



R O M Â N I A
CURTEA CONSTITUȚIONALĂ
CABINETUL PREȘEDINTELUI

Palatul Parlamentului

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

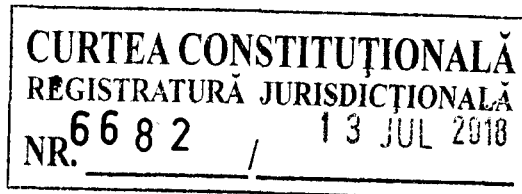
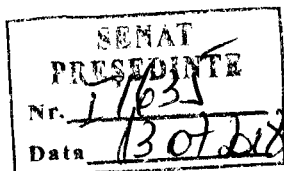
Telefon: (+40-21) 313 25 31

Fax: (+40-21) 312 54 80

Internet : <http://www.ccr.ro>

E-mail: pres@ccr.ro

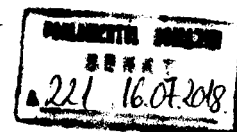
Dosar nr.888A/2018



DOMNULUI

CĂLIN CONSTANTIN ANTON POPESCU-TĂRICEANU

Președintele Senatului



22.7.2018
În conformitate cu dispozițiile art.18 alin.(2) din Legea nr.47/1992 privind organizarea și funcționarea Curții Constituționale, vă comunicăm alăturat Decizia nr.455 din 4 iulie 2018, prin care Curtea Constituțională, cu unanimitate de voturi, a admis obiecția de neconstituționalitate și a constatat că Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice este neconstituțională, în ansamblul său.

Vă asigurăm de deplina noastră considerație.

PREȘEDINTE,

Prof.univ.dr. Valer Dorneanu

ROMÂNIA
CURTEA CONSTITUȚIONALĂ

Dosar nr.888A/2018

DECIZIA nr.455
din 4 iulie 2018

referitoare la obiecția de neconstituționalitate a dispozițiilor Legii privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice

Valer Dorneanu	- președinte
Marian Enache	- judecător
Petre Lăzăroiu	- judecător
Mircea Ștefan 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 soluționarea obiecției de neconstituționalitate a dispozițiilor Legii privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, obiecție formulată de Președintele României.

2. Obiecția de neconstituționalitate a fost înregistrată la Curtea Constituțională cu nr.4494 din 11 iunie 2018 și constituie obiectul Dosarului nr.888A/2018.

3. **În motivarea obiecției de neconstituționalitate**, Președintele României susține că legea criticată contravine dispozițiilor constituționale cuprinse în art. 1 alin.

(5), în componenta sa privind principiul legalității și principiul securității raporturilor juridice și art. 119 referitor la Consiliul Suprem de Apărare a Țării.

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 căroră, *„În România, respectarea Constituției, a supremației sale și a legilor este obligatorie”*, coroborat cu art. 119 din Constituție.

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

13. **Președintele Camerei Deputaților** apreciază că sesizarea de neconstituționalitate este neîntemeiată. Astfel, se arată că obiectul de reglementare al legii deduse controlului de constituționalitate este stabilirea cadrului juridic și instituțional și măsurile și mecanismele necesare asigurării unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice și a stimulării cooperării în domeniu. Scopurile avute în vedere prin promovarea actului normativ criticat sunt instituirea cadrului de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice, desemnarea autorității competente la nivel național și a entităților de drept public și privat care dețin competențe și responsabilități în aplicarea prevederilor legii, a punctului unic de contact la nivel național și a echipei naționale de intervenție în caz de incidente de securitate informatică, precum și stabilirea cerințelor de securitate și notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale și instituirea mecanismelor de actualizare a acestora în funcție de evoluția amenințărilor la adresa securității rețelelor și sistemelor informatice, prin transpunerea în legislația națională a Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

14. Coordonarea strategică, la nivel național a activităților prevăzute de lege se realizează de către Guvern, prin Ministerul Comunicațiilor și Societății Informaționale, sub aspectul politicilor publice și al inițiativei legislative în domeniu, iar strategia națională privind securitatea rețelilor și 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 salvagardarea funcțiilor lor esențiale de stat, în special pentru salvagardarea securității naționale, inclusiv acțiuni de protejare a informațiilor a căror divulgare este considerată de statele membre contrară intereselor esențiale ale securității lor”*.

16. Ca orice act normativ care are rolul reglementării unui anumit domeniu de activitate, legea criticată trebuie să respecte cerințele privind claritatea, precizia și previzibilitatea normelor juridice, atribute care să asigure sistematizarea, unificarea și coordonarea legislației. De aceea, legea dedusă controlului de constituționalitate, în ansamblul său, răspunde acestor cerințe. Este clară, întrucât în conținutul său nu se regăsesc pasaje obscure sau soluții normative contradictorii, este precisă, fiind redactată într-un stil specific normativ dispozitiv, care prezintă norma instituită fără explicații sau justificări, prin folosirea cuvintelor în înțelesul lor curent din limba română. Conceptele și noțiunile utilizate sunt configurate în concordanță cu dreptul pozitiv, iar stabilirea soluțiilor normative este departe de a fi ambiguă, acestea fiind redacte previzibil și 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, Președintele 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 și protecția infrastructurilor critice, aprobată cu modificări prin Legea nr. 18/2011, cu modificările ulterioare, astfel cum autorul obiecției de neconstituționalitate susține. În sprijinul acestei afirmații se invocă prevederile art. 2 alin. (2) din legea criticată, potrivit cărora dispozițiile legii nu se aplică instituțiilor din domeniul apărării, ordinii publice și securității naționale, precum și Oficiului Registrului Național al Informațiilor Secrete de Stat.

18. Prin urmare, argumentele autorului obiecției de neconstituționalitate 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 reține nici încălcarea jurisprudenței Curții Constituționale 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 susține 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 obiecției de neconstituționalitate, 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 susține că obiecția de neconstituționalitate formulată este neîntemeiată.

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

CURTEA,

examinând obiecția de neconstituționalitate, punctul de vedere al președintelui Camerei Deputaților, raportul întocmit de judecătorul-raportor, dispozițiile legii criticate, raportate la prevederile Constituției, precum și Legea nr.47/1992, reține următoarele:

14. Curtea Constituțională a fost legal sesizată și este competentă, potrivit dispozițiilor art.146 lit.a) din Constituție, precum și ale art.1, art.10, art.15 și art.18 din Legea nr.47/1992, republicată, să soluționeze obiecția de neconstituționalitate.

15. **Obiectul controlului de constituționalitate** îl constituie dispozițiile Legii privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

16. Textele constituționale invocate în motivarea obiecției de neconstituționalitate sunt art.1 alin.(5) privind principiul legalității și principiul securității raporturilor juridice și art.119 referitor la Consiliul Suprem de Apărare a Țării.

17. **Analizând admisibilitatea obiecției de neconstituționalitate**, sub aspectul **titularului dreptului de sesizare**, a **termenului** în care acesta este îndrituit să sesizeze instanța constituțională, precum și a **obiectului controlului de constituționalitate**, Curtea constată că sesizarea care formează obiectul Dosarului nr.888A/2018 îndeplinește condițiile de admisibilitate prevăzute de art.146 lit.a) teza întâi din Constituție. Astfel, în acord cu cele statuate în jurisprudența sa, Curtea constată că primele două condiții se referă la regularitatea sesizării instanței constituționale, din perspectiva legalei sale sesizări, iar cea de-a treia vizează stabilirea sferei sale de competență, astfel încât constatarea neîndeplinirii uneia dintre aceste condiții are efecte dirimante, făcând inutilă analiza celorlalte condiții [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 și 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 privește **titularul dreptului de sesizare**, Curtea constată că este îndeplinită condiția de admisibilitate, obiecția de neconstituționalitate fiind formulată de Președintele României, în temeiul art.146 lit.a) teza întâi din Constituție.

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

20. În interiorul termenului de promulgare de 20 de zile, prevăzut de art.77 alin. (1) din Constituție, Președintele României a formulat la data de 11 iunie 2018 prezenta obiecție de neconstituționalitate, astfel că și sub acest aspect sesizarea este admisibilă. Cu privire la modul de calcul al termenelor în interiorul cărora poate fi exercitat controlul *a priori*, Curtea Constituțională s-a pronunțat în jurisprudența sa și 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 desfășurarea raporturilor constituționale dintre autoritățile publice și, prin urmare, în măsura în care nu se prevede altfel în mod expres, nu se calculează pe zile libere”. Dispozițiile art.181 alin.(1) pct.2 din Codul de procedură civilă, potrivit cărora „când termenul se socotește pe zile, nu intră în calcul ziua de la care începe să curgă termenul, nici ziua când acesta se împlinește”, 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 și ziua în care el începe să curgă și ziua când se împlinește (a se vedea și 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 rețelelor și sistemelor informatice a fost, potrivit Hotărârii nr.E43 din 4 aprilie 2018, inițiat de Guvern și a fost supus spre adoptare Senatului, ca primă Cameră sesizată, cu procedura de urgență prevăzută de art.76 alin.(3) din Constituție. Legea a fost adoptată de Senat, cu respectarea prevederilor art.76 alin.(2) din Constituție, la data de 25 aprilie 2018 (rezultat vot: pentru=86, contra=0, abțineri=0). Ulterior a fost dezbătută și adoptată de plenul Camerei Deputaților, la data de 16 mai 2018, (rezultat vot: pentru=253, contra=0, abțineri =1, nu au votat =1).

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

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

24. Așa fiind, înainte de a analiza lipsa avizului Consiliului Suprem de Apărare a Țării 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 rețelelor și sistemelor informatice vizează securitatea națională, fapt care ar impune obligativitatea obținerii acestui aviz.** În acest sens, Curtea constată că Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice a fost emisă în aplicarea Directivei 2016/1148 (NIS, Network Internet Security) a Parlamentului European și a Consiliului Uniunii Europene din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și 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 rețelelor și sistemelor informatice menit să transpună obiectivele Strategiei Europene de securitate cibernetică stabilite pentru pilonul NIS. Directiva a fost emisă în vederea protejării rețelelor, sistemelor și serviciilor informatice care îndeplinesc un rol vital în societate, fiabilitatea și securitatea lor fiind esențiale pentru activitățile economice și societale și, în special, pentru funcționarea pieței interne. Totodată, s-a urmărit contracararea amplitudinii, frecvenței și impactului incidentelor de securitate care sunt în creștere și reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Aceasta cu atât mai mult cu cât sistemele respective pot să devină, de asemenea, o țintă pentru acțiunile dăunătoare deliberate menite să afecteze sau să întrerupă funcționarea sistemelor. Având în vedere dimensiunea mondială a problemelor de securitate care afectează rețelele și sistemele informatice, este nevoie de o cooperare internațională mai strânsă pentru a îmbunătăți standardele de securitate și schimbul de informații și pentru a promova o abordare internațională comună a aspectelor de securitate. Responsabilitatea asigurării securității rețelelor și a sistemelor informatice revine în mare măsură operatorilor de servicii esențiale și furnizorilor de servicii digitale. Ar trebui să se promoveze și să se dezvolte prin cerințe adecvate de

reglementare și practici voluntare sectoriale o cultură a gestionării riscurilor, care să implice evaluarea riscurilor și aplicarea unor măsuri de securitate adecvate riscurilor întâmpinate. Stabilirea unor condiții de concurență al căror caracter echitabil să prezinte încredere este și ea esențială pentru funcționarea eficace a grupului de cooperare și a rețelei 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 național a adoptat prezenta lege, al cărei obiect constă în stabilirea unui cadru 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.

27. În acord cu art.2 alin.(1) din lege, scopul său constă în **stabilirea cadrului de cooperare la nivel național și de participare la nivel european și internațional în domeniul asigurării securității rețelelor și sistemelor informatice**; desemnarea **autorității competente la nivel național și a entităților de drept public și privat care dețin competențe și responsabilități în aplicarea prevederilor prezentei legi, a Punctului unic de contact la nivel național și a echipei naționale de intervenție în caz de incidente de securitate informatică**; precum și în stabilirea cerințelor de securitate și notificare pentru operatorii de servicii esențiale și pentru furnizorii de servicii digitale și instituirea mecanismelor de actualizare a acestora **în funcție de evoluția amenințărilor la adresa securității rețelelor și sistemelor informatice**.

28. În legislația națională există deja în vigoare o serie de reglementări, acte normative cu caracter primar sau secundar, care au legătură cu domeniul securității naționale. Astfel, **Ordonanța de urgență a Guvernului nr.98/2010** privind identificarea, desemnarea și protecția infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I, nr. 757 din 12 noiembrie 2010, aprobată cu modificări prin Legea nr.18/2011, publicată în Monitorul Oficial al României, Partea I, nr. 183 din 16 martie 2011, stabilește cadrul legal privind identificarea, desemnarea

infrastructurilor critice naționale/europene și evaluarea necesității de a îmbunătăți protecția acestora, în scopul creșterii capacității de asigurare a stabilității, securității și siguranței sistemelor economico-sociale și protecției persoanelor. Ordonanța transpune prevederile Directivei 2008/114/CE a Parlamentului European și Consiliului Uniunii Europene din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, publicată în Jurnalul Oficial al Uniunii Europene seria L nr. 345 din 23 decembrie 2008. Actul normativ definește infrastructura critică națională, denumită ICN, ca fiind un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național, care este esențial pentru menținerea funcțiilor vitale ale societății, a sănătății, siguranței, securității, bunăstării sociale ori economice a persoanelor și a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel național ca urmare a incapacității de a menține respectivele funcții, iar potrivit anexei nr.1 lista sectoarelor infrastructurii critice naționale vizează **energia**, tehnologia informației și comunicații, **alimentare cu apă**, alimentație, **sănătate**, **securitate națională**, administrație, **transporturi**, industria chimică și nucleară și spațiu și cercetare. Or, o parte dintre aceste sectoare critice se regăsesc și în legea contestată în prezenta cauză respectiv, energie, alimentare cu apă, sănătate și transporturi.

29. În aplicarea ordonanței de urgență mai sus menționate, a fost adoptată **Hotărârea Guvernului nr.718/2011** pentru aprobarea Strategiei naționale privind protecția infrastructurilor critice, publicată în Monitorul Oficial al României, Partea I, nr. 555 din 4 august 2011.

30. De asemenea, Curtea reține că prin **Hotărârea Guvernului nr.494/2011**, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, s-a reglementat înființarea ca instituție publică cu personalitate juridică, în coordonarea Ministerului Comunicațiilor și Societății Informaționale (MCSI), a **Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO** (instituție la care face trimitere și **Legea privind asigurarea unui nivel comun**

ridicat de securitate a rețelelor și sistemelor informatice), structură independentă de expertiză și cercetare-dezvoltare în domeniul **protecției infrastructurilor cibernetice**. Centrul este condus de un director general și de un director general adjunct, sprijiniți de **Comitetul de coordonare, din care fac parte reprezentanți ai MCSI, Ministerului Apărării Naționale, Ministerului Administrației și Internelor, Serviciului Român de Informații, Serviciului de Informații Externe, Serviciului de Telecomunicații Speciale, Serviciului de Protecție și Pază, Oficiului Registrului Național al Informațiilor Secrete de Stat și ai Autorității Naționale pentru Administrare și Reglementare în Comunicații**. Hotărârea de Guvern definește termeni și expresii, precum infrastructură cibernetică, spațiu cibernetic, securitate cibernetică, atac cibernetic, incident cibernetic etc. și stabilește atribuțiile CERT-RO.

31. Un alt act normativ emis în domeniul securității naționale îl constituie **Hotărârea Guvernului nr.271/2013** pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național 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 și direcțiile majore de acțiune pentru cunoașterea, prevenirea și contracararea amenințărilor, vulnerabilităților și riscurilor la adresa securității cibernetice a României și pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic. În acest sens, stabilește semnificația termenilor și expresiilor utilizați în domeniu, prevede înființarea **Sistemului național de securitate cibernetică (SNSC)** care reprezintă cadrul general de cooperare ce reunește autorități și instituții publice cu responsabilități și capacități în domeniu, în vederea coordonării acțiunilor la nivel național pentru asigurarea securității spațiului cibernetic, inclusiv prin cooperarea cu mediul academic și cel de afaceri, asociațiile profesionale și organizațiile neguvernamentale. De asemenea, potrivit acesteia, **Consiliul operativ de securitate cibernetică (COSCC)** reprezintă organismul prin care se realizează coordonarea unitară

a SNSC. Din COSC fac parte, în calitate de membri permanenți, reprezentanți ai Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului pentru Societatea Informațională, Serviciului Român de Informații, Serviciului de Telecomunicații Speciale, Serviciului de Informații Externe, Serviciului de Protecție și Pază, Oficiului Registrului Național al Informațiilor Secrete de Stat, precum și secretarul Consiliului Suprem de Apărare a Tării. Conducerea COSC este asigurată de un președinte (consilierul prezidențial pe probleme de securitate națională) și un vicepreședinte (consilierul prim-ministrului pe probleme de securitate națională). Coordonatorul tehnic al COSC este Serviciul Român de Informații, în condițiile legii.

33. Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică este conținut în anexa nr.2 la hotărâre și este un document clasificat.

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 siguranței naționale” printre scopurile care pot sta la baza restrângerii exercițiului unor drepturi sau al unor libertăți. Ca urmare a revizuirii Constituției în anul 2003, conceptul de „siguranță națională” a fost înlocuit cu cel de „securitate națională”. Totodată, Curtea a observat că, în Raportul asupra amendamentelor la Propunerea legislativă privind revizuirea Constituției întocmit de Comisia pentru elaborarea propunerii legislative privind revizuirea Constituției, referitor la înlocuirea sintagmei „siguranță națională” cu cea de „securitate națională”, s-a precizat că „sintagma «securitate națională» este utilizată atât în Uniunea Europeană, cât și în cadrul North Atlantic Treaty Organization (NATO) cu un conținut ce asigură compatibilitatea țării noastre cu standardele de apărare colectivă ale acestora, iar termenul «siguranță națională» 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, siguranța națională a României. Ulterior, prin Legea nr.255/2013 pentru punerea în aplicare a Legii nr. 135/2010 privind Codul de procedură penală și pentru modificarea și completarea unor acte normative care cuprind dispoziții procesual penale, sintagma „siguranță națională” a fost înlocuită cu cea de „securitate națională”, atât în titlul, cât și în cuprinsul Legii nr. 51/1991. De asemenea, Curtea a reținut că, în același raport, anterior menționat, referitor la introducerea în Legea fundamentală a unui nou articol cu denumirea marginală „*Securitatea națională*”, care conținea definirea acestei noțiuni, Comisia pentru elaborarea propunerii legislative privind revizuirea Constituției a precizat că „noțiunea de «securitate națională», **prin diversitatea, complexitatea și dinamica ei**, este necesar a fi de domeniul legiuitorului ordinar, nu constituent, deoarece tocmai datorită acestei caracteristici, orice definiție s-ar putea dovedi inadecvată”.

37. Curtea a observat, totodată, că, în ceea ce privește Convenția pentru apărarea drepturilor omului și a libertăților fundamentale, securitatea națională este menționată în art.8 paragraful 2, art.10 și art.11 ca un prim scop legitim care poate sta

la baza restrângerii drepturilor și libertăților prevăzute de aceste prevederi. Convenția pentru apărarea drepturilor omului și a libertăților fundamentale nu definește termenul de „*securitate națională*”, Comisia Europeană a Drepturilor Omului statuând că acesta nu poate fi definit în mod exhaustiv, bucurându-se de un nivel de elasticitate și flexibilitate, care se reflectă în marja de apreciere a statului în această materie. Astfel, Comisia a reținut că principiile accesibilității și previzibilității nu necesită în mod necesar o definiție exhaustivă a noțiunii de „*interese ale securității naționale*”. Multe legi, care prin obiectul lor de reglementare trebuie să prezinte un anumit grad de flexibilitate, intră, în mod inevitabil, în categoria celor care folosesc termeni care sunt într-o măsură mai mare sau mai mică vagi și a căror interpretare și aplicare sunt chestiuni de practică (Decizia de inadmisibilitate din 2 aprilie 1993, pronunțată în *Cauza Esbester împotriva Regatului Unit*).

38. Curtea a reținut că termenul „*securitate națională*” este unul plurivalent. Astfel, din punct de vedere al art.53 alin.(1) din Constituție, se poate vorbi de *securitate militară, economică, financiară, informatică, socială a țării*. Oricare dintre aceste tipuri de securitate poate fi ținta unei amenințări interne sau externe, motiv pentru care legiuitorul ar putea recurge la restrângerea exercițiului unor drepturi sau libertăți constituționale. De asemenea, s-a precizat că termenul de „siguranță națională” vizează protecția statului, mai ales în ceea ce privește integritatea teritorială și independența națională și că siguranța sau securitatea socială **vizează protecția societății**. Totodată, Curtea a reamintit jurisprudența sa referitoare la noțiunea de „*securitate națională*”, potrivit căreia, această noțiune nu implică numai securitatea militară, deci domeniul militar, ci **are și o componentă socială și economică**. Astfel, nu numai existența unei situații *manu militari* atrage aplicabilitatea noțiunii de „*securitate națională*” din textul art. 53 din Legea fundamentală, ci și alte aspecte din viața statului - precum cele economice, financiare, sociale - care ar putea afecta însăși ființa statului prin amploarea și gravitatea fenomenului.

39. Așa fiind, Curtea a constatat că, deși sintagma în discuție a fost, în mod tradițional, asociată cu apărarea militară a statului, **sfera de cuprindere a acesteia transcende strategiilor exclusiv militare, înglobând elemente și 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 noțiunea de „*securitate națională*” este folosită ca o continuare și dezvoltare a celei de „*siguranță națională*”. Astfel, potrivit art.1 din Legea nr.51/1991, „*Prin securitatea națională a României se înțelege starea de legalitate, de echilibru și de stabilitate socială, economică și politică necesară existenței și dezvoltării statului național român ca stat suveran, unitar, independent și indivizibil, menținerii ordinii de drept, precum și a climatului de exercitare neîngrădită a drepturilor, libertăților și îndatoririlor fundamentale ale cetățenilor, potrivit principiilor și normelor democratice statornicite prin Constituție*”. Potrivit art.2 alin.(1) din Legea nr.51/1991, realizarea securității naționale se înfăptuiește prin cunoașterea, prevenirea și înlăturarea amenințărilor interne sau externe ce pot aduce atingere valorilor prevăzute în art.1 din același act normativ. Astfel, Curtea a constatat că realizarea securității naționale nu reprezintă o proiecție viitoare, ci este un proces continuu care menține starea de securitate națională existentă. În acest sens, Curtea a statuat că, spre deosebire de „apărarea țării”, care presupune posibilitatea unei intervenții active, dinamice în cazul unor atacuri sau al unor acțiuni ostile din exterior, **„securitatea națională” implică activități destinate menținerii unei stări preexistente de liniște și de siguranță 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, pronunțată în Cauza C-373/13 din 24 iunie 2015, prin care Curtea de Justiție a Uniunii Europene a interpretat noțiunea „*motive imperioase de siguranță națională 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 conviețuirii în pace a popoarelor ori atingerea adusă intereselor militare pot afecta siguranța publică. În plus, Curtea a decis că noțiunea „ *motive imperative de siguranță publică*” presupune nu numai existența unei atingeri aduse siguranței publice, ci și ca o asemenea atingere să prezinte un nivel de gravitate deosebit de ridicat, exprimat prin utilizarea sintagmei „ *motive imperative*”. Noțiunea „ *ordine publică*” a fost interpretată în jurisprudența Curții în sensul că recurgerea la aceasta presupune întotdeauna, pe lângă tulburarea ordinii sociale pe care o reprezintă orice încălcare a legii, existența unei amenințări reale, actuale și suficient de grave la adresa unui interes fundamental al societății. Curtea a stabilit, totodată, că statele membre rămân libere să stabilească, în conformitate cu nevoile lor naționale, care pot varia de la un stat membru la altul și de la o perioadă la alta, cerințele de ordine publică și de siguranță națională.

42. Chiar dacă legea contestată nu mai definește securitatea cibernetică ca fiind o componentă a securității naționale a României, Curtea va analiza dacă, din interpretarea sistematică a normelor instituite prin legea criticată, acestea au sau nu incidență/legătură asupra/cu securității/securitatea naționale/națională.

43. Atât prin Directiva 2016/1148, cât și prin prezenta lege, în cazul sistemelor informatice care asigură furnizarea serviciilor esențiale 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 și care pot viza, inclusiv acțiuni de spionaj cibernetic, cu scopul de a obține neautorizat informații confidențiale, în interesul unei entități 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 și sunt săvârșite cu vinovăție, prin intermediul ori asupra infrastructurilor ciberneticе (a se vedea în acest sens art.181 din Codul penal referitor la definirea expresiilor „Sistem informatic” și „Date informatice”, art.360 din Codul penal referitor la *Accesul ilegal la un sistem informatic* și 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 și extinderea lui, ceea ce ar duce la urmări sociale foarte grave, cu atât mai mult cu cât dezvoltarea rapidă a tehnologiilor moderne de informații și comunicații - condiție *sine qua non* a edificării societății informaționale - a avut un impact major asupra ansamblului social, marcând adevărate mutații în filozofia de funcționare a economicului, politicului și culturalului, dar și asupra vieții de zi cu zi a individului.

44. Practic, dispozițiile Directivei 2016/1148 (NIS, Network Internet Security) creează structurile necesare pentru cooperarea strategică și operațională între statele membre și vizează creșterea nivelului de reziliență al rețelelor și al sistemelor informatice de pe teritoriul Uniunii Europene. Mai mult decât atât, aceasta impune o abordare globală la nivelul Uniunii, care să includă cerințele comune privitoare la crearea capacităților minime și a planificării, a schimbului de informații, a cooperării și măsurilor comune de securitate pentru operatorii de servicii esențiale și a furnizorilor de servicii digitale, fără a-i împiedica pe aceștia 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 rețelelor și sistemelor, precum și în cele de cooperare cu autorități din alte domenii, cum ar fi asigurarea ordinii publice, protecția datelor cu caracter personal.

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

47. Deși în art.2 alin.(2) din actul normativ contestat se menționează că prezenta lege nu se aplică instituțiilor din domeniul apărării, ordinii publice și securității naționale, precum și Oficiului Registrului Național al Informațiilor Secrete de Stat, cu toate acestea, Curtea constată că modul în care sunt definite conceptele de: *operator de servicii esențiale, securitatea rețelelor și a sistemelor informatice, strategie națională privind securitatea rețelelor și a sistemelor informatice și 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 rețin:

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

- „*securitatea rețelelor și a sistemelor informatice*” ca fiind capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea, confidențialitatea

sau nonrepudierea datelor stocate ori transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

- „*strategie națională privind securitatea rețelelor și a sistemelor informatice*” ca fiind cadrul care furnizează obiective și priorități strategice privind securitatea rețelelor și sistemelor informatice la nivel național.

49. Totodată, potrivit **art.6 alin.(1) lit.a) și art.14 din lege** „*Un serviciu este considerat esențial dacă furnizarea lui îndeplinește cumulativ următoarele condiții: a) serviciul este esențial în susținerea unor activități societale și/sau economice de cea mai mare importanță; b) furnizarea sa depinde de o rețea sau de un sistem informatic; c) furnizarea serviciului este perturbată semnificativ în cazul producerii unui incident*” iar „*Strategia națională privind securitatea rețelelor și 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 rețelelor și sistemelor informatice, Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO) se consultă și cooperează, între altele, atât cu Serviciul Român de Informații, **pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale a căror afectare aduce atingere securității naționale**, cât și cu Ministerul Afacerilor Interne, Oficiul Registrului Național al Informațiilor Secrete de Stat, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază, pentru securitatea rețelelor și a sistemelor informatice care asigură servicii esențiale **în domeniul lor de activitate și responsabilitate** [a se vedea art.15 alin.(2) lit.a) și c) din lege].

51. Totodată, CERT-RO în calitate de autoritate competentă la nivel național „*elaborează și actualizează, după consultarea celorlalte instituții cu responsabilități în domeniul apărării, ordinii publice și securității naționale, precum și a altor instituții și autorități, după caz, normele metodologice, tehnice, precum și*

regulamentele privind cerințele referitoare la înființarea, autorizarea și funcționarea 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 relațiile sociale referitoare la securitatea rețelelor și sistemelor informatice vizează un interes general a cărui amploare **impune calificarea acestui domeniu ca fiind în strânsă interdependență cu securitatea națională**. Această teză este susținută de împrejurarea că, Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice **reglementează cu privire la servicii publice esențiale (energie, alimentare cu apă, sănătate și transporturi), care prin natura lor pot afecta securitatea națională**.

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

54. Astfel, criticile vizând lipsa solicitării sau existenței unor avize în procedura de elaborare a actelor normative au fost calificate de Curte ca aspecte ce țin de respectarea obligațiilor legale ale autorităților implicate în această procedură și, implicit, ca vizând o neconstituționalitate a actelor normative, care poate fi analizată doar în condițiile **art.146 lit. a) și d) din Constituție** (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 Constituție, Consiliul Suprem de Apărare a Țării *„organizează și coordonează unitar activitățile care privesc apărarea țării și securitatea națională [...]”*. În realizarea acestui rol, potrivit art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea și funcționarea Consiliului Suprem de Apărare a

Țării, „avizează proiectele de acte normative inițiate sau emise de Guvern privind: **securitatea națională** [...]”, competență ce își are izvorul în textul constituțional.

56. Deși norma constituțională, exprimând rolul Consiliului Suprem de Apărare a Țării de coordonare unitară a activităților care privesc securitatea națională, nu face niciun fel de referire expresă la obligația inițiatorilor proiectelor de acte normative de a solicita avizul acestei autorități, avizarea proiectelor de acte normative ce privesc securitatea națională este tratată în Legea nr.415/2002, mai sus menționată, și care reprezintă o reflectare a normei constituționale consacrate de art.119 din Legea fundamentală. De aceea, indiferent că este vorba de o competență acordată prin lege sau direct prin textul Constituției, autoritățile sunt obligate să o aplice și să o respecte în virtutea art.1 alin.(5) din Constituție, potrivit căruia „În România, respectarea Constituției, a supremației sale și a legilor este obligatorie”. O atare concluzie se impune datorită faptului că principiul legalității este unul de rang constituțional (a se vedea Decizia Curții Constituționale nr.901 din 17 iunie 2009, publicată în Monitorul Oficial al României, Partea I, nr. 503 din 21 iulie 2009).

57. În jurisprudența sa, Curtea Constituțională a statuat că lipsa avizului autorităților publice implicate nu conduce în mod automat la neconstituționalitatea legii asupra căreia acesta nu a fost dat, întrucât ceea ce prevalează constă în obligația Guvernului de a-l solicita. Împrejurarea că autoritatea care trebuie să emită un astfel de aviz, deși i s-a solicitat, nu și-a îndeplinit această atribuție „constituie o înțelegere greșită a rolului său legal și constituțional, fără a fi însă afectată constituționalitatea 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. și 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 față Curtea constată că, dimpotrivă, avizul Consiliului Suprem de Apărare a Țării nu a fost solicitat.**

59. Așa fiind, potrivit art.4 lit.d) pct.1 din Legea nr.415/2002 privind organizarea și funcționarea Consiliului Suprem de Apărare a Țării, acesta „avizează proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională”, 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 inițiatorul trebuie să solicite avizul autorităților interesate în aplicarea acestora, în funcție de obiectul reglementării”. De asemenea, art.31 alin.(3) din aceeași lege prevede că „Forma finală a instrumentelor de prezentare și motivare a proiectelor de acte normative trebuie să cuprindă referiri la avizul Consiliului Legislativ și, după caz, al **Consiliului Suprem de Apărare a Țării**, Curții de Conturi sau Consiliului Economic și Social”. Așadar, în temeiul acestor dispoziții legale, Guvernul avea obligația de a solicita avizul Consiliului Suprem de Apărare a Țării atunci când a elaborat proiectul Legii privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

60. Pentru argumentele expuse, întrucât în cadrul procedurii legislative, inițiatorul nu a respectat obligația legală, conform căreia Consiliul Suprem de Apărare a Țării avizează proiectele de acte normative inițiate sau emise de Guvern privind securitatea națională, Curtea constată că actul normativ a fost adoptat cu încălcarea prevederilor constituționale ale art.1 alin.(5) care consacră principiul legalității și ale art.119 referitoare la atribuțiile Consiliului Suprem de Apărare a Țării (a se vedea și 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) și al art.147 alin.(4) din Constituție, precum și al art.11 alin.(1) lit.A.a), al art.15 alin.(1) și al art.18 alin.(2) din Legea nr.47/1992, cu unanimitate de voturi,

CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

Admite obiecția de neconstituționalitate formulată și constată că Legea privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice este neconstituțională, în ansamblul său.

Definitivă și general obligatorie.

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

Pronunțată în ședința din data de 4 iulie 2018.

**PREȘEDINTELE
CURȚII CONSTITUȚIONALE,**


Prof.univ.dr. Valer Dorneanu


MAGISTRAT-ASISTENT,

Afrodita Laura Tuțunaru

