DECIZIA nr.455
din 4 iulie 2018

referitoare la obiecţia de neconstituţionalitate a dispoziţiilor Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice

Valer Dorneanu	**- preşedinte**
Marian Enache	**- judecător**
Petre Lăzăroiu	**- judecător**
Mircea Ştefan Minea	**- judecător**
Daniel Marius Morar	**- judecător**
Mona-Maria Pivniceru	**- judecător**
Livia Doina Stanciu	**- judecător**
Simona-Maya Teodoroiu	**- judecător**
Afrodita Laura Tutunaru	**- magistrat-asistent**

1. Pe rol se află soluţionarea obiecţiei de neconstituţionalitate a dispoziţiilor Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, obiecție formulată de Președintele României.

2. Obiecţia de neconstituţionalitate a fost înregistrată la Curtea Constituţională cu nr.4494 din 11 iunie 2018 şi constituie obiectul Dosarului nr.888A/2018.

3. **În motivarea obiecţiei de neconstituţionalitate,** Președintele României susține că legea criticată contravine dispoziţiilor constituţionale cuprinse în art. 1 alin. (5), în componenta sa privind principiul legalităţii şi principiul securităţii raporturilor juridice şi art. 119 referitor la Consiliul Suprem de Apărare a Ţării.

4. În acest sens, se arată că, legea supusă controlului de constituționalitate transpune Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune. Astfel, actul normativ stabilește cadrul juridic și

instituțional, măsurile și mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu.

5. Art.2 alin.(2) din legea criticată prevede că dispozițiile sale nu se aplică instituțiilor din domeniul apărării, ordinii publice și securității naționale și nici Oficiului Registrului Național al Informațiilor Secrete de Stat. Cu toate acestea, modul în care sunt definite conceptele de: securitate a rețelelor și a sistemelor informatice; strategie națională privind securitatea rețelelor și a sistemelor informatice; operator de servicii esențiale și furnizor de servicii digitale, coroborat cu prevederile Anexei, în care sunt prezentate sectoarele de activitate vizate de lege, duc la concluzia că legea reglementează securitatea componentelor de tehnologia informației și comunicații, aferente unor infrastructuri critice naționale sau europene, așa cum sunt definite la art.3 al Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice. Potrivit acestui text, infrastructura critică națională reprezintă *„un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții.”*

6. Prin urmare, actul normativ supus controlului de constituționalitate are implicații asupra infrastructurilor critice, care, potrivit Strategiei Naționale de Apărare a Țării, fac parte din obiectivele naționale de securitate, legea având astfel implicații directe asupra sistemului de apărare a țării și securității naționale.

7. Or, potrivit art.4 lit. d) pct. 1 din Legea nr. 415/2002 privind organizarea și funcționarea Consiliului Suprem de Apărare a Țării, această autoritate administrativă avizează proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională. Corelativ, art.9 alin.(1) din Legea nr. 24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative dispune că *„În cazurile prevăzute de*

lege, în faza de elaborare a proiectelor de acte normative, inițiatorul trebuie să solicite avizul autorităților interesate în aplicarea acestora, în funcție de obiectul reglementării”.

8. Mai mult, aceste dispoziții legale își găsesc suportul constituțional în prevederile art.119 din Constituție, potrivit căruia *„Consiliul Suprem de Apărare a Țării organizează și coordonează unitar activitățile care privesc apărarea țării și securitatea națională [...]”.*

9. De altfel, în jurisprudența sa, într-o situație similară, cu referire la o lege care privea tot aspecte legate de securitatea cibernetică, Curtea Constituțională a invalidat actul normativ în ansamblu cu argumentul că una din etapele obligatorii ale procedurii legislative, anume obținerea avizului Consiliului Suprem de Apărare a Țării (C.S.A.T.), nu a fost respectată.

10. Astfel, în Decizia nr.17 din 21 ianuarie 2015, Curtea Constituțională a arătat: *„întrucât în cadrul procedurii legislative, inițiatorul nu a respectat obligația legală, conform căreia Consiliul Suprem de Apărare a Țării avizează proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională, Curtea constată că actul normativ a fost adoptat cu încălcarea prevederilor constituționale ale art.1 alin. (5) care consacră principiul legalității și ale art. 119 referitoare la atribuțiile Consiliului Suprem de Apărare a Țării.*”

11. Având în vedere aceste aspecte, precum și faptul că legea criticată a fost elaborată cu încălcarea prevederilor legale antereferite, fără obținerea avizului Consiliului Suprem de Apărare a Țării, se consideră că Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice contravine prevederilor art. 1 alin. (5) din Constituție, potrivit cărora, *„În România, respectarea Constituției, a supremației sale și a legilor este obligatorie*”, coroborat cu art. 119 din Constituție.

12. 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 şi Guvernului, pentru a comunica punctele lor de vedere.

13. **Preşedintele Camerei Deputaţilor** apreciază că sesizarea de neconstituționalitate este neîntemeiată. Astfel, se arată că obiectul de reglementare al legii deduse controlului de constituționalitate este stabilirea cadrului juridic şi instituţional și măsurile şi mecanismele necesare asigurării unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice şi a stimulării cooperării în domeniu. Scopurile avute în vedere prin promovarea actului normativ criticat sunt instituirea cadrului de cooperare la nivel naţional şi de participare la nivel european şi internaţional în domeniul asigurării securităţii reţelelor şi sistemelor informatice, desemnarea autorităţii competente la nivel naţional şi a entităţilor de drept public şi privat care deţin competenţe şi responsabilităţi în aplicarea prevederilor legii, a punctului unic de contact la nivel naţional şi a echipei naţionale de intervenţie în caz de incidente de securitate informatică, precum şi stabilirea cerinţelor de securitate şi notificare pentru operatorii de servicii esenţiale şi pentru furnizorii de servicii digitale şi instituirea mecanismelor de actualizare a acestora în funcţie de evoluţia ameninţărilor la adresa securităţii reţelelor şi sistemelor informatice, prin transpunerea în legislația națională a Directivei (UE) 2016/1148 a Parlamentului European şi a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune.

14. Coordonarea strategică, la nivel naţional a activităţilor prevăzute de lege se realizează de către Guvern, prin Ministerul Comunicaţiilor şi Societăţii Informaţionale, sub aspectul politicilor publice şi al iniţiativei legislative în domeniu, iar strategia naţională privind securitatea reţelelor şi a sistemelor informatice se aprobă prin hotărâre a Guvernului.

15. Totodată, se apreciază ca fiind relevante aspecte referitoare la obiectul și domeniul de aplicare al directivei transpuse prin legea care face obiectul sesizării, care la art. 1 alin. (6) prevede că „*prezenta directivă nu aduce atingere acțiunilor*

întreprinse de statele membre pentru salvgardarea funcţiilor lor esenţiale de stat, în special pentru salvgardarea securităţii naţionale, inclusiv acţiuni de protejare a informaţiilor a căror divulgare este considerată de statele membre contrară intereselor esenţiale ale securităţii lor”.

16. Ca orice act normativ care are rolul reglementării unui anumit domeniu de activitate, legea criticată trebuie să respecte cerinţele privind claritatea, precizia şi previzibilitatea normelor juridice, atribute care să asigure sistematizarea, unificarea şi coordonarea legislaţiei. De aceea, legea dedusă controlului de constituţionalitate, în ansamblul său, răspunde acestor cerinţe. Este clară, întrucât în conţinutul său nu se regăsesc pasaje obscure sau soluţii normative contradictorii, este precisă, fiind redactată într-un stil specific normativ dispozitiv, care prezintă norma instituită fără explicaţii sau justificări, prin folosirea cuvintelor în înţelesul lor curent din limba română. Conceptele şi noţiunile utilizate sunt configurate în concordanţă cu dreptul pozitiv, iar stabilirea soluţiilor normative este departe de a fi ambiguă, acestea fiind redate previzibil şi univoc, cu respectarea prevederilor Legii nr. 24/2000.

17. Cu privire la soluțiile normative alese pentru configurarea conceptelor de securitate a rețelei și a sistemelor informatice, precum și definirea strategiei naționale în domeniu și stabilirea sectoarelor de activitate vizate, astfel instituite, Preşedintele Camerei Deputaților apreciază că acestea nu au trăsături ale infrastructurii naționale critice, în sensul dispozițiilor art. 3 din Ordonanța de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, cu modificările ulterioare, astfel cum autorul obiecţiei de neconstituționalitate susține. În sprijinul acestei afirmaţii se invocă prevederile art. 2 alin. (2) din legea criticată, potrivit cărora dispozițiile legii nu se aplică instituţiilor din domeniul apărării, ordinii publice şi securităţii naţionale, precum şi Oficiului Registrului Naţional al Informaţiilor Secrete de Stat.

18. Prin urmare, argumentele autorului obiecţiei de neconstituţionalitate care ar susține necesitatea solicitării avizului Consiliului Suprem de Apărare a Țării,

întrucât legea are „implicații directe asupra sistemului de apărare a țării și securității naționale” sunt fundamentate pe supoziții care nu surprind natura juridică a reglementării criticate.

19. Nu se poate reţine nici încălcarea jurisprudenţei Curţii Constituţionale invocate, respectiv a Deciziei nr.17 din 21 ianuarie 2015, întrucât, în cazul Legii privind securitatea cibernetică a României, la care se face referire, instanța de contencios constituțional a reținut necesitatea emiterii avizului Consiliului Suprem de Apărare a Țării ca urmare a dispozițiilor art. 3 alin. (1) din respectiva lege, prin care securitatea cibernetică se definea ca fiind o componentă a securității naționale a României, prevederi similare care să introducă mecanisme cu privire la apărarea țării și/sau siguranța națională neregăsindu-se în conținutul normativ al legii criticate.

20. Pe cale de consecință, întrucât actul normativ criticat nu conține prevederi ale căror aplicare ar determina afectarea infrastructurii critice care, potrivit Strategiei Naționale de Apărare a Țării, face parte din sistemul de apărare a țării, respectiv, dispoziții care să definească neechivoc apartenența la securitatea națională a relațiilor sociale edictate, se apreciază că în procedura de elaborare a proiectului de lege Guvernul nu a avut obligația de a solicita avizul Consiliului Suprem de Apărare a Țării.

21. Prin urmare, pentru argumentele expuse, se susţine că legea a fost adoptată cu respectarea prevederilor constituționale ale art. 1 alin. (5) care consacră principiul legalității și ale art. 119 referitoare la atribuțiile Consiliului Suprem de Apărare a Țării.

22. Totodată, din analiza coroborată a tuturor susținerilor autorului obiecţiei de neconstituţionalitate, se arată că acestea sunt în profund dezacord, atât cu rolul de unică autoritate legiuitoare a țării al Parlamentului și cu procedurile parlamentare aplicabile edictării legilor, cât și cu interdicția prevăzută la art. 69 din actul fundamental, care stabilește că orice mandat imperativ care ar putea fi stabilit în sarcina deputaților și al senatorilor este nul.

23. Având în vedere considerentele prezentate, se susţine că obiecţia de neconstituţionalitate formulată este neîntemeiată.

24. **Președintele Senatului și Guvernul** nu au transmis Curții Constituționale punctele lor de vedere.

CURTEA,

examinând obiecţia de neconstituţionalitate, punctul de vedere al președintelui Camerei Deputaţilor, raportul întocmit de judecătorul-raportor, dispoziţiile legii criticate, raportate la prevederile Constituţiei, precum şi Legea nr.47/1992, reţine următoarele:

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

15. **Obiectul controlului de constituţionalitate** îl constituie dispoziţiile Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice.

16. Textele constituţionale invocate în motivarea obiecţiei de neconstituţionalitate sunt art.1 alin.(5) privind principiul legalităţii şi principiul securităţii raporturilor juridice şi art.119 referitor la Consiliul Suprem de Apărare a Ţării.

17. **Analizând admisibilitatea obiecţiei de neconstituţionalitate,** sub aspectul **titularului dreptului de sesizare**, a **termenului** în care acesta este îndrituit să sesizeze instanţa constituţională, precum şi a **obiectului controlului de constituţionalitate**, Curtea constată că sesizarea care formează obiectul Dosarului nr.888A/2018 îndeplineşte condiţiile de admisibilitate prevăzute de art.146 lit.a) teza întâi din Constituţie. Astfel, în acord cu cele statuate în jurisprudenţa sa, Curtea constată că primele două condiţii se referă la regularitatea sesizării instanţei constituţionale, din perspectiva legalei sale sesizări, iar cea de-a treia vizează stabilirea

sferei sale de competenţă, astfel încât constatarea neîndeplinirii uneia dintre aceste condiţii are efecte dirimante, făcând inutilă analiza celorlalte condiţii [în acest sens, Decizia nr.66 din 21 februarie 2018, publicată în Monitorul Oficial al României, Partea I, nr.213 din 9 martie 2018, par.38, precum şi Decizia nr.334 din 10 mai 2018, par. 27, publicată în Monitorul Oficial al României, Partea I, nr.455 din 31 mai 2018].

18. În ceea ce priveşte ***titularul dreptului de sesizare,*** Curtea constată că este îndeplinită condiţia de admisibilitate, obiecţia de neconstituţionalitate fiind formulată de Preşedintele României, în temeiul art.146 lit.a) teza întâi din Constituţie.

19. Referitor la ***termenul în care a fost formulată*** prezenta obiecţie de neconstituţionalitate, **examinând procesul legislativ de adoptare a legii criticate,** Curtea constată că Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice a fost depusă la Secretarul general pentru exercitarea dreptului de sesizare asupra constituţionalităţii ei la data de 22 mai 2018, iar la data de 24 mai 2018 a fost trimisă Preşedintelui României pentru promulgare.

20. În interiorul termenului de promulgare de 20 de zile, prevăzut de art.77 alin. (1) din Constituţie, Preşedintele României a formulat la data de 11 iunie 2018 prezenta obiecţie de neconstituţionalitate, astfel că şi sub acest aspect sesizarea este admisibilă. Cu privire la modul de calcul al termenelor în interiorul cărora poate fi exercitat controlul *a priori*, Curtea Constituţională s-a pronunţat în jurisprudenţa sa şi a statuat prin Decizia nr.223 din 10 decembrie 1999, publicată în Monitorul Oficial al României, Partea I, nr. 638 din 28 decembrie 1999, că acestea „sunt termene care privesc desfăşurarea raporturilor constituţionale dintre autorităţile publice şi, prin urmare, în măsura în care nu se prevede altfel în mod expres, nu se calculează pe zile libere". Dispoziţiile art.181 alin.(1) pct.2 din Codul de procedură civilă, potrivit cărora „când termenul se socoteşte pe zile, nu intră în calcul ziua de la care începe să curgă termenul, nici ziua când acesta se împlineşte", nu sunt aplicabile în dreptul public, supus regulii în virtutea căreia termenele, în acest domeniu, se calculează pe zile calendaristice, în sensul că se includ în termen şi ziua în care el începe să curgă şi ziua

când se împlineşte (a se vedea şi Decizia nr.89 din 26 ianuarie 2010, publicată în Monitorul Oficial al României, Partea I, nr.115 din 19 februarie 2010).

21. **Examinând procesul legislativ de adoptare a legii criticate,** Curtea observă că proiectul Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice a fost, potrivit Hotărârii nr.E43 din 4 aprilie 2018, iniţiat de Guvern şi a fost supus spre adoptare Senatului, ca primă Cameră sesizată, cu procedura de urgenţă prevăzută de art.76 alin.(3) din Constituţie. Legea a fost adoptată de Senat, cu respectarea prevederilor art.76 alin.(2) din Constituţie, la data de 25 aprilie 2018 (rezultat vot: pentru=86, contra=0, abţineri=0). Ulterior a fost dezbătută şi adoptată de plenul Camerei Deputaţilor, la data de 16 mai 2018, (rezultat vot: pentru=253, contra=0, abţineri =1, nu au votat =1).

22. La data de 22 mai 2018, Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice a fost depusă la Secretarul general pentru exercitarea dreptului de sesizare asupra constituţionalităţii legii, iar la data de 24 mai 2018 a fost trimisă Preşedintelui României pentru promulgare.

23. **În ceea ce priveşte critica de neconstituţionalitate formulată,** Curtea constată că autorul sesizării a contestat Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, în ansamblul său, întrucât, în cadrul procedurii legislative, nu s-a solicitat avizul Consiliului Suprem de Apărare a Ţării.

24. Aşa fiind, înainte de a analiza lipsa avizului Consiliului Suprem de Apărare a Ţării în procedura de adoptare a legii – invocată de autorul sesizării – **Curtea va stabili dacă sfera de reglementare a Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice vizează securitatea naţională, fapt care ar impune obligativitatea obţinerii acestui aviz.** În acest sens, Curtea constată că Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice a fost emisă în aplicarea Directivei 2016/1148 (NIS, Network Internet Security) a Parlamentului European şi a Consiliului

Uniunii Europene din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a reţelelor şi a sistemelor informatice în Uniune, publicată în Jurnalul Oficial al Uniunii Europene nr.194L din 19 iulie 2016.

25. Directiva 2016/1148 este primul act legislativ al Uniunii privind securitatea reţelelor şi sistemelor informatice menit să transpună obiectivele Strategiei Europene de securitate cibernetică stabilite pentru pilonul NIS. Directiva a fost emisă în vederea protejării reţelelor, sistemelor şi serviciilor informatice care îndeplinesc un rol vital în societate, fiabilitatea şi securitatea lor fiind esenţiale pentru activităţile economice şi societale şi, în special, pentru funcţionarea pieţei interne. Totodată, s-a urmărit contracararea amplorii, frecvenţei şi impactului incidentelor de securitate care sunt în creştere şi reprezintă o ameninţare gravă pentru funcţionarea reţelelor şi a sistemelor informatice. Aceasta cu atât mai mult cu cât sistemele respective pot să devină, de asemenea, o ţintă pentru acţiunile dăunătoare deliberate menite să afecteze sau să întrerupă funcţionarea sistemelor. Având în vedere dimensiunea mondială a problemelor de securitate care afectează reţelele şi sistemele informatice, este nevoie de o cooperare internaţională mai strânsă pentru a îmbunătăţi standardele de securitate şi schimbul de informaţii şi pentru a promova o abordare internaţională comună a aspectelor de securitate. Responsabilitatea asigurării securităţii reţelelor şi a sistemelor informatice revine în mare măsură operatorilor de servicii esenţiale şi furnizorilor de servicii digitale. Ar trebui să se promoveze şi să se dezvolte prin cerinţe adecvate de reglementare şi practici voluntare sectoriale o cultură a gestionării riscurilor, care să implice evaluarea riscurilor şi aplicarea unor măsuri de securitate adecvate riscurilor întâmpinate. Stabilirea unor condiţii de concurenţă al căror caracter echitabil să prezinte încredere este şi ea esenţială pentru funcţionarea eficace a grupului de cooperare şi a reţelei Computer Security Incident Response Team (CSIRT), în scopul asigurării unei cooperări efective din partea tuturor statelor membre.

26. Având în vedere aceste aspecte de drept european, legiuitorul naţional a adoptat prezenta lege, al cărei obiect constă în stabilirea unui cadru juridic şi

instituţional, măsurile şi mecanismele necesare în vederea asigurării unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice şi a stimulării cooperării în domeniu.

27. În acord cu art.2 alin.(1) din lege, scopul său constă în **stabilirea cadrului de cooperare la nivel naţional şi de participare la nivel european şi internaţional** în **domeniul asigurării securităţii reţelelor şi sistemelor informatice**; desemnarea **autorităţii competente la nivel naţional şi a entităţilor de drept public** şi privat care deţin competenţe şi responsabilităţi în aplicarea prevederilor prezentei legi, a **Punctului unic de contact la nivel naţional şi a echipei naţionale de intervenţie în caz de incidente de securitate informatică**; precum şi în stabilirea cerinţelor de securitate şi notificare pentru operatorii de servicii esenţiale şi pentru furnizorii de servicii digitale şi instituirea mecanismelor de actualizare a acestora **în funcţie de evoluţia ameninţărilor la adresa securităţii reţelelor şi sistemelor informatice.**

28. În legislaţia naţională există deja în vigoare o serie de reglementări, acte normative cu caracter primar sau secundar, care au legătură cu domeniul securităţii naţionale. 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 cu modificări 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 Parlamentului European şi Consiliului Uniunii Europene 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 seria L nr. 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, iar potrivit anexei nr.1 lista sectoarelor infrastructurii critice naţionale vizează **energia**, tehnologia informaţiei şi comunicaţii, **alimentare cu apă,** alimentaţie, **sănătate**, **securitate naţională**, administraţie, **transporturi**, industria chimică şi nucleară şi spaţiu şi cercetare. Or, o parte dintre aceste sectoare critice se regăsesc şi în legea contestată în prezenta cauză respectiv, energie, alimentare cu apă, sănătate şi transporturi.

29. În aplicarea ordonanţei de urgenţă mai sus menţionate, a fost adoptată **Hotărârea Guvernului nr.718/2011** pentru aprobarea Strategiei naţionale privind protecţia infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I, nr. 555 din 4 august 2011.

30. De asemenea, Curtea reţine că prin **Hotărârea Guvernului nr.494/2011**, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, s-a reglementat înfiinţarea ca instituţie publică cu personalitate juridică, în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaţionale (MCSI), a **Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO (instituţie la care face trimitere şi Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice**), 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.

31. Un alt act normativ emis în domeniul securităţii naţionale îl constituie **Hotărârea Guvernului nr.271/2013** pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate cibernetică, publicată în Monitorul Oficial al României, Partea I, nr. 296 din 23 mai 2013.

32. **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 ce 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, potrivit acesteia, **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 al Informaţiilor 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**.

33. 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.

34. **Instanța de control constituțional** a dezvoltat cu privire la sintagma ***„securitate națională”*** o jurisprudență bogată, în acest sens fiind Decizia nr. 375 din 6 iulie 2005, publicată în Monitorul Oficial al României, Partea I, nr. 591 din 8 iulie 2005, Decizia nr.1.414 din 4 noiembrie 2009, publicată în Monitorul Oficial al României, Partea I, nr. 796 din 23 noiembrie 2009, Decizia nr. 872 din 25 iunie 2010, publicată în Monitorul Oficial al României, Partea I, nr. 433 din 28 iunie 2010, Decizia nr.80 din 16 februarie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 246 din 7 aprilie 2014, Decizia nr.17 din 21 ianuarie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 79 din 30 ianuarie 2015, și Decizia nr.91 din 28 februarie 2018, publicată în Monitorul Oficial al României, Partea I, nr.348 din 20 aprilie 2018.

35. Astfel, în Decizia nr.91 din 28 februarie 2018, precitată, paragrafele 42-53, Curtea a reținut, făcând referire la jurisprudența sa anterioară, că Legea fundamentală, adoptată în anul 1991, prevedea în art.49 (devenit art.53 după revizuire), *„apărarea siguranţei naţionale”* printre scopurile care pot sta la baza restrângerii exerciţiului unor drepturi sau al unor libertăţi. Ca urmare a revizuirii Constituţiei în anul 2003, conceptul de *„siguranţă naţională”* a fost înlocuit cu cel de *„securitate naţională”*. Totodată, Curtea a observat că, în Raportul asupra amendamentelor la Propunerea legislativă privind revizuirea Constituţiei întocmit de Comisia pentru elaborarea propunerii legislative privind revizuirea Constituţiei, referitor la înlocuirea sintagmei *„siguranţă naţională”* cu cea de *„securitate naţională”*, s-a precizat că „sintagma «securitate naţională» este utilizată atât în Uniunea Europeană, cât şi în

cadrul North Atlantic Treaty Organization (NATO) cu un conţinut ce asigură compatibilitatea ţării noastre cu standardele de apărare colectivă ale acestora, iar termenul «siguranţă naţională» era utilizat numai în perioada antebelică.

36. În acest context, Curtea a constatat că Legea nr.51/1991, publicată în Monitorul Oficial al României, Partea I, nr. 163 din 7 august 1991, reglementa, potrivit titlului său, siguranţa naţională a României. Ulterior, prin Legea nr.255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală şi pentru modificarea şi completarea unor acte normative care cuprind dispoziţii procesual penale, sintagma „siguranţă naţională" a fost înlocuită cu cea de „securitate naţională", atât în titlul, cât şi în cuprinsul Legii nr. 51/1991. De asemenea, Curtea a reţinut că, în acelaşi raport, anterior menţionat, referitor la introducerea în Legea fundamentală a unui nou articol cu denumirea marginală *„Securitatea naţională",* care conţinea definirea acestei noţiuni, Comisia pentru elaborarea propunerii legislative privind revizuirea Constituţiei a precizat că „noţiunea de «securitate naţională», **prin diversitatea, complexitatea şi dinamica ei**, este necesar a fi de domeniul legiuitorului ordinar, nu constituant, deoarece tocmai datorită acestei caracteristici, orice definiţie s-ar putea dovedi inadecvată".

37. Curtea a observat, totodată, că, în ceea ce priveşte Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale, securitatea naţională este menţionată în art.8 paragraful 2, art.10 şi art.11 ca un prim scop legitim care poate sta la baza restrângerii drepturilor şi libertăţilor prevăzute de aceste prevederi. Convenţia pentru apărarea drepturilor omului şi a libertăţilor fundamentale nu defineşte termenul de *„securitate naţională",* Comisia Europeană a Drepturilor Omului statuând că acesta nu poate fi definit în mod exhaustiv, bucurându-se de un nivel de elasticitate şi flexibilitate, care se reflectă în marja de apreciere a statului în această materie. Astfel, Comisia a reţinut că principiile accesibilităţii şi previzibilităţii nu necesită în mod necesar o definiţie exhaustivă a noţiunii de *„interese ale securităţii naţionale".* Multe legi, care prin obiectul lor de reglementare trebuie să prezinte un anumit grad de

flexibilitate, intră, în mod inevitabil, în categoria celor care folosesc termeni care sunt într-o măsură mai mare sau mai mică vagi şi a căror interpretare şi aplicare sunt chestiuni de practică (Decizia de inadmisibilitate din 2 aprilie 1993, pronunţată în *Cauza Esbester împotriva Regatului Unit*).

38. Curtea a reținut că termenul *„securitate naţională”* este unul plurivalent. Astfel, din punct de vedere al art.53 alin.(1) din Constituţie, se poate vorbi de ***securitate*** *militară, economică, financiară,* ***informatică, socială a ţării***. Oricare dintre aceste tipuri de securitate poate fi ţinta unei ameninţări interne sau externe, motiv pentru care legiuitorul ar putea recurge la restrângerea exerciţiului unor drepturi sau libertăţi constituţionale. De asemenea, s-a precizat că termenul de „siguranţă naţională” vizează protecţia statului, mai ales în ceea ce priveşte integritatea teritorială şi independenţa naţională şi că siguranţa sau securitatea socială **vizează protecţia societăţii**. Totodată, Curtea a reamintit jurisprudența sa referitoare la noţiunea de *„securitate naţională”,* potrivit căreia, această noțiune nu implică numai securitatea militară, deci domeniul militar, ci **are şi o componentă socială şi economică**. Astfel, nu numai existenţa unei situaţii *manu militari* atrage aplicabilitatea noţiunii de *„securitate naţională”* din textul art. 53 din Legea fundamentală, ci şi alte aspecte din viaţa statului - precum cele economice, financiare, sociale - care ar putea afecta însăşi fiinţa statului prin amploarea şi gravitatea fenomenului.

39. Aşa fiind, Curtea a constatat că, deşi sintagma în discuţie a fost, în mod tradiţional, asociată cu apărarea militară a statului, **sfera de cuprindere a acesteia transcende strategiilor exclusiv militare, înglobând elemente şi mijloace nonmilitare, primelor adăugându-li-se componente de natură economică, financiară, tehnologică** etc.

40. Din această perspectivă, instanța de control constituțional a constatat, în Decizia nr.91 din 28 februarie 2018, precitată, că noţiunea de *„securitate naţională”* este folosită ca o continuare şi dezvoltare a celei de *„siguranţă naţională”*. Astfel, potrivit art.1 din Legea nr.51/1991, *„Prin securitatea naţională a României se înţelege*

starea de legalitate, de echilibru şi de stabilitate socială, economică şi politică necesară existenţei şi dezvoltării statului naţional român ca stat suveran, unitar, independent şi indivizibil, menţinerii ordinii de drept, precum şi a climatului de exercitare neîngrădită a drepturilor, libertăţilor şi îndatoririlor fundamentale ale cetăţenilor, potrivit principiilor şi normelor democratice statornicite prin Constituţie". Potrivit art.2 alin.(1) din Legea nr.51/1991, realizarea securităţii naţionale se înfăptuieşte prin cunoaşterea, prevenirea şi înlăturarea ameninţărilor interne sau externe ce pot aduce atingere valorilor prevăzute în art.1 din acelaşi act normativ. Astfel, Curtea a constatat că realizarea securităţii naţionale nu reprezintă o proiecţie viitoare, ci este un proces continuu care menţine starea de securitate naţională existentă. În acest sens, Curtea a statuat că, spre deosebire de „apărarea ţării", care presupune posibilitatea unei intervenţii active, dinamice în cazul unor atacuri sau al unor acţiuni ostile din exterior, ***„securitatea naţională"*** **implică activităţi destinate menţinerii unei stări preexistente de linişte şi de siguranţă internă** (Decizia nr. 80 din 16 februarie 2014, paragraful 343).

41. Distinct de considerentele jurisprudențiale precitate, cu referire la noțiunea de *„securitate națională"*, Curtea reține și Hotărârea din 24 iunie 2015, pronunţată în Cauza C-373/13 din 24 iunie 2015, prin care Curtea de Justiție a Uniunii Europene a interpretat noțiunea *„motive imperioase de siguranţă naţională sau de ordine publică"*, în sensul art.24 alin.(1) din Directiva 2004/83/CE a Consiliului Uniunii Europene din 29 aprilie 2004 privind standardele minime referitoare la condițiile pe care trebuie să le îndeplinească resortisanții țărilor terțe sau apatrizii pentru a putea beneficia de statutul de refugiat sau persoanele care, din alte motive, au nevoie de protecție internațională și referitoare la conținutul protecției acordate. În speță, Curtea a reținut că noțiunea *„siguranță publică" acoperă atât securitatea internă a unui stat membru, cât și securitatea sa externă* și că, prin urmare, *atingerea adusă funcționării instituțiilor și a* ***serviciilor publice esențiale****, precum și supraviețuirea populației, ca și riscul unei perturbări grave a relațiilor externe sau a*

convieţuirii în pace a popoarelor ori atingerea adusă intereselor militare pot afecta siguranţa publică. În plus, Curtea a decis că noţiunea *„motive imperative de siguranţă publică”* presupune nu numai existenţa unei atingeri aduse siguranţei publice, ci şi ca *o asemenea atingere să prezinte un nivel de gravitate deosebit de ridicat,* exprimat prin utilizarea sintagmei „motive imperative”. Noţiunea *„ordine publică”* a fost interpretată în jurisprudenţa Curţii în sensul că recurgerea la aceasta presupune întotdeauna, pe lângă tulburarea ordinii sociale pe care o reprezintă orice încălcare a legii, existenţa unei ameninţări reale, actuale şi suficient de grave la adresa unui interes fundamental al societăţii. *Curtea a stabilit, totodată, că statele membre rămân libere să stabilească, în conformitate cu nevoile lor naţionale, care pot varia de la un stat membru la altul şi de la o perioadă la alta, cerinţele de ordine publică şi de siguranţă naţională.*

42. Chiar dacă legea contestată nu mai defineşte securitatea cibernetică ca fiind o componentă a securităţii naţionale a României, Curtea va analiza dacă, din interpretarea sistematică a normelor instituite prin legea criticată, acestea au sau nu incidenţă/legătură asupra/cu securităţii/securitatea naţionale/naţională.

43. Atât prin Directiva 2016/1148, cât şi prin prezenta lege, în cazul sistemelor informatice care asigură furnizarea serviciilor esenţiale sunt avute în vedere urmările ce vizează, în mod direct, incidente de securitate. Acestea sunt evenimente care au un impact real negativ asupra sistemelor informatice şi care pot viza, inclusiv acţiuni de spionaj cibernetic, cu scopul de a obţine neautorizat informaţii confidenţiale, în interesul unei entităţi statale sau nonstatale ori referitoare la criminalitatea informatică, concretizată în fapte prevăzute de legea penală sau de alte legi speciale, fapte care prezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul ori asupra infrastructurilor cibernetice (a se vedea în acest sens art.181 din Codul penal referitor la definirea expresiilor „*Sistem informatic*” şi „*Date informatice*”, art.360 din Codul penal referitor la *Accesul ilegal la un sistem informatic* şi art.361 din Codul penal referitor la *Interceptarea ilegală a unei transmisii de date informatice*). Un astfel

de fenomen nu poate fi îngăduit, căci tolerarea sa ar însemna încurajarea şi extinderea lui, ceea ce ar duce la urmări sociale foarte grave, cu atât mai mult cu cât dezvoltarea rapidă a tehnologiilor moderne de informaţii şi comunicaţii - condiţie *sine qua non* a edificării societăţii informaţionale - a avut un impact major asupra ansamblului social, marcând adevărate mutaţii în filozofia de funcţionare a economicului, politicului şi culturalului, dar şi asupra vieţii de zi cu zi a individului.

44. Practic, dispoziţiile Directivei 2016/1148 (NIS, Network Internet Security) creează structurile necesare pentru cooperarea strategică şi operaţională între statele membre şi vizează creşterea nivelului de rezilienţă al reţelelor şi al sistemelor informatice de pe teritoriul Uniunii Europene. Mai mult decât atât, aceasta impune o abordare globală la nivelul Uniunii, care să includă cerinţele comune privitoare la crearea capacităţilor minime şi a planificării, a schimbului de informaţii, a cooperării şi măsurilor comune de securitate pentru operatorii de servicii esenţiale şi a furnizorilor de servicii digitale, fără a-i împiedica pe aceştia să adopte măsuri de securitate mai stricte decât cele prevăzute de directivă.

45. Totodată, directiva prevede reguli de aplicabilitate raportate la reglementările cuprinse în alte norme europene privind securitatea reţelelor şi sistemelor, precum şi în cele de cooperare cu autorităţi din alte domenii, cum ar fi asigurarea ordinii publice, protecţia datelor cu caracter personal.

46. Aşa cum se arată în Expunerea de motive a Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice, transpunerea prevederilor Directivei (UE) 2016/1148 (NIS, Network Internet Security), reprezintă un demers ce vizează şi respectă atât principiile responsabilităţii, cooperării şi coordonării, cât şi regulile generale aplicabile securităţii reţelelor şi sistemelor informatice ce susţin servicii esenţiale din domenii cheie la nivel social, având drept scop inclusiv transpunerea obiectivelor Strategiei Europene de securitate cibernetică stabilite pentru pilonul NIS.

47. Deşi în art.2 alin.(2) din actul normativ contestat se menţionează că prezenta lege nu se aplică instituţiilor din domeniul apărării, ordinii publice şi securităţii naţionale, precum şi Oficiului Registrului Naţional al Informaţiilor Secrete de Stat, cu toate acestea, Curtea constată că modul în care sunt definite conceptele de: *operator de servicii esenţiale, securitatea reţelelor şi a sistemelor informatice*, *strategie naţională privind securitatea reţelelor şi a sistemelor informatice* şi *furnizor de servicii digitale*, coroborat cu prevederile Anexei I, în care sunt prezentate sectoarele de activitate vizate de lege, duc la concluzia că legea reglementează securitatea componentelor de tehnologia informației și comunicații, aferente unor infrastructuri critice naționale sau europene, așa cum sunt definite la art.3 al Ordonanței de urgență a Guvernului nr.98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice.

48. Astfel, **în art.3 din legea contestată** au fost definiți termenii mai sus menționați, între care se reţin:

- „*operator de servicii esenţiale*” ca fiind o persoană fizică sau *juridică de drept public* sau privat de tipul celor prevăzute în anexă şi care furnizează un serviciu care îndeplineşte condiţiile prevăzute la art.6 alin.(1);

- „*securitatea reţelelor şi a sistemelor informatice*” ca fiind capacitatea unei reţele şi a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acţiuni care compromite disponibilitatea, autenticitatea, integritatea, confidenţialitatea sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de reţeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

- „*strategie naţională privind securitatea reţelelor şi a sistemelor informatice*” ca fiind cadrul care furnizează obiective şi priorităţi strategice privind securitatea reţelelor şi sistemelor informatice la nivel naţional.

49. Totodată, potrivit **art.6 alin.(1) lit.a) şi art.14 din lege** „*Un serviciu este considerat esenţial dacă furnizarea lui îndeplineşte cumulativ următoarele condiţii: a)*

serviciul este esenţial în susţinerea unor activităţi societale şi/sau economice de cea mai mare importanţă*; b) furnizarea sa depinde de o reţea sau de un sistem informatic; c) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident*" iar *„Strategia naţională privind securitatea reţelelor şi a sistemelor informatice se aprobă prin hotărâre a Guvernului, la propunerea MCSI în termen de 6 luni de la data intrării în vigoare a prezentei legi*".

50. Pentru asigurarea unui nivel ridicat de securitate a reţelelor şi sistemelor informatice, Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) se consultă şi cooperează, între altele, atât cu Serviciul Român de Informaţii, **pentru securitatea reţelelor şi a sistemelor informatice care asigură servicii esenţiale a căror afectare aduce atingere securităţii naţionale**, cât şi cu 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, pentru securitatea reţelelor şi a sistemelor informatice care asigură servicii esenţiale **în domeniul lor de activitate şi responsabilitate** [a se vedea art.15 alin.(2) lit.a) şi c) din lege].

51. Totodată, CERT-RO în calitate de autoritate competentă la nivel naţional „elaborează şi actualizează, **după consultarea celorlalte instituţii cu responsabilităţi în domeniul apărării, ordinii publice şi securităţii naţionale**, precum şi a altor instituţii şi autorităţi, după caz, normele metodologice, tehnice, precum şi regulamentele privind cerinţele referitoare la înfiinţarea, autorizarea şi funcţionarea echipelor Computer Security Incident Response Team (CSIRT), desemnarea echipelor CSIRT sectoriale" [a se vedea art.20 lit.e) din lege].

52. Curtea constată că ritmul actual al realităților obiective este în continuă schimbare, iar relaţiile sociale referitoare la securitatea reţelelor şi sistemelor informatice vizează un interes general a cărui amploare **impune calificarea acestui domeniu ca fiind în strânsă interdependenţă cu securitatea naţională**. Această teză este susţinută de împrejurarea că, Legea privind asigurarea unui nivel comun ridicat de

securitate a reţelelor şi sistemelor informatice **reglementează cu privire la servicii publice esenţiale (energie, alimentare cu apă, sănătate şi transporturi), care prin natura lor pot afecta securitatea naţională**.

53. Autorul sesizării a criticat Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice întrucât, **în dezacord cu exigenţele art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării,** publicată în Monitorul Oficial al României, Partea I, nr.494 din 10 iulie 2002, **nu s-a solicitat avizul acestei** din urmă instituţii.

54. Astfel, criticile vizând lipsa solicitării sau existenţei unor avize în procedura de elaborare a actelor normative au fost calificate de Curte ca aspecte ce ţin de respectarea obligaţiilor legale ale autorităţilor implicate în această procedură şi, implicit, ca vizând o neconstituţionalitate a actelor normative, care poate fi analizată doar în condiţiile art.**146 lit. a)** şi d) din Constituţie (a se vedea Decizia nr.63 din 8 februarie 2017, publicată în Monitorul Oficial al României, Partea I, nr.145 din 27 februarie 2017, par.108).

55. Potrivit art.119 din Constituţie, Consiliul Suprem de Apărare a Ţării *„organizează şi coordonează unitar activităţile care privesc apărarea ţării şi **securitatea naţională** [...]”*. În realizarea acestui rol, potrivit art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării, *„avizează proiectele de acte normative iniţiate sau emise de Guvern privind: **securitatea naţională** [...]*”, competenţă ce îşi are izvorul în textul constituţional.

56. Deşi norma constituţională, exprimând rolul Consiliului Suprem de Apărare a Ţării de coordonare unitară a activităţilor care privesc securitatea naţională, nu face niciun fel de referire expresă la obligaţia iniţiatorilor proiectelor de acte normative de a solicita avizul acestei autorităţi, avizarea proiectelor de acte normative ce privesc securitatea naţională este tratată în Legea nr.415/2002, mai sus menţionată, şi care reprezintă o reflectare a normei constituţionale consacrate de art.119 din Legea

fundamentală. De aceea, indiferent că este vorba de o competenţă acordată prin lege sau direct prin textul Constituţiei, autorităţile sunt obligate să o aplice şi să o respecte în virtutea art.1 alin.(5) din Constituţie, potrivit căruia „*În România, respectarea Constituţiei, a supremaţiei sale şi a legilor este obligatorie*". O atare concluzie se impune datorită faptului că principiul legalităţii este unul de rang constituţional (a se vedea Decizia Curţii Constituţionale nr.901 din 17 iunie 2009, publicată în Monitorul Oficial al României, Partea I, nr. 503 din 21 iulie 2009).

57. În jurisprudenţa sa, Curtea Constituţională a statuat că lipsa avizului autorităţilor publice implicate nu conduce în mod automat la neconstituţionalitatea legii asupra căreia acesta nu a fost dat, întrucât ceea ce prevalează constă în obligaţia Guvernului de a-l solicita. Împrejurarea că autoritatea care trebuie să emită un astfel de aviz, deşi i s-a solicitat, nu şi-a îndeplinit această atribuţie „*constituie o înţelegere greşită a rolului său legal şi constituţional, fără a fi însă afectată constituţionalitatea legii asupra căreia nu a fost dat avizul*" (a se vedea Decizia nr.383 din 23 martie 2011, publicată în Monitorul Oficial al României, Partea I, nr.281 din 21 aprilie 2011, par.I.3, Decizia nr.574 din 4 mai 2011, par.I.2. şi Decizia nr.575 din 4 mai 2011, par.IV.A.2., publicate în Monitorul Oficial al României, Partea I, nr.368 din 26 mai 2011).

58. **În cauza de faţă Curtea constată că, dimpotrivă, avizul Consiliului Suprem de Apărare a Ţării nu a fost solicitat**.

59. Aşa fiind, potrivit art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea şi funcţionarea Consiliului Suprem de Apărare a Ţării, acesta „avizează proiectele de acte normative iniţiate sau emise de Guvern privind securitatea naţională", iar potrivit art.9 - *Avizarea proiectelor* din Legea nr.24/2000 privind normele de tehnică legislativă pentru elaborarea actelor normative, republicată în Monitorul Oficial al României, Partea I, nr. 260 din 21 aprilie 2010, *„(1) 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 acestor dispoziţii legale, Guvernul avea obligaţia de a solicita avizul Consiliului Suprem de Apărare a Ţării atunci când a elaborat proiectul Legii privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice.

60. 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 (a se vedea şi Decizia nr.17 din 21 ianuarie 2015, publicată în Monitorul Oficial al României, Partea I, nr.79 din 30 ianuarie 2015, par.42).

61. 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 unanimitate de voturi,

CURTEA CONSTITUŢIONALĂ

În numele legii

DECIDE:

Admite obiecţia de neconstituţionalitate formulată şi constată că Legea privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice este neconstituţională, în ansamblul său.

Definitivă şi general obligatorie.

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

Pronunţată în şedinţa din data de 4 iulie 2018.