivoc, cu respectarea strictă a regulilor gramaticale și de ortografie”**.

96. Curtea constată că prin reglementarea normelor de tehnică legislativă legiuitorul a impus o serie de criterii obligatorii pentru adoptarea oricărui act normativ, a căror respectare este necesară pentru a asigura sistematizarea, unificarea și coordonarea legislației, precum și conținutul și forma juridică adecvate pentru fiecare act normativ. Astfel, respectarea acestor norme concură la asigurarea unei legislații care respectă principiul securității raporturilor juridice, având claritatea și previzibilitatea necesară.

97. Pentru toate argumentele prezentate, **Curtea constată că Legea privind securitatea cibernetică a României este viciată în integralitatea ei, astfel că obiecția de neconstituționalitate urmează a fi admisă și constatată neconstituționalitatea actului normativ, în ansamblul său.**

98. În acord cu jurisprudența sa, Curtea reține că, în situația determinată de constatarea neconstituționalității legii în ansamblul său, pronunțarea unei astfel de decizii are un efect definitiv cu privire la actul normativ, consecința fiind încetarea procesului legislativ în privința respectivei reglementări.

99. Pe de altă parte, în condițiile în care prevederile art.61 alin.(1) din Constituție stabilesc că „Parlamentul este organul reprezentativ suprem al poporului român și unica autoritate legiuitoare a țării”, competența de legiferare a acestuia cu privire la un anumit domeniu nu poate fi limitată dacă legea astfel adoptată respectă exigențele Legii fundamentale. Prin urmare, opțiunea legiuitorului de a legifera în materia în care Curtea Constituțională a admis o sesizare de neconstituționalitate cu privire la o lege în ansamblul său presupune parcurgerea tuturor fazelor procesului legislativ prevăzut de Constituție și de regulamentele celor două Camere ale Parlamentului (a se vedea în acest sens Decizia Curții Constituționale nr.308 din 28 martie 2012, publicată în Monitorul Oficial al României, Partea I, nr.309 din 9 mai 2012).

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

CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

Admite obiecția de neconstituționalitate și constată că Legea privind securitatea cibernetică a României este neconstituțională, în ansamblul ei.

Definitivă și general obligatorie.

Decizia se comunică Președintelui României, președinților celor două Camere ale Parlamentului și prim-ministrului și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 21 ianuarie 2015.