DECIZIA nr.17
din 21 ianuarie 2015

asupra obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind securitatea cibernetică a României

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

1. Pe rol se află pronunţarea asupra obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind securitatea cibernetică a României, obiecţie formulată de un număr de 69 de deputaţi aparţinând Grupului parlamentar al Partidului Naţional Liberal din Camera Deputaţilor.

2. Cu Adresa nr.2/6103 din 23 decembrie 2014, Secretarul general al Camerei Deputaţilor a transmis Curţii Constituţionale sesizarea de neconstituţionalitate, care a fost înregistrată la Curtea Constituţională sub nr.6188 din 23 decembrie 2014 şi constituie obiectul Dosarului nr.1419A/2014. La sesizare a fost anexată, în copie, Legea privind securitatea cibernetică a României.

3. **În motivarea obiecţiei de neconstituţionalitate**, autorii susţin că dispoziţiile legale sunt contrare art.1 alin.(3) şi (4) referitor la statul de drept şi obligaţia respectării Constituţiei şi a legilor. Se apreciază că legea criticată introduce multe confuzii şi condiţionări pentru deţinătorii de infrastructuri cibernetice care sunt de natură a genera restrângeri ale drepturilor şi libertăţilor fundamentale ale cetăţenilor. Prevederile legale nu respectă dispoziţiile art.6 din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea

actelor normative şi încalcă, astfel, principiul legalităţii, care este fundamental pentru buna funcţionare a statului de drept. La art.1 din lege se prevăd doar obligaţii pentru deţinătorii de infrastructuri cibernetice fără a se stabili şi drepturile acestora. Enumerarea cuprinsă în art.2 a persoanelor/entităţilor cărora li se aplică legea nu este una precisă, omiţând să prevadă situaţia intermediarilor de infrastructuri cibernetice, a infrastructurilor neoperaţionale, a acţionarilor unor persoane juridice sau cea a fondatorilor unor asociaţii sau fundaţii care deţin astfel de infrastructuri.

4. Autorii sesizării susţin că legea are probleme fundamentale de concepţie, propunând o serie de măsuri cu efect limitativ asupra dreptului prevăzut de art.26 alin.(1) din Constituţie privind viaţa intimă, familială şi privată, şi încalcă în mod evident reglementările europene aflate în dezbatere referitoare la securitatea informaţiei în domeniul digital.

5. În temeiul legii criticate, autorii obiecției de neconstituționalitate susțin că se restrâng drepturi şi libertăţi ale cetăţenilor prin permiterea accesului la o infrastructură cibernetică şi la datele conţinute de aceasta în urma unei simple solicitări motivate a instituţiilor nominalizate de lege, comunicate deţinătorilor de infrastructuri, fără aprobarea prealabilă a unui judecător, aşa cum prevede Codul de procedură penală sau jurisprudenţa Curţii Constituţionale, în Deciziile nr.440/2014 şi nr.461/2014, fapt ce determină încălcarea prevederilor constituţionale cuprinse în art.23 alin.(1) referitor la inviolabilitatea libertăţii individuale şi a siguranţei persoanei şi în art.28 privind secretul corespondenţei.

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 şi 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, şi nu ar trebui să desfăşoare activităţi în domeniul informațiilor", Parlamentul României acordă acces nelimitat şi nesupravegheat la toate datele informatice deținute de persoane de drept public şi privat unor instituții care nu îndeplinesc niciuna din condițiile de mai sus. Faptul că în jurisprudenţa recentă a Curţii Constituţionale, aceasta a declarat neconstituţionalitatea a două legi care, în esenţă, încălcau aceleaşi drepturi ca şi legea supusă în prezent controlului, constituie un motiv serios pentru o dezbatere reală a implicaţiilor Legii securităţii cibernetice şi, într-un cadru mai larg, a echilibrului dintre drepturile individuale şi securitatea naţională pe care România trebuie 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 corespondenţei, adică în dreptul la viață privată, drept garantat de art. 26 şi 28 din Constituţie. O astfel de ingerință nu numai că nu este necesară într-o societate democratică, dar ea are tocmai efectul contrar: subminează esența societăţii democratice. Astfel, sub pretextul protecției împotriva atacurilor cibernetice, orice fel de date pot fi accesate la bunul plac al puterii executive, fără existenţa vreunui control al societăţii civile.

7. În sesizarea de neconstituționalitate, se arată că art.148 alin.(2) din Constituţie este, de asemenea, încălcat prin netranspunerea corectă a reglementărilor comunitare în materie. Astfel, prevederile art.17 alin.(1) lit.a) nu sunt conforme cu jurisprudenţa Curţii de Justiţie a Uniunii Europene, întrucât nu precizează exact ce date sunt necesare a fi deţinute, iar cadrul în care se solicită aceste date nu prezintă suficiente garanţii procesuale. Pentru îndeplinirea acestei obligaţii este necesară o monitorizare perpetuă a tuturor persoanelor, aspect ce creează o sarcină disproporţionată pentru subiecţii vizaţi şi implică totodată încălcarea drepturilor persoanelor monitorizate fără să existe în legătură cu acestea o suspiciune relativă la comiterea vreunei infracţiuni. Se mai arată că legea contravine din multe puncte de vedere şi 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 şi 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 ambiguităţi prezente în lege, începând de la definirea vagă a deținătorilor de sisteme informatice şi continuând cu obligațiile ce le revin celor care cad sub incidenţa legii.”

8. În concluzie, autorii obiecţiei de neconstituţionalitate 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”. Deşi 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, aşa 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 faţa atacurilor cibernetice, situație ce poate submina garanția unui proces echitabil”.

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

10. **Preşedintele Camerei Deputaţilor** a transmis cu Adresa nr.2/51/7 ianuarie 2015, înregistrată la Curtea Constituţională sub nr.99 din 7 ianuarie 2015, punctul său de vedere, în care se apreciază că sesizarea de neconstituţionalitate 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 relaţiilor sociale ce reprezintă obiectul de reglementare al acestei legi. Astfel, legea porneşte de la premisa că măsurile privind securitatea cibernetică trebuie să asigure un mediu virtual sigur, care să constituie un real suport pentru maximizarea beneficiilor cetăţenilor, mediului de afaceri şi societăţii româneşti, în ansamblul ei. Toţi deţinătorii şi utilizatorii de infrastructuri cibernetice, indiferent că sunt intermediari sau nu, trebuie să întreprindă măsurile necesare pentru securitatea infrastructurilor proprii şi să nu afecteze securitatea celorlalţi deţinători sau utilizatori.

12. Pe de altă parte, se arată că, întrucât dispoziţiile acestei legi se aplică numai persoanelor juridice de drept public sau privat, deţinătoare de infrastructuri cibernetice, nu şi persoanelor fizice, dispoziţiile art. 26 alin. (1) din Constituţie nu au incidenţă.

13. În ceea ce priveşte criticile aduse art.17 din lege referitoare la accesul la date, Preşedintele Camerei Deputaţilor susţine că legea vizează datele relevante luării masurilor proactive şi reactive la nivelul infrastructurilor cibernetice, şi nicidecum datele de trafic, astfel încât nu se aduce atingere drepturilor prevăzute la art. 23 şi 28 din Legea fundamentală. Mai mult decât atât, dispoziţiile art.12 şi 14 din legea criticată prevăd că autorităţile şi instituţiile publice cu atribuţii în aplicarea acestei legi asigură securitatea infrastructurilor cibernetice potrivit legii şi competenţelor legale. Aceste entităţi sunt aşadar obligate şi limitate strict de respectarea cadrului legal.

14. Cu privire la desemnarea Serviciului Român de Informaţii ca autoritate naţională în domeniul securităţii cibernetice, se arată, pe de o parte, că Directiva NIS nu impune statelor membre ale Uniunii Europene desemnarea unei autorităţi civile, şi, pe de altă parte, că, potrivit art.1 din Legea nr.14/1992 privind organizarea şi funcţionarea Serviciului Român de Informaţii, activitatea acestei instituţii este supusă controlului parlamentar efectuat prin intermediul Comisiei comune permanente a Camerei Deputaţilor şi a Senatului.

15. **Guvernul** a transmis punctul său de vedere prin Adresa nr.5/7033/2014 înregistrată la Curtea Constituţională 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 desfăşurate 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 neconstituţionalitate formulate, Guvernul apreciază că „citirea atentă a legii demonstrează că aceste aspecte nu sunt reale, ci se bazează pe o interpretare tendenţioasă a art.17 din lege, respectiv nu se ia în considerare contextul general de asigurare a securităţii cibernetice”. Se arată că autorităţile competente la care face referire articolul vor avea acces la date relevante ale deţinătorilor 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 şi transmitere a datelor (log-uri), date tehnice sau date de configurare ale sistemelor informatice, şi nu includ mesaje ori alte date de conţinut. În situația în care în urma analizei preliminare se constată că se impun investigații aprofundate asupra datelor de conținut, accesul la acestea şi orice alte activităţi care vizează restrângerea unor drepturi şi libertăţi 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 ineficient ca autoritățile competente să aştepte un aviz întocmit de un procuror şi analizat şi aprobat de un judecător pentru a obţine acces la date tehnice care nu lezează în vreun fel drepturile şi libertățile constituționale. Este fizic imposibil ca fiecare dintre aceste incidente să fie investigate, de aceea autoritățile competente se concentrează doar asupra celora care pot produce efecte negative semnificative, inclusiv în planul securității naționale. Guvernul susţine 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 şi „situaţiile în care apar intermediari ce pun la dispoziţie astfel de infrastructuri”, Guvernul menţionează că în cazurile în care apar astfel de intermediari în fluxul infrastructurilor cibernetice, aceştia se circumscriu calităţii de deţinători de astfel de infrastructuri, aşa cum sunt definiţi la art.2 din lege.

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

19. **Preşedintele Senatului** nu a comunicat punctul său de vedere asupra obiecţiei de neconstituţionalitate.

CURTEA,

examinând obiecţia de neconstituţionalitate, raportul judecătorului-raportor, punctele de vedere ale Preşedintelui Camerei Deputaţilor şi Guvernului, dispoziţiile Legii privind securitatea cibernetică a României, precum şi prevederile Constituţiei, reţine următoarele:

20. Curtea a fost legal sesizată şi este competentă, potrivit dispoziţiilor art.146 lit. a) din Constituţie şi ale art.1, art.10, art.15, art.16 şi art.18 din Legea nr.47/1992, să se pronunţe asupra constituţionalităţii prevederilor legale criticate.

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

22. Dispoziţiile constituţionale pretins a fi încălcate sunt cele ale art.1 alin.(3) şi (5) referitoare la statul de drept şi obligaţia respectării legii şi a supremaţiei Constituţiei, art.23 alin.(1) referitor la inviolabilitatea libertăţii individuale şi a siguranţei persoanei, art.26 privind viaţa intimă, familială şi privată, art.28 privind secretul corespondenţei, precum şi cele ale art.148 referitor la integrarea în Uniunea Europeană.

23. Examinând obiecţia de neconstituţionalitate, Curtea reţine că Legea privind securitatea cibernetică a României, care are ca scop completarea cadrului

legislativ în materia securităţii naţionale, a fost iniţiată de Guvernul României şi, ulterior, adoptată de Parlament în data de 19 decembrie 2015. În „Expunerea de motive" care însoţeşte legea, Guvernul afirmă că, „prin adoptarea acestuia act normativ, România va continua să transmită semnale puternice de racordare la realităţile internaţionale, fiind pe deplin conştientă de necesitatea armonizării cu demersurile similare ale statelor europene", în lipsa unei atare reglementări, „ţara noastră nu-şi va putea armoniza demersurile pe dimensiunea securităţii cibernetice cu cele ale partenerilor săi din Uniunea Europeană şi NATO, demersuri necesare unei abordări coerente şi suficiente a provocărilor şi oportunităţilor spaţiului cibernetic".

24. Cu privire la aspectele invocate, Curtea ia act de faptul că, la nivel european, în temeiul art.114 din Tratatul privind funcţionarea Uniunii Europene, a fost iniţiată procedura legislativă ordinară de adoptare a unei directive privind măsuri de asigurare a unui nivel comun ridicat de securitate a reţelelor şi a informaţiei în Uniune – Directiva NIS (Network and Information Security). Iniţiativa aparţine Comisiei Europene, care la data de 7 februarie 2013 a transmis propunerea de directivă Consiliului şi 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 parţial cu privire la modificările Parlamentului. *Prin urmare, la data soluţionării cauzei deduse judecăţii Curţii Constituţionale, 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 reţinute la nivelul instituţiilor 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 rezilienţei şi stabilităţii reţelelor şi a sistemelor informatice, care sunt esenţiale pentru definitivarea pieţei digitale unice şi pentru buna funcţionare a pieţei interne* şi, pe de altă parte, în asigurarea unei capacităţi şi a

unei pregătiri similare la nivelul statelor membre de natură să ofere o securitate globală a reţelelor şi a informaţiei 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 capacităţi naţionale prin înfiinţarea autorităţilor competente în materie de reţele şi sisteme informatice*, să creeze echipe de intervenţie în caz de urgenţă informatică *(Computer Emergency Response Teams - CERT)* şi *să adopte strategii naţionale privind securitatea cibernetică şi planurile naţionale de cooperare* în domeniul vizat; în al doilea rând, *autorităţile naţionale competente trebuie să coopereze în cadrul unei reţele* care să permită o coordonare sigură şi eficace, inclusiv schimbul coordonat de informaţii la nivelul U.E., pentru a contracara ameninţările şi incidentele în materie de securitate cibernetică, pe baza planului european de cooperare în domeniu; în al treilea rând, conform modelului Directivei-cadru privind comunicaţiile electronice, propunerea urmăreşte să asigure dezvoltarea unei culturi a gestionării riscurilor şi partajarea informaţiilor de către sectoarele public şi privat.

26. De asemenea, Curtea reţine considerentul 41 al preambulului directivei care prevede că *„Prezenta directivă respectă drepturile fundamentale şi principiile recunoscute de Carta drepturilor fundamentale a Uniunii Europene*, în special dreptul la *respectarea vieţii private şi a secretului comunicaţiilor, dreptul la protecţia datelor cu caracter personal*, libertatea de a desfăşura o activitate comercială, dreptul de proprietate, *dreptul la o cale de atac eficientă în faţa unei instanţe judecătoreşti* şi dreptul de a fi ascultat. Prezenta directivă trebuie pusă în aplicare în conformitate cu aceste drepturi şi principii."

27. Propunerea de directivă, în forma adoptată de Parlamentul European, conţine mai multe dispoziţii cu caracter obligatoriu pentru statele membre, dispoziţii care ar urma să fie transpuse în legislaţia naţională a fiecărui stat. Astfel, preambulul directivei NIS (considerentul 10) prevede că autorităţile competente şi punctele unice de contact ar trebui să fie ***organisme civile***, care *să*

funcţioneze integral pe baza controlului democratic, şi care ***nu ar trebui să desfăşoare activităţi în domeniul informaţiilor***, al aplicării legii sau al apărării şi *nici să fie legate organizaţional în vreun fel de organismele active în aceste domenii*. Astfel, dispoziţiile art.6 din directivă, în forma modificată de PE, prevăd că „(1) ***Fiecare stat membru desemnează una sau mai multe autorităţi naţionale civile*** competente în domeniul securităţii reţelelor şi a sistemelor informatice."

28. În propunerea de Directivă NIS ***nu se prevede dreptul autorităţilor desemnate de a accesa, la solicitarea motivată, datele stocate în reţelele şi sistemele informatice***, aşa cum prevede art.17 alin.(1) lit.a) din legea supusă controlului de constituţionalitate, ci doar obligaţia de notificare a riscurilor şi incidentelor cibernetice (art.14) şi de a se supune auditării pentru deţinătorii de infrastructuri critice (art.15). Astfel, în cazurile în care notificările conţin date cu caracter personal, acestea sunt comunicate doar destinatarilor din cadrul autorităţilor competente care trebuie să prelucreze aceste date pentru a-şi 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 autorităţile competente sunt împuternicite să solicite operatorilor de piaţă 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 naţională***, şi să transmită dovezile autorităţii competente sau punctului unic de contact"- art.15 alin.(2) din directivă.

29. De asemenea, art.3 din propunerea de directivă defineşte noţiunea de ***operator de piaţă***, ca fiind „un operator al unei infrastructuri care este esenţială pentru menţinerea activităţilor economice şi societale vitale în domeniile energiei, transporturilor, serviciilor bancare, pieţelor financiare, IXP (Internet Exchange points), lanţurilor de aprovizionare alimentară şi sănătăţii, activităţi 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, şi, pe de altă parte, *domeniile referitoare la serviciile esenţiale*, precum energie, transporturi, bănci, infrastructuri ale pieței financiare şi sectorul sănătății. De asemenea, sub incidenţa proiectului de Directivă şi, deci, a prevederilor privind securitatea cibernetică intră şi *domeniul administraţiilor publice* (pct.26 din Preambul şi 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 stabileşte că ***microîntreprinderile nu intră sub incidenţa directivei cu excepţia situaţiei în care acestea acţionează în calitate de filială a unui operator de piaţă***.

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

32. La momentul efectuării controlului de constituţionalitate, Curtea reţine că, în legislaţia naţională în domeniul securităţii, există deja în vigoare o serie de reglementări, acte normative cu caracter primar sau secundar. Astfel,

Ordonanţa de urgenţă a Guvernului nr.98/2010 privind identificarea, desemnarea şi protecţia 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, stabileşte cadrul legal privind identificarea, desemnarea infrastructurilor critice naţionale/europene şi evaluarea necesităţii de a îmbunătăţi protecţia acestora, în scopul creşterii capacităţii de asigurare a stabilităţii, securităţii şi siguranţei sistemelor economico-sociale şi protecţiei persoanelor. Ordonanţa transpune prevederile Directivei 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, publicată în Jurnalul Oficial al Uniunii Europene nr. L 345 din 23 decembrie 2008. Actul normativ *defineşte infrastructura critică naţională*, denumită ICN ca fiind un element, un sistem sau o componentă a acestuia, aflat pe teritoriul naţional, care este esenţial pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, siguranţei, securităţii, bunăstării sociale ori economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii. Actul normativ *stabileşte criteriile intersectoriale de identificare a ICN*: criteriul privind victimele, evaluat în funcţie de numărul posibil de decese sau vătămări; criteriul privind efectele economice, evaluat în funcţie de importanţa pierderilor economice şi/sau a degradării produselor sau serviciilor, inclusiv eventualele efecte asupra mediului; criteriul privind efectul asupra populaţiei, evaluat în funcţie de impactul asupra încrederii acesteia, suferinţa fizică sau perturbarea vieţii cotidiene, inclusiv pierderea de servicii esenţiale. În conformitate cu procedura prevăzută de ordonanţa de urgenţă, autorităţile publice responsabile identifică potenţialele ICN care corespund criteriilor sectoriale şi intersectoriale. *Actul normativ conţine 3 anexe*: Anexa nr.1 - Lista sectoarelor, subsectoarelor infrastructurii critice naţionale/infrastructurii critice europene (ICN/ICE) şi autorităţilor publice

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

33. În aplicarea ordonanţei de urgenţă, 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 naţională privind protecţia infrastructurilor critice*.

34. ***Hotărârea Guvernului nr.494/2011***, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, *reglementează înfiinţarea* ca instituţie publică cu personalitate juridică, în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, a *Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, structură independentă de expertiză şi cercetare-dezvoltare în domeniul protecţiei infrastructurilor cibernetice.* Centrul este condus de un director general şi de un director general adjunct, sprijiniţi de Comitetul de coordonare, din care fac parte reprezentanţi ai MCSI, Ministerului Apărării Naţionale, Ministerului Administraţiei şi Internelor, Serviciului Român de Informaţii, Serviciului de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat şi ai Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii. Hotărârea de Guvern *defineşte termeni şi expresii precum infrastructură cibernetică, spaţiu cibernetic, securitate cibernetică, atac cibernetic, incident cibernetic* etc., şi stabileşte atribuţiile CERT-RO.

35. Un alt act normativ emis în domeniul securităţii naţionale 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 şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică*.

36. Strategia de securitate cibernetică prezintă obiectivele, principiile şi direcţiile majore de acţiune pentru cunoaşterea, prevenirea şi contracararea ameninţărilor, vulnerabilităţilor şi riscurilor la adresa securităţii cibernetice a României şi pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic. În acest sens, stabileşte semnificaţia termenilor şi expresiilor utilizaţi în domeniu, prevede *înfiinţarea Sistemului naţional de securitate cibernetică (SNSC)* care reprezintă cadrul general de cooperare care reuneşte autorităţi şi instituţii publice, cu responsabilităţi şi capabilităţi în domeniu, în vederea coordonării acţiunilor la nivel naţional pentru asigurarea securităţii spaţiului cibernetic, inclusiv prin cooperarea cu mediul academic şi cel de afaceri, asociaţiile profesionale şi organizaţiile 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 permanenţi, reprezentanţi ai Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informaţională, Serviciului Român de Informaţii, Serviciului de Telecomunicaţii Speciale, Serviciului de Informaţii Externe, Serviciului de Protecţie şi Pază, Oficiului Registrului Naţional pentru Informaţii Secrete de Stat, precum şi secretarul Consiliului Suprem de Apărare a Ţării. Conducerea COSC este asigurată de un preşedinte (consilierul prezidenţial pe probleme de securitate naţională) şi un vicepreşedinte (consilierul prim-ministrului pe probleme de securitate naţională). Coordonatorul tehnic al COSC este Serviciul Român de Informaţii, în condiţiile legii.

37. *Planul de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică* este conţinut în Anexa nr.2 la Hotărâre şi este un document clasificat.

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

impune adoptarea de măsuri necesare dezvoltării mecanismelor de apărare cibernetică. Motivul emiterii actului normativ, aşa cum reiese din „Expunerea de motive” care îl însoţeşte, îl constituie „evoluţia recentă a atacurilor cibernetice din ţara noastră” care determină aprecierea că „România este cu certitudine vizată de entităţi ostile în mediul virtual, nivelul de securitate cibernetică fiind, în prezent, insuficient pentru a face faţă unor atacuri de nivel ridicat ori cu intenţii distructive.” Legea vizează stabilirea cadrului general de reglementare a activităţilor în domeniul securităţii cibernetice, definirea obligaţiilor ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice, precum şi asigurarea cadrului general de cooperare pentru realizarea securităţii cibernetice, prin constituirea Sistemului Naţional de Securitate Cibernetică.

39. Proiectul de lege a fost adoptat, la data de 17 septembrie 2014, de Camera Deputaţilor, în calitate de primă Cameră sesizată, în temeiul art.75 alin.(2) teza a treia din Constituţie – ca urmare a depăşirii 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 Preşedintelui României pentru promulgare, iar în termenul prevăzut de lege, un număr de 69 de deputaţi a formulat cererea de sesizare a Curţii Constituţionale, care face obiectul prezentului dosar.

40. Din analiza documentului elaborat de iniţiatorul legii intitulat „Expunere de motive”, Secţiunea a 6-a - Consultări efectuate în vederea elaborării proiectului de act normativ, la rubrica Informaţii privind avizarea de către autorităţile competente, Curtea constată că Guvernul menţionează doar avizul Consiliului Legislativ.

41. Potrivit dispoziţiilor art.1 din legea criticată, aceasta stabileşte cadrul general de reglementare a activităţilor în domeniul securităţii cibernetice şi obligaţiile ce revin persoanelor juridice de drept public sau privat în scopul protejării infrastructurilor cibernetice, iar dispoziţiile art.3 alin.(1) din lege stabilesc că „securitatea cibernetică este componentă a securităţii naţionale a

României". Cu privire la domeniul de reglementare a actului normativ supus controlului de constituţionalitate, Curtea reţine că, în temeiul prevederilor art.119 din Legea fundamentală, „Consiliul Suprem de Apărare a Ţării organizează şi coordonează unitar activităţile care privesc apărarea ţării şi securitatea naţională, participarea la menţinerea securităţii internaţionale şi la apărarea colectivă în sistemele de alianţă militară, precum şi la acţiuni de menţinere sau de restabilire a păcii". În aplicarea acestor prevederi, art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării, prevede, printre atribuţiile ***CSAT***, că acesta ***„avizează proiectele de acte normative iniţiate sau emise de Guvern privind securitatea naţională"***. 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 iniţiatorul trebuie să solicite avizul autorităţilor interesate în aplicarea acestora, în funcţie de obiectul reglementării". De asemenea, art.31 alin.(3) din aceeaşi lege prevede că „Forma finală a instrumentelor de prezentare şi motivare a proiectelor de acte normative trebuie să cuprindă referiri la avizul Consiliului Legislativ şi, după caz, al Consiliului Suprem de Apărare a Ţării, Curţii de Conturi sau Consiliului Economic şi Social." Aşadar, în temeiul dispoziţiilor legale, Guvernul avea obligaţia de a solicita avizul Consiliului Suprem de Apărare a Ţării atunci când a elaborat proiectul Legii privind securitatea cibernetică a României.

42. Pentru argumentele expuse, întrucât în cadrul procedurii legislative, iniţiatorul nu a respectat obligaţia legală, conform căreia Consiliul Suprem de Apărare a Ţării avizează proiectele de acte normative iniţiate sau emise de Guvern privind securitatea naţională, **Curtea constată că actul normativ a fost adoptat cu încălcarea prevederilor constituţionale ale art.1 alin.(5) care consacră principiul legalităţii, şi ale art.119 referitoare la atribuţiile Consiliului Suprem de Apărare a Ţării.**

43. Examinând conţinutul normativ al legii, Curtea reţine că aceasta prevede înfiinţarea *Sistemului Naţional de Securitate Cibernetică*, denumit SNSC, care reuneşte autorităţile şi instituţiile publice cu responsabilităţi şi capacităţi în domeniu (art.6). Coordonarea unitară a activităţilor SNSC se realizează de către *Consiliul Operativ de Securitate Cibernetică*, denumit COSC (art.8). Serviciul Român de Informaţii este desemnat autoritate naţională în domeniul securităţii cibernetice, calitate în care asigură coordonarea tehnică a COSC, precum şi organizarea şi executarea activităţilor care privesc securitatea cibernetică a României. În acest scop, în structura SRI funcţionează *Centrul Naţional de Securitate Cibernetică*, denumit CNSC (art.10 alin.(1)). Sunt desemnate autorităţi în domeniul securităţii cibernetice pentru domeniile lor de activitate, asigurând securitatea infrastructurilor cibernetice proprii sau aflate în responsabilitate: Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale şi Serviciul de Protecţie şi Pază. *Centrul Naţional de Răspuns la Incidente de Securitate*, denumit în continuare CERT-RO, reprezintă un punct naţional de contact cu structurile de tip CERT care funcţionează în cadrul instituţiilor sau autorităţilor publice ori al altor persoane juridice de drept public sau privat, naţionale ori internaţionale, cu respectarea competenţelor ce revin celorlalte autorităţi şi instituţii publice cu atribuţii în domeniu, potrivit legii (art.10 alin.(5)). Autoritatea implicată în securitatea infrastructurilor cibernetice deţinute sau administrate de furnizorii de reţele publice de comunicaţii electronice sau de servicii de comunicaţii electronice destinate publicului este *Autoritatea Naţională pentru Administrare şi Reglementare în Comunicaţii*, denumită ANCOM (art.13 alin.(2)), instituţie înfiinţată prin Ordonanţa de urgenţă Guvernului nr.22/2009.

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

organizarea şi executarea activităţilor care privesc securitatea cibernetică a României. În acest scop, *în structura SRI funcţionează Centrul Naţional de Securitate Cibernetică (CNSC), care a fost constituit, organizat şi funcţionează deja în cadrul SRI, cu personal militar specializat, potrivit unor hotărâri ale Consiliului Suprem de Apărare a Ţării*. Autorităţile şi instituţiile publice din componenţa COSC deleagă un reprezentant în cadrul CNSC. Potrivit art.11 din lege, principalele atribuţii ale CNSC vizează acţiuni în scopul cunoaşterii, prevenirii, protecţiei, reacţiei şi managementului consecinţelor ameninţărilor şi atacurilor cibernetice; asigurarea schimbului de date şi informaţii între autorităţile şi instituţiile publice componente ale SNSC; analiza şi integrarea datelor şi informaţiilor obţinute de autorităţile şi instituţiile publice componente ale SNSC, în scopul stabilirii, întreprinderii sau propunerii măsurilor ce se impun pentru asigurarea securităţii cibernetice; asigurarea colectării şi identificării evenimentelor survenite în spaţiul cibernetic; primirea notificărilor făcute de persoanele juridice de drept public care deţin sau administrează infrastructuri cibernetice de interes naţional (ICIN); în caz de atac cibernetic, asigurarea colectării şi evaluarea datelor şi informaţiilor cu privire la incident, propunerea sau luarea de măsuri reactive de primă urgenţă pentru asigurarea integrităţii datelor şi remedierea situaţiei de fapt, informarea organelor competente pentru investigare şi cercetare, sau, după caz, sesizarea organelor de urmărire penală.

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

46. Cu privire la desemnarea SRI, recte CNSC, ca autoritate naţională în domeniul securităţii cibernetice, autorii criticilor de neconstituţionalitate susţin că legiuitorul acordă acces nelimitat şi nesupravegheat la toate datele informatice deținute de persoane de drept public şi privat unei instituţii care nu

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

47. În analiza de constituţionalitate, Curtea porneşte de la premisa că strategia de securitate cibernetică și legea privind securitatea cibernetică au un rol important în asigurarea securităţii naţionale a României, pe de o parte, şi 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, pronunţată în *Cauza Klass şi alţii împotriva Germaniei*, Curtea Europeană a Drepturilor Omului a apreciat că „Societăţile democratice sunt ameninţate în prezent de modalităţi complexe de spionaj şi de terorism, astfel că statul trebuie să fie capabil, pentru a combate eficient aceste ameninţări, să supravegheze în mod secret elementele subversive care operează pe teritoriul său" (paragraful 42). Cu toate acestea, Curtea, conştientă de pericolul inerent măsurilor de supraveghere secretă, „de a submina, chiar de a distruge democraţia sub motivul apărării acesteia, afirmă că statele nu pot lua, în numele combaterii spionajului şi terorismului, orice măsură pe care acestea o consideră adecvată" (paragraful 49).

48. În această lumină, Curtea Constituţională trebuie să verifice dacă reglementarea domeniului vizat concordă cu respectarea dreptului la viaţă intimă, familială şi privată, cu inviolabilitatea secretului corespondenţei, cu dreptul la protecţia datelor cu caracter personal, valori fundamentele care ar trebui să reprezinte principii directoare ale politicii de securitate cibernetică la nivel naţional, şi să se asigure că legislaţia adoptată nu conduce la măsuri care ar constitui interferențe neconstituţionale cu drepturile menţionate. Aşa 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 şi rețelelor cibernetice, precum și a informației, care să constituie punctul de contact pentru relaţionarea cu organismele similare din străinătate (aşa cum prevede art.10 alin.(4) din lege), inclusiv al cooperării transfrontaliere la nivelul

Uniunii Europene, trebuie să vizeze *un organism civil, care să funcţioneze 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 priveşte dispoziţiile art.1 alin.(3), teza întâi din Constituţie, care consacră principiul statului de drept, Curtea a reţinut în jurisprudenţa 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 exigenţele acestuia privesc scopurile majore ale activităţii statale, prefigurate în ceea ce îndeobşte este numit ca fiind domnia legii, sintagmă ce implică subordonarea statului faţă de drept, asigurarea acelor mijloace care să permită dreptului să cenzureze opţiunile politice şi, în acest cadru, să pondereze eventualele tendinţe abuzive, discreţionare, ale structurilor etatice. Statul de drept asigură supremaţia Constituţiei, corelarea legilor şi tuturor actelor normative cu aceasta, existenţa regimului de separaţie a puterilor publice, care trebuie să acţioneze în limitele legii, şi anume în limitele unei legi ce exprimă voinţa generală. *Statul de drept consacră o serie de garanţii, inclusiv jurisdicţionale, care să asigure respectarea drepturilor şi libertăţilor cetăţenilor prin autolimitarea statului, respectiv încadrarea autorităţilor publice în coordonatele dreptului*.

50. În analiza Curţii, opțiunea pentru desemnarea în calitate de autoritate naţională în domeniul securității cibernetice a unui organism civil, iar nu a unei entități militare cu activitate în domeniul informaţiilor, se justifică prin necesitatea preîntâmpinării riscului de a deturna scopul legii securităţii cibernetice în sensul folosirii atribuţiilor conferite prin această lege de către serviciile de informaţii în scopul obţinerii de informaţii şi date cu consecinţa încălcării drepturilor constituţionale la viaţă intimă, familială şi privată şi la secretul corespondenţei. Or, tocmai acest lucru nu evită legea supusă controlului de constituţionalitate prin desemnarea SRI și a structurii sale militarizate CNSC.

51. Astfel, examinând atribuţiile stabilite de actul normativ supus controlului, apare cu evidenţă intenţia legiuitorului de a stabili în competenţa

CNSC colectarea tuturor datelor privind starea de securitate a infrastructurii, oricare ar fi natura acestora, atât din mediul public, cât şi din cel privat. Or, în condiţiile în care Centrul Naţional de Securitate Cibernetică constituie o structură militară, în cadrul unui serviciu de informaţii, subordonată ierarhic conducerii acestei instituţii, deci sub un control direct militar-administrativ, apare cu evidenţă că *o atare entitate nu îndeplineşte condiţiile cu privire la garanţiile necesare respectării drepturilor fundamentale referitoare la viaţă intimă, familială şi privată şi la secretul corespondenţei*.

52. De asemenea, în condiţiile în care autoritatea națională desemnată deserveşte drept punct unic de contact național în domeniul securității rețelelor și al sistemelor informatice, asigurând relaţionarea cu organismele similare din cadrul Uniunii Europene, împrejurarea că România desemnează o autoritate care nu ar îndeplini exigenţele actului normativ european, aflat în curs de adoptare, pune sub semnul întrebării atât o eventuală concordanţă a reglementării naţionale cu cea de drept european, cât şi cooperarea efectivă între instituţii care, deşi au acelaşi scop, nu se întemeiază pe o structură organizatorică similară şi nu funcţionează 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 viaţă intimă, familială şi privată, respectiv secretul corespondenţei, din perspectiva lipsei garanţiilor necesare garantării acestor drepturi.**

54. Curtea observă că dispoziţiile art.2 prevăd sfera de incidenţă a legii, sub aspectul destinatarilor săi, arătând că persoanele juridice de drept public sau privat cărora le sunt aplicabile prevederile legale, intitulaţi generic ***deţinători de infrastructuri cibernetice***, sunt: proprietarii, administratorii, operatorii sau utilizatorii de infrastructuri cibernetice, definite la art.5 lit.g) ca fiind infrastructuri din domeniul tehnologiei informaţiei şi comunicaţii, constând în

sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice.

55. Definirea expresiei „deţinători de infrastructuri cibernetice” este deosebit de importantă, deoarece includerea în această categorie implică pentru persoanele vizate obligaţia de a respecta prevederile legii, pe de o parte, şi justificarea pentru autorităţile desemnate de lege cu competenţe în domeniul securităţii cibernetice de a dispune măsuri speciale în ceea ce le priveşte.

56. Obligaţiile care incumbă destinatarilor legii vizează asigurarea rezilienţei infrastructurilor cibernetice, respectiv capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic şi de a reveni la starea de normalitate. Această stare este menţinută în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. ***Includerea în sfera de incidenţă 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-şi îndeplinească obligaţiile şi responsabilităţile prevăzute de lege, în condiţiile 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 obligaţiile şi responsabilităţile 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 şi să prevadă consecinţele 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 constituţionalitate, Curtea reține că acesta nu are un caracter precis şi previzibil, și, prin urmare, **dispozițiile art.2 contravin art.1 alin.(5) din Legea fundamentală**.

58. Curtea reţine că tuturor deţinătorilor de infrastructuri cibernetice le sunt aplicabile dispoziţiile art.16 (care stabilesc obligaţiile ce le incumbă), şi ale art.17 (care consacră responsabilităţile pe care aceştia trebuie să le îndeplinească). Printre responsabilităţile acestor persoane este şi aceea de ***a acorda sprijinul necesar, la solicitarea motivată*** a Serviciului Român de Informaţii, Ministerului Apărării Naţionale, Ministerului Afacerilor Interne, Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, Serviciului de Informaţii Externe, Serviciului de Telecomunicaţii Speciale, Serviciului de Protecţie şi Pază, CERT-RO şi ANCOM, ***în îndeplinirea atribuţiilor ce le revin acestora, şi „să permită accesul reprezentanţilor desemnaţi în acest scop la datele deţinute, 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 modalităţii în care se realizează accesul.

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

vedere că infrastructurile cibernetice constau în sisteme informatice, în rețele şi servicii de comunicaţii 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 viaţa privată*** a persoanelor utilizatoare. Prevederea în temeiul căreia accesul se realizează cu privire la *„datele deţinute, 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 şi transmitere a datelor, datele tehnice, datele de configurare ale sistemelor informatice, mesajele sau orice alte date de conţinut. Lipsa unei reglementări legale precise, care să determine cu exactitate sfera acelor date necesare identificării evenimentelor survenite în spaţiul cibernetic (ameninţări, atacuri sau incidente cibernetice), deschide posibilitatea unor abuzuri din partea autorităţilor 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 chemaţi 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 conexate 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, aplicaţii aferente, reţele şi servicii de comunicaţii electronice) în sensul legii supusă controlului de constituţionalitate se suprapune cu noţiunea de „acces la un sistem informatic”, reglementată de art.138 alin.(1) lit.b) şi 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 distanţă, prin intermediul unor programe specializate ori prin intermediul unei reţele, în scopul de a identifica probe”. De asemenea, în acelaşi context, prin *date deţinute* se înţelege „datele informatice” reglementate de art.138 alin.(5) din Codul de procedură penală, care sunt „orice reprezentare de fapte, informaţii sau concepte, sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic”. Or, accesul la un sistem informatic în scopul obţinerii 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 condiţiile 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 şi cele generate sau prelucrate de către furnizorii de reţele publice de comunicaţii electronice sau furnizorii de servicii de comunicaţii electronice destinate publicului şi reţinute de către aceştia, însă şi acestea pot fi obţinute 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 autorităţile care pot solicita accesul la datele deţinute pe baza formulării unei solicitări motivate, fără a reglementa modalitatea în care se realizează accesul efectiv la datele deţinute, aşa încât persoanele ale căror date au fost păstrate să beneficieze de garanţii suficiente care să le asigure protecţia

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

64. ***Solicitările 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 condiţiile în care măsurile adoptate prin legea supusă controlului de constituţionalitate nu au un caracter precis şi previzibil, ingerinţa statului în exercitarea drepturilor constituţionale la viaţă intimă, familială şi privată şi la secretul corespondenţei, deşi prevăzută de lege, nu este

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

66. În continuarea analizei sale, Curtea observă că, din coroborarea dispoziţiilor art.2 cu art.19 şi art.20 din lege, rezultă că, în cadrul deţinătorilor de infrastructuri cibernetice, *se creează o subcategorie – deţinătorii de infrastructuri cibernetice de interes naţional (ICIN*), care, potrivit art.2 lit.h) din lege, reprezintă infrastructurile cibernetice care susţin servicii publice sau de interes public, ori servicii ale societăţii informaţionale, a căror afectare poate aduce atingere securităţii naţionale, sau prejudicii grave statului român ori cetăţenilor acestuia. Aceştia sunt cuprinşi în ***Catalogul ICIN***, întocmit de Ministerul pentru Societatea Informaţională, cu consultarea COSC, la propunerea CNSC sau, după caz, a CERT-RO, şi a ANCOM. Potrivit art.19 alin.(1), catalogul ***este aprobat prin hotărâre a Guvernului***. ***Identificarea ICIN*** se realizează *pe baza criteriilor de selecţie cuprinse în metodologia elaborată de Serviciul Român de Informaţii şi Ministerul pentru Societatea Informaţională* şi este ***aprobată prin hotărâre de Guvern.***

67. Cu privire la aceste aspecte, Curtea apreciază că ***modalitatea prin care se stabilesc criteriile în funcţie de care se realizează selecţia infrastructurilor cibernetice de interes naţional şi, implicit, a deţinătorilor***

ICIN nu respectă cerinţele de previzibilitate, certitudine şi transparenţă. Astfel, trimiterea la o legislaţie infralegală, respectiv hotărâri de Guvern, acte normative caracterizate printr-un grad sporit de instabilitate, pentru reglementarea criteriilor în funcţie de care devin incidente obligaţii în materia securităţii naţionale încalcă principiul constituţional al legalităţii, consacrat de art.1 alin.(5) din Constituţie. Opţiunea pentru o atare modalitate de reglementare apare cu atât mai nejustificată cu cât într-o materie similară, cea a identificării infrastructurilor critice naţionale, Ordonanţa de urgenţă a Guvernului nr.98/2010 stabileşte în chiar conţinutul său criteriile intersectoriale de identificare a ICN. Mai mult, prin Anexa la actul normativ se aprobă lista sectoarelor, subsectoarelor infrastructurii critice naţionale/infrastructurii critice europene (ICN/ICE) şi autorităţilor publice responsabile (energetic, tehnologia informaţiei şi comunicaţii, alimentare cu apă, alimentaţie, sănătate, securitate naţională, administraţie, transporturi, industria chimică şi nucleară, spaţiu şi cercetare). Or, în cazul Legii privind securitatea cibernetică, dispoziţiile art.19 fac trimitere la acte normative cu forţă juridică inferioară legii, *identificarea ICIN realizându-se pe baza unei metodologii elaborate de Serviciul Român de Informaţii şi de Ministerul pentru Societatea Informaţională, în baza unei proceduri neprevăzute de lege, netransparente, şi deci, susceptibilă de a fi calificată arbitrară*.

68. Prin urmare, Curtea reţine că atât ***criteriile în funcţie de care se realizează selecţia infrastructurilor cibernetice de interes naţional, cât şi modalitatea prin care se stabilesc acestea trebuie prevăzute de lege***, *iar* ***actul normativ de reglementare primară trebuie să conţină o listă cât mai completă a domeniilor în care sunt incidente prevederile legale***.

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

interes naţional pot avea implicaţii asupra securităţii României, prin dimensiunea, dispersia şi accesibilitatea unei astfel de infrastructuri, prin efectele economice, evaluate în funcţie de importanţa pierderilor economice şi/sau a degradării produselor sau serviciilor, prin efectele asupra populaţiei, evaluate în funcţie de impactul asupra încrederii acesteia sau perturbarea vieţii cotidiene, inclusiv prin pierderea unor servicii esenţiale. Or, dispoziţiile legale în forma supusă controlului de constituţionalitate prezintă un grad mare de generalitate, obligaţiile vizând totalitatea deţinătorilor de infrastructuri cibernetice, constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice, indiferent de importanţa acestora care poate viza interesul naţional 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 importanţă nesemnificativă 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 **dispoziţiile art.19 alin.(1) şi (3) din Legea securităţii cibernetice a României încalcă prevederile art.1 alin.(5) din Constituţie, întrucât nu respectă cerinţele de previzibilitate, stabilitate şi certitudine.**

71. În continuare, Curtea reţine că dispoziţiile art.20 şi art.21 alin.(2) din legea criticată prevăd ***obligaţiile care incumbă persoanelor juridice de drept public sau privat care deţin 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 autorităţilor competente potrivit prezentei legi, să constituie structuri sau să desemneze persoane responsabile cu prevenirea, identificarea şi reacţia la incidentele cibernetice, să notifice imediat, după caz, CNSC, CERT-RO, ANCOM sau autorităţile desemnate, în condiţiile

legii, în domeniul securităţii cibernetice cu privire la riscurile şi 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, deţinătorii de ICIN au obligaţia să permită autorităţilor competente să intervină pentru identificarea şi analizarea cauzelor incidentelor cibernetice, respectiv pentru înlăturarea sau reducerea efectelor incidentelor cibernetice, să reţină şi să asigure integritatea datelor referitoare la incidentele cibernetice pentru o perioadă de 6 luni de la data notificării.

72. Legea stabileşte că *sunt exceptate de la aplicarea acestor dispoziţii autorităţile prevăzute la art.10 alin.(1) şi (2) din lege*, respectiv Serviciul Român de Informaţii, Ministerul Apărării Naţionale, Ministerul Afacerilor Interne, Oficiul Registrului Naţional al Informaţiilor Secrete de Stat, Serviciul de Informaţii Externe, Serviciul de Telecomunicaţii Speciale şi Serviciul de Protecţie şi Pază. Or, *Curtea consideră nejustificată această exceptare în condiţiile în care şi autorităţile enumerate desfăşoară activităţi în domeniul securităţii naţionale, sunt deţinătoare de ICIN sau au în responsabilitate ICIN* şi sunt susceptibile a face obiectul unor atacuri cibernetice.

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

aplică sancţiunea, potrivit art.30 lit.c) din lege. Or, *o atare situaţie este inacceptabilă* într-o societate guvernată de principiile statului de drept. Dispoziţiile legale sunt susceptibile de a genera o aplicare discreţionară, chiar abuzivă a legii, fiind nepermis ca toate atribuţiile din domeniul reglementat să fie concentrate în sarcina unei singure instituţii. *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 cibernetice și să transmită rezultatul evaluării efectuate autorității competente sau punctului unic de contact.

74. Pornind de la definiţia noţiunii de „audit de securitate cibernetică", prevăzută în art.5 lit.d), care stabileşte că aceasta reprezintă o evaluare sistematică, detaliată, măsurabilă şi tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, precum şi emiterea de recomandări pentru minimizarea riscurilor identificate, Curtea reţine că, în accepţiunea legii, această auditare presupune doar o evaluare a politicilor de securitate cibernetică şi nicidecum accesul la datele stocate în infrastructurile cibernetice.

75. În ceea ce priveşte norma prevăzută de art.20 alin.(1) lit.h) şi anume ***obligaţia de a notifica imediat, după caz, CNSC, CERT-RO, ANCOM sau autorităţile desemnate***, în condiţiile legii, în domeniul securităţii cibernetice cu privire la riscurile şi incidentele cibernetice, Curtea consideră că aceasta *ar trebui să stabilească cu exactitate circumstanţele 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 şi 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 şi 22 din Legea nr.477/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Analizând, însă, dispoziţiile art.20 alin.(2), Curtea constată că *legiuitorul deleagă atribuţia sa de legiferare Ministerului pentru Societatea Informaţională, ANCOM sau autorităţilor desemnate, în condiţiile legii*, în domeniul securităţii cibernetice, care vor stabili „cerinţele minime de securitate cibernetică, modalitatea de notificare, precum şi datele şi informaţiile care însoţesc 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 autorităţilor sau instituţiilor publice respective*, publicate în Monitorul Oficial al României, Partea I". ***Trimiterea la acte administrative, cu o forţă juridică inferioară legii, într-un domeniu critic pentru securitatea naţională, cu impact asupra drepturilor şi libertăţilor fundamentale ale cetăţenilor, încalcă prevederile constituţionale cuprinse în art.1 alin.(5) referitoare la principiul legalităţii***. O dispoziţie 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 cerinţe minimale aplicabile tuturor destinatarilor săi. Or, atâta vreme cât ordinele sau deciziile sunt emise de conducătorii autorităţilor sau instituţiilor publice desemnate de lege, apare cu evidenţă că *legea relativizează în mod nepermis reglementarea acestui domeniu*, lăsând la latitudinea fiecărei entităţi stabilirea, în mod diferenţiat, a unor măsuri esenţiale, precum cerinţele minime de securitate cibernetică, modalitatea de notificare, precum şi datele şi informaţiile care însoţesc notificarea. Pe de altă parte, enumerând autorităţile care stabilesc aceste aspecte, legiuitorul omite chiar Consiliul Suprem de Apărare a Ţării, care

potrivit art.9 alin.(1) lit.f) din lege, aprobă propunerile COSC privind cerinţele minime de securitate cibernetică şi politici de securitate cibernetică pentru autorităţile şi instituţiile publice prevăzute la art.10 alin. (l) şi (2) din lege.

76. În concluzie, Curtea constată că **dispoziţiile art.20 alin.(1) lit.c) şi lit.h) coroborate cu art.20 alin.(2) sunt neconstituţionale, întrucât contravin prevederilor art.1 alin.(3) şi (5), art.26 şi art.28 din Constituţie**.

77. Din analiza legii, Curtea reţine că ***aceasta omite să reglementeze posibilitatea subiecţilor cărora le este destinată legea, în sarcina cărora au fost instituite obligaţii şi responsabilităţi, de a contesta în justiţie actele administrative*** încheiate cu privire la îndeplinirea acestor obligaţii şi care sunt susceptibile a prejudicia un drept sau un interes legitim.

78. Potrivit art.21 din Constituţie, orice persoană se poate adresa justiţiei pentru apărarea drepturilor, libertăţilor şi 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 Constituţională a statuat că liberul acces la justiţie presupune accesul la toate mijloacele procedurale prin care se înfăptuieşte actul de justiţie. S-a considerat că legiuitorul are competenţa exclusivă de a stabili regulile de desfăşurare a procesului în faţa instanţelor judecătoreşti, astfel cum rezultă din art. 126 alin. (2) din Constituţie. Totodată, în jurisprudenţa sa (Decizia nr.71 din 15 ianuarie 2009, publicată în Monitorul Oficial al României, Partea I, nr. 49 din 27 ianuarie 2009), Curtea a reţinut că liberul acces la justiţie este pe deplin respectat ori de câte ori partea interesată, în vederea valorificării unui drept sau interes legitim, a putut să se adreseze cel puţin o singură dată unei instanţe naţionale.

79. Pe de altă parte, potrivit art.6 paragraful 1 din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, orice persoană are dreptul la judecarea în mod echitabil a cauzei sale, de către o instanţă independentă şi imparţială, care va hotărî asupra încălcării drepturilor şi obligaţiilor sale cu caracter civil. Curtea Europeană a Drepturilor Omului a statuat în jurisprudenţa sa, cu titlu general, că art. 6 paragraful 1 din Convenţie

garantează oricărei persoane dreptul de a aduce în faţa unei instanţe orice pretenţie referitoare la drepturi şi obligaţii cu caracter civil (a se vedea Hotărârea din 21 februarie 1975, pronunţată în Cauza Golder împotriva Marii Britanii, paragraful 36, şi Hotărârea din 20 decembrie 2011, pronunţată în Cauza Dokic împotriva Serbiei, paragraful 35). De asemenea, în Hotărârea din 26 ianuarie 2006, pronunţată 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 justiţie implică prin natura sa o reglementare din partea statului şi poate fi supus unor limitări, atât timp cât nu este atinsă substanţa dreptului.

80. România este un stat de drept în care, potrivit art.1 alin.(5) din Constituţie, „respectarea Constituţiei, a supremaţiei sale şi a legilor este obligatorie”. În condiţiile în care art.20 alin.(1) din Constituţie prevede că dispoziţiile constituţionale privind drepturile şi libertăţile cetăţenilor vor fi interpretate şi aplicate în concordanţă cu Declaraţia Universală a Drepturilor Omului, cu pactele şi cu celelalte tratate la care România este parte, iar art.21 din Constituţie consacră liberul acces la justiţie, a cărei exercitare, potrivit alin.(2), nicio lege nu o poate îngrădi, Parlamentul are îndatorirea de a legifera norme corespunzătoare pentru asigurarea reală a respectării acestui drept, în lipsa căruia nu se poate concepe existenţa statului de drept, prevăzută prin art.1 alin.(3) din Constituţie. Fără îndeplinirea acestei îndatoriri, normele constituţionale menţionate ar avea un caracter pur declarativ, situaţie inadmisibilă pentru un stat care împărtăşeşte valorile democratice ce fac parte din ordinea publică europeană, aşa cum este prefigurat de Convenţia Europeană a Drepturilor Omului şi de Carta drepturilor fundamentale a Uniunii Europene (în acest sens, este şi Decizia Curţii Constituţionale 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 conţinutul legii prin care să se asigure**

posibilitatea persoanei ale cărei drepturi, libertăţi sau interese legitime au fost afectate prin acte sau fapte care au ca temei dispoziţiile Legii privind securitatea cibernetică a României de a se adresa unei instanţe judecătoreşti independente şi imparţiale contravine prevederilor art.1 alin.(3) şi (5), art.21, precum şi art.6 din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale.

82. Potrivit dispoziţiilor art.27 alin.(1), monitorizarea şi controlul aplicării prevederilor legii criticate se asigură, potrivit competenţelor stabilite prin lege, de către Camera Deputaţilor şi Senat, Administraţia Prezidenţială, Guvern, CSAT, precum şi instituţiile şi autorităţile publice prevăzute la art. 10 alin. (1) şi (2), pentru infrastructurile cibernetice proprii sau aflate în responsabilitate, Serviciul Român de Informaţii pentru infrastructurile cibernetice proprii sau aflate în responsabilitate, precum şi pentru deţinătorii de ICIN persoane juridice de drept public, Ministerul pentru Societatea Informaţională, respectiv ANCOM, după caz, pentru deţinătorii de ICIN, persoane juridice de drept privat.

83. ***Opţiunea legiuitorului de a atribui competenţe de monitorizare şi control al aplicării prevederilor legale Camerei Deputaţilor, Senatului, Administraţiei Prezidenţiale, Secretariatul General al Guvernului şi CSAT-ului***, în condiţiile în care art.10 alin.(1) şi (2) stabileşte autorităţile competente în domeniul securităţii cibernetice privind infrastructurile cibernetice proprii sau aflate în responsabilitate, fără a include în această categorie autorităţile enumerate mai sus, acestea regăsindu-se în întregul act normativ în categoria persoane juridice drept public, în sarcina cărora incumbă respectarea obligaţiilor prevăzute de lege, ***denotă inconsecvenţă şi generează confuzie cu privire la regimul juridic aplicabil acestor instituţii.*** Din interpretarea coroborată a dispoziţiilor art.20 alin.(1) cu cele ale art.21 alin.(1) lit.a), rezultă că, pe de o parte, Parlamentul, Administraţia Prezidenţială, Secretariatul General al Guvernului şi CSAT au obligaţia, de exemplu, de a permite efectuarea unor auditări de securitate cibernetică efectuate de SRI sau de a notifica CNSC cu

privire la riscurile şi incidentele cibernetice, pe de altă parte, *ele vor monitoriza şi controla respectarea acestor obligaţii, iar, în cazul neîndeplinirii dispoziţiilor legale, potrivit art.28 coroborat cu art30 lit.c) din lege, autorităţile îşi vor aplica lor însele sancţiuni, ca urmare a constatării contravenţiilor*. Curtea constată, aşadar, că legiuitorul eludează principiile de drept potrivit cărora controlul trebuie efectuat de o entitate independentă, exterioară autorităţii controlate, iar prin normele edictate face iluzorie respectarea obligaţiilor referitoare la securitatea cibernetică. Mai mult, dispoziţiile în temeiul cărora Parlamentul, Administraţia Prezidenţială, Secretariatul General al Guvernului şi CSAT devin agenţi constatatori ai săvârşirii de contravenţii şi dispun aplicarea de sancţiuni contravenţionale vădesc ignorarea principiilor de drept care guvernează un stat democratic, respectiv a **principiului separaţiei puterilor în stat, prevăzut de art.1 alin.(4) din Constituţie şi a principiului legalităţii, consacrat de art.1 alin.(5)**. Astfel, în virtutea legii criticate, autoritatea legiuitoare, administraţia prezidenţială, Guvernul sau CSAT, autorităţii de rang constituţional ale căror atribuţii sunt expres prevăzute în Legea fundamentală, *se subrogă în atribuţii care, potrivit Ordonanţei Guvernului nr.2/2001 privind regimul juridic al contravenţiilor (la care legea criticată face, de altfel, trimitere), revin în competenţa autorităţilor administraţiei publice centrale sau locale.*

84. Pe de altă parte, Curtea observă că ***legea supusă controlului nu stabileşte competenţe de control şi monitorizare faţă de toţi deţinătorii de infrastructuri cibernetice,*** *dispoziţiile art.27 alin.(1) stabilind aceste competenţe doar în ceea ce priveşte persoanele juridice de drept public sau privat, deţinătoare de ICIN.* Or, în condiţiile în care legea prevede, la art.15, 16 şi 17, obligaţii şi responsabilităţi pentru toate persoanele juridice de drept public sau privat deţinătoare de infrastructuri cibernetice, iar art.28 lit.a), b), c) califică drept contravenţii nerespectarea respectivelor obligaţii, *omisiunea legislativă cu privire la autoritatea competentă să efectueze controlul deţinătorilor de infrastructuri care nu sunt calificate ICIN* **viciază constituţionalitatea textului**

legal cuprins în art.27 alin.(1), din perspectiva art.1 alin.(5) din Constituţie. Normele edictate în materie contravenţională, atât în ceea ce priveşte fapta incriminată, cât şi procedura de constatare şi sancţionare a acesteia, trebuie să fie clare, precise, previzibile, astfel încât destinatarul lor să îşi poată conforma conduita prescripţiei legale.

85. De asemenea, Curtea reţine că dispoziţiile ***art.30*** din lege conţin prevederi referitoare la constatarea contravenţiilor şi aplicarea sancţiunilor. Curtea face o primă observaţie cu privire la ***confuzia generată de textul legal ca urmare a necorelării cu prevederile art.28*** care consacră contravenţiile săvârşite prin nerespectarea dispoziţiilor legale. Astfel, Curtea identifică: *omisiunea identificării autorităţii competente să constate şi să aplice sancţiunea pentru contravenţiile* prevăzute de art.28 lit.i) şi j) săvârşite de persoane juridice de drept privat; *omisiunea identificării autorităţii competente să constate şi să aplice sancţiunea pentru contravenţiile* prevăzute de art.28 lit.a), i) şi j) săvârşite de persoane juridice de drept public; *sancţionarea contravenţională reglementată de art.30 lit.c) pentru nerespectarea unor obligaţii* de către autorităţile şi instituţiile publice prevăzute la art.27 alin.(l) lit. a) din lege, cu privire la infrastructurile cibernetice proprii, obligaţii *de la care acestea erau exceptate*, potrivit art.20 alin.(1) teza a doua (contravenţii prevăzute de art.28 li.e)-h) din lege).

86. În jurisprudenţa sa, Curtea Constituţională a reţinut în repetate rânduri că orice act normativ trebuie să îndeplinească anumite condiţii calitative, printre acestea numărându-se previzibilitatea, ceea ce presupune că acesta *trebuie să fie suficient de precis şi clar pentru a putea fi aplicat* (a se vedea, spre exemplu, Decizia nr. 189 din 2 martie 2006, publicată în Monitorul Oficial al României, Partea I, nr. 307 din 5 aprilie 2006, Decizia nr. 903 din 6 iulie 2010, publicată în Monitorul Oficial al României, Partea I, nr. 584 din 17 august 2010 sau Decizia nr. 26 din 18 ianuarie 2012, publicată în Monitorul Oficial al României, Partea I, nr. 116 din 15 februarie 2012). În acelaşi sens, Curtea Europeană a Drepturilor Omului a statuat că legea trebuie, într-adevăr, să fie

accesibilă justiţiabilului şi previzibilă în ceea ce priveşte efectele sale. Pentru ca legea să satisfacă cerinţa de previzibilitate, ea trebuie să precizeze cu suficientă claritate întinderea şi modalităţile de exercitare a puterii de apreciere a autorităţilor în domeniul respectiv, ţinând cont de scopul legitim urmărit, pentru a oferi persoanei o protecţie adecvată împotriva arbitrariului. În plus, nu poate fi considerată "lege" decât *o normă enunţată cu suficientă precizie, pentru a permite cetăţeanului să îşi adapteze conduita în funcţie de aceasta*; apelând la nevoie la consiliere de specialitate în materie, el trebuie să fie capabil să prevadă, într-o măsură rezonabilă, faţă de circumstanţele speţei, consecinţele care ar putea rezulta dintr-o anumită faptă (a se vedea Hotărârea din 4 mai 2000, pronunţată în *Cauza Rotaru împotriva României*, paragraful 52, şi Hotărârea din 25 ianuarie 2007, pronunţată în *Cauza Sissanis împotriva României*, paragraful 66).

87. Aşa fiind, Curtea apreciază că imprecizia textelor de lege supuse controlului de constituţionalitate, constând în *lipsa stabilirii cu suficientă claritate a procedurilor de monitorizare şi control, respectiv a celor privind constatarea şi sancţionarea contravenţiilor*, afectează, pe cale de consecinţă, şi garanţiile constituţionale şi convenţionale care caracterizează dreptul la un proces echitabil, inclusiv componenta sa privind dreptul la apărare. De altfel, Curtea Europeană a Drepturilor Omului a reţinut, în esenţă, că nerespectarea garanţiilor fundamentale, care protejează presupuşii autori ai unor fapte ilicite, în faţa posibilelor abuzuri ale autorităţilor desemnate să-i urmărească şi să-i sancţioneze, reprezintă un aspect ce trebuie examinat în temeiul art. 6 din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale (a se vedea, spre exemplu, Hotărârea din 4 octombrie 2007, pronunţată în *Cauza Anghel împotriva României*, paragraful 68).

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

enunţate mai sus, Curtea reţine că, în mod evident, prevederile art.27 alin.(1) şi 30 din lege, caracterizate printr-o tehnică legislativă deficitară, **nu întrunesc exigenţele de claritate, precizie şi previzibilitate şi sunt astfel incompatibile cu principiul fundamental privind respectarea Constituţiei, a supremaţiei sale şi a legilor, prevăzut de art.1 alin. (5) din Constituţie şi cu dreptul la un proces echitabil, prevăzut de art.21 alin. (3) din Constituţie, precum şi de art.6 din Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale.**

89. Potrivit dispoziţiilor art.27 alin.(2) din lege, în cadrul activităţii de monitorizare şi control, persoanele desemnate de conducătorii autorităţilor prevăzute la art.27 alin.(1) ***au dreptul să solicite declaraţii sau orice documente necesare pentru efectuarea controlului, să facă inspecţii, inclusiv inopinate, la orice instalaţie, incintă sau infrastructură, destinate ICIN***, şi să primească, la cerere sau la faţa locului, informaţii sau justificări. Norma cuprinsă în art.27 alin.(2) lit.b) care permite autorităţilor publice prevăzute de art.10 alin.(1) şi (2) din lege să facă inspecţii la orice instalaţie, incintă sau infrastructură destinată ICIN, aflată în responsabilitatea lor, presupune accesul la o anumită locaţie, cu privire la anumite obiecte, sisteme informatice de stocare, prelucrare şi transmitere a datelor, inclusiv a celor cu caracter personal, acces care pune în discuţie protecţia drepturilor constituţionale la viaţă intimă, familială şi privată şi la secretul corespondenţei. Or, în măsura în care noţiunile cu care legea operează (instalaţii, incinte şi infrastructuri) nu sunt în mod predictibil determinate, iar sfera datelor asupra cărora se realizează controlul este incertă, Curtea apreciază că legea criticată nu reglementează garanţii care să permită o protecţie eficientă împotriva riscurilor de abuz, precum şi faţă de orice accesare şi utilizare ilicită a datelor cu caracter personal. În vreme ce noţiunea de infrastructură cibernetică e definită prin lege, noţiunea de *instalaţie* folosită în textul de art.27 alin.(2) lit.b) poate reprezenta tot un sistem informatic ori o reţea sau serviciu de comunicaţii electronice, având în vedere domeniul de reglementare al legii şi definiţiile cuprinse în aceasta, astfel că accesul la aceste

sisteme informatice nu poate fi permis decât cu autorizarea judecătorului. De asemenea, noţiunea de *incintă* poate semnifica şi locul unde se găsesc aceste sisteme informatice, caz în care Curtea reţine că sunt aplicabile dispoziţiile privind percheziţia 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. Faţă de cele prezentate, trimiterea la *„respectarea prevederilor legale în vigoare”* este una confuză, întrucât nu sunt identificate ca fiind prevederi aplicabile nici dispoziţiile Codului de procedură penală, indicate mai sus, şi nici prevederile altor acte normative.

91. Prin urmare, considerentele Deciziilor Curţii Constituţionale nr.440/2014 şi nr.461/2014 sunt valabile *mutatis mutandis*, astfel că argumentele expuse în prealabil cu privire la neconstituţionalitatea dispoziţiilor art.17 alin.(1) lit.a) din Legea privind securitatea cibernetică a României sunt pe deplin sustenabile şi în ceea ce priveşte **dispoziţiile art.27 alin.(2) din lege**. Aşa fiind, Curtea conchide că acestea **încalcă prevederile art.1 alin.(5), art.26, art.28, şi art.53 din Constituţie**.

92. Dincolo de aspectele punctuale a căror neconstituţionalitate a fost motivată *supra*, Curtea constată că întregul act normativ suferă de deficienţe sub aspectul respectării normelor de tehnică legislativă, a coerenţei, a clarităţii, a previzibilităţii, **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 esenţiale 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 dispoziţiile art.15 alin.(2), art.17 alin.(1) lit.b), art.19 alin.(1) şi (3), art.20 alin.(2), art.23 alin.(2), (5) şi (6), art.30 lit.d) din lege.

93. De asemenea, cu excepţia cazurilor în care trimiterea vizează chiar legea securităţii cibernetice, situaţie în care s-a folosit sintagma „prezenta lege”, *legea foloseşte în repetate rânduri sintagmele „potrivit legii”, „conform competenţelor prevăzute de lege” sau „în condiţiile legii”, fără a preciza*

concret la dispoziţiile căror legi se face trimiterea. Această situaţie se regăseşte în cuprinsul art.7 alin.(1) lit.d), art.10 alin.(2) şi (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 menţionează 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 şi a datei publicării acelui act** sau numai a categoriei juridice şi 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/instituţii/autorităţi înfiinţate 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 apariţia actului de reglementare primară prin care se stabileşte cadrul general de reglementare a domeniului securităţii 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 priveşte aspectele referitoare la criteriile de claritate, precizie, previzibilitate şi predictibilitate pe care un text de lege trebuie să le îndeplinească, Curtea constată că autoritatea legiuitoare, Parlamentul sau Guvernul, după caz, are obligaţia 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 şi inteligibil, fără dificultăţi sintactice şi pasaje obscure sau echivoce”*, iar potrivit art.36 alin.(1) din aceeaşi lege, *„actele normative trebuie redactate într-un limbaj şi stil juridic specific normativ, concis, sobru, clar şi precis, care să excludă orice echivoc, cu respectarea strictă a regulilor gramaticale şi de ortografie”*.

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 şi coordonarea legislaţiei, precum şi conţinutul şi forma juridică adecvate pentru fiecare act normativ. Astfel, respectarea acestor norme concură la asigurarea unei legislaţii care respectă principiul securităţii raporturilor juridice, având claritatea şi previzibilitatea necesară.

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

98. În acord cu jurisprudenţa sa, Curtea reţine că, în situaţia determinată de constatarea neconstituţionalităţii legii în ansamblul său, pronunţarea unei astfel de decizii are un efect definitiv cu privire la actul normativ, consecinţa fiind încetarea procesului legislativ în privinţa respectivei reglementări.

99. Pe de altă parte, în condiţiile în care prevederile art.61 alin.(1) din Constituţie stabilesc că „Parlamentul este organul reprezentativ suprem al poporului român şi unica autoritate legiuitoare a ţării”, competenţa de legiferare a acestuia cu privire la un anumit domeniu nu poate fi limitată dacă legea astfel adoptată respectă exigenţele Legii fundamentale. Prin urmare, opţiunea legiuitorului de a legifera în materia în care Curtea Constituţională a admis o sesizare de neconstituţionalitate cu privire la o lege în ansamblul său presupune parcurgerea tuturor fazelor procesului legislativ prevăzut de Constituţie şi de regulamentele celor două Camere ale Parlamentului (a se vedea în acest sens Decizia Curţii Constituţionale 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) şi al art. 147 alin. (4) din Constituţie, precum şi al art. 11 alin. (1) lit. A.a), al art. 15 alin. (1) şi al art. 18 alin. (2) din Legea nr. 47/1992, cu majoritate de voturi,

CURTEA CONSTITUŢIONALĂ

În numele legii

DECIDE:

Admite obiecţia de neconstituţionalitate şi constată că Legea privind securitatea cibernetică a României este neconstituţională, în ansamblul ei.

Definitivă şi general obligatorie.

Decizia se comunică Preşedintelui României, preşedinţilor celor două Camere ale Parlamentului şi prim-ministrului şi se publică în Monitorul Oficial al României, Partea I.

Pronunţată în şedinţa din data de 21 ianuarie 2015.