MONITORUL OFICIAL AL ROMÂNIEI

Anul 189 (XXXIII) — Nr. 918

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Vineri, 24 septembrie 2021

SUMAR

DECIZII ALE CURȚII CONSTITUȚIONALE

CURTEA CONSTITUȚIONALĂ

DECIZIA Nr. 384
din 8 iunie 2021

referitoare la excepția de neconstituționalitate a prevederilor art. 42 și art. 43 din Ordonanța de urgență a Guvernului nr. 80/2013 privind taxele judiciare de timbru

Valer Dorneanu — președinte
Cristian Deliorga — judecător
Marian Enache — judecător
Daniel Marius Morar — judecător
Gheorghe Stan — judecător
Livia Doina Stanciu — judecător
Elena-Simina Tănăsescu — judecător
Varga Attila — judecător
Ingrid Alina Tudora — magistrat-asistent

Cu participarea reprezentantului Ministerului Public, procuror Loredana Brezeanu.

1. Pe rol se află soluționarea excepției de neconstituționalitate a prevederilor art. 42 și art. 43 din Ordonanța de urgență a Guvernului nr. 80/2013 privind taxele judiciare de timbru, excepție ridicată de Kasai Marec în Dosarul nr. 25.561/325/2017 al Tribunalului Timiș — Secția de contencios administrativ și fiscal. Excepția formează obiectul Dosarului Curții Constituționale nr. 1.703D/2018.

2. La apelul nominal lipsesc părțile. Procedura de citare este legal îndeplinită.

3. Cauza fiind în stare de judecată, președintele Curții acordă cuvântul reprezentantului Ministerului Public, care pune concluzii de respingere, ca neîntemeiată, a excepției de neconstituționalitate. În acest sens, invocă jurisprudența în materie a Curții Constituționale, concretizată, spre exemplu, prin Decizia nr. 552 din 7 iulie 2020.

C U R T E A,

având în vedere actele și lucrările dosarului, reține următoarele:

4. Prin Încheierea din 24 octombrie 2018, pronunțată în Dosarul nr. 25.561/325/2017, **Tribunalul Timiș — Secția de contencios administrativ și fiscal a sesizat Curtea Constituțională cu excepția de neconstituționalitate a prevederilor art. 42 și art. 43 din Ordonanța de urgență a Guvernului nr. 80/2013 privind taxele judiciare de timbru.** Excepția de neconstituționalitate a fost ridicată de Kasai Marec într-o cauză având ca obiect o plângere contravențională.

5. **În motivarea excepției de neconstituționalitate**, autorul acesteia susține, în esență, că accesul liber la justiție este compatibil cu reglementarea unor proceduri speciale, pentru situații deosebite, cu condiția asigurării posibilității neîngrădite a tuturor celor interesați de a utiliza aceste proceduri, în formele și modalitățile prevăzute de lege, precum și a asigurării caracterului efectiv al acestui drept. Susține că procedura contravențională este o parte specială a procedurii de drept administrativ, iar întreaga procedură de contestare a procesului-verbal de contravenție, ce presupune judecata în primă instanță și în calea de atac a apelului, intră în sfera de jurisdicție specială administrativă, context în care arată că art. 21 alin. (4) din Constituție consacră accesul gratuit și necondiționat de plata unor taxe judiciare de timbru.

6. În ceea ce privește art. 16 din Constituție, care consacră principiul general al egalității, autorul excepției arată că acesta se referă la o egalitate juridică formală, și nu la o egalitate de condiții, iar egalitatea în fața legii și a autorităților publice nu implică ideea de uniformizare, în sensul de a se aplica tuturor cetățenilor același regim juridic, indiferent de situația naturală sau socioprofesională a acestora. Dimpotrivă, presupune și dreptul la diferențiere în aplicarea tratamentului juridic, dacă situațiile în care se află cetățenii sunt diferite. Învederează, totodată, că jurisprudența recentă a instanței constituționale confirmă această interpretare a principiului egalității, care se referă la egalitatea cetățenilor în fața legii și a autorităților publice, iar nu la egalitatea de tratament juridic aplicat unei categorii de cetățeni în comparație cu alta. Aceasta, deoarece drepturile fundamentale reprezintă o constantă a personalității cetățeanului, o șansă egală acordată oricărui individ, iar art. 16 alin. (1) din Constituție vizează egalitatea în drepturi între cetățeni, nu și identitatea de tratament juridic asupra aplicării unor măsuri, indiferent de natura lor, astfel că instanța de contencios constituțional justifică nu numai constituționalitatea administrării unui regim juridic diferit față de anumite categorii de persoane, dar și necesitatea unui asemenea tratament juridic.

7. **Tribunalul Timiș — Secția de contencios administrativ și fiscal** arată că prevederile criticate reglementează procedura de soluționare a cererilor formulate de persoanele fizice sau juridice având ca obiect scutiri, reduceri, eșalonări sau amânări pentru plata taxelor judiciare de timbru, respectiv situațiile când pot fi formulate aceste cereri, instanța competentă, probatoriul necesar, procedura de soluționare, hotărârea pronunțată, calea de atac și termenul. În opinia instanței această procedură nu contravine însă dispozițiilor constituționale care consacră dreptul de acces la justiție și nici principiului egalității cetățenilor în fața legilor și autorităților publice, întrucât cererile pentru acordarea facilităților pentru plata taxelor de timbru pot fi formulate de orice persoană, fără niciun fel de limitări sau îngrădiri. Referitor la încălcarea dispozițiilor art. 1 alin. 5 din Constituție, instanța consideră că invocarea acestora nu are nicio relevanță în cauză.

8. Potrivit prevederilor art. 30 alin. (1) din Legea nr. 47/1992, încheierea de sesizare a fost comunicată președinților celor două Camere ale Parlamentului, Guvernului și Avocatului Poporului, pentru a-și exprima punctele de vedere asupra excepției de neconstituționalitate.

9. **Președinții celor două Camere ale Parlamentului, Guvernul** și **Avocatul Poporului** nu au comunicat punctele lor de vedere asupra excepției de neconstituționalitate.

C U R T E A,

examinând încheierea de sesizare, raportul întocmit de judecătorul-raportor, concluziile procurorului, dispozițiile legale criticate, raportate la prevederile Constituției, precum și Legea nr. 47/1992, reține următoarele:

10. Curtea Constituțională a fost legal sesizată și este competentă, potrivit dispozițiilor art. 146 lit. d) din Constituție, precum și ale art. 1 alin. (2), ale art. 2, 3, 10 și 29 din Legea nr. 47/1992, să soluționeze excepția de neconstituționalitate.

11. **Obiectul excepției de neconstituționalitate** îl constituie prevederile art. 42 și art. 43 din Ordonanța de urgență a Guvernului nr. 80/2013 privind taxele judiciare de timbru, publicată în Monitorul Oficial al României, Partea I, nr. 392 din 29 iunie 2013, cu modificările și completările ulterioare, care au următorul cuprins:

— Art. 42: *„(1) Persoanele fizice pot beneficia de scutiri, reduceri, eșalonări sau amânări pentru plata taxelor judiciare de timbru, în condițiile Ordonanței de urgență a Guvernului nr. 51/2008 privind ajutorul public judiciar în materie civilă,*

aprobată cu modificări și completări prin Legea nr. 193/2008, cu modificările și completările ulterioare.

(2) Instanța acordă persoanelor juridice, la cerere, facilități sub formă de reduceri, eșalonări sau amânări pentru plata taxelor judiciare de timbru datorate pentru acțiuni și cereri introduse la instanțele judecătorești, în următoarele situații:

a) cuantumul taxei reprezintă mai mult de 10% din media venitului net pe ultimele 3 luni de activitate;

b) plata integrală a taxei nu este posibilă deoarece persoana juridică se află în curs de lichidare sau dizolvare ori bunurile acesteia sunt, în condițiile legii, indisponibilizate.

(3) În mod excepțional, instanța poate acorda persoanelor juridice reduceri, eșalonări sau amânări pentru plata taxelor judiciare de timbru, în alte cazuri în care apreciază, față de datele referitoare la situația economico-financiară a persoanei juridice, că plata taxei de timbru, la valoarea datorată, ar fi de natură să afecteze în mod semnificativ activitatea curentă a persoanei juridice.

(4) Reducerea taxei de timbru poate fi acordată separat sau, după caz, împreună cu eșalonarea sau amânarea plății.”;

— Art. 43: *„(1) Cererea pentru acordarea facilităților la plata taxei judiciare de timbru se poate formula prin cererea de chemare în judecată sau în condițiile art. 33 alin. (2) ori art. 36.*

(2) Pentru soluționarea cererii de acordare a facilităților la plata taxei judiciare de timbru, instanța poate solicita orice lămuriri și dovezi părții sau informații scrise autorităților competente.

(3) Asupra cererii de acordare a facilităților la plata taxei de timbru instanța se pronunță fără citare, prin încheiere motivată dată în camera de consiliu. Încheierea se comunică solicitantului și părții adverse, dacă este cazul.

(4) Împotriva încheierii, părțile interesate pot formula cerere de reexaminare, în termen de 5 zile de la data comunicării încheierii. Cererea este scutită de la plata taxei judiciare de timbru.

(5) Cererea de reexaminare se soluționează în camera de consiliu de un alt complet, instanța pronunțându-se prin încheiere irevocabilă.”

12. În opinia autorului excepției de neconstituționalitate, aceste prevederi contravin dispozițiilor constituționale ale art. 1 alin. (5) privind obligativitatea respectării Constituției, a supremației sale și a legilor, ale art. 4 alin. (2) privind criteriile de nediscriminare coroborate cu art. 16 privind egalitatea în drepturi, precum și celor ale art. 21 privind accesul liber la justiție.

13. Examinând excepția de neconstituționalitate, Curtea reține că prevederile criticate din Ordonanța de urgență a Guvernului nr. 80/2013 au mai constituit obiect al controlului de constituționalitate, prin raportare la aceleași dispoziții constituționale invocate și în prezenta cauză, în acest sens fiind, cu titlu exemplificativ, Decizia nr. 479 din 30 iunie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 997 din 12 decembrie 2016, Decizia nr. 801 din 6 decembrie 2018, publicată în Monitorul Oficial al României, Partea I, nr. 244 din 29 martie 2019, Decizia nr. 29 din 17 ianuarie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 248 din 1 aprilie 2019, Decizia nr. 462 din 11 iulie 2019, publicată în Monitorul Oficial al României, Partea I, nr. 867 din 28 octombrie 2019, sau Decizia nr. 552 din 7 iulie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 756 din 19 august 2020, prin care Curtea a respins excepția de neconstituționalitate și a constatat că prevederile criticate sunt constituționale.

14. Raportat la criticile formulate în prezenta cauză, în jurisprudența sa, Curtea a statuat, cu valoare de principiu, că accesul la justiție nu presupune gratuitatea actului de justiție și nici, implicit, realizarea unor drepturi pe cale judecătorească în mod gratuit. De asemenea, art. 21 din Constituție nu instituie nicio interdicție cu privire la taxele în justiție, fiind legal și normal ca justițiabilii care trag un folos nemijlocit din activitatea desfășurată de autoritățile judecătorești să contribuie la acoperirea cheltuielilor acestora. Curtea a statuat că obligația de plată a taxelor judiciare de timbru este o obligație fiscală și este prevăzută de legea specială numai în sarcina celor care apelează la justiție, iar între beneficiarul serviciului public al justiției și instanța de judecată se stabilește un raport de drept fiscal, caracterizat prin relația de subordonare a părților. Plătitorul taxei judiciare de timbru se află într-un raport de autoritate cu instanța de judecată, separat și distinct de raportul juridic pe care îl are cu partea cu care se judecă și care este, de regulă, unul de drept privat, procesul debutând numai în măsura în care obligația de plată a taxei judiciare de timbru a fost executată.

15. În același sens este, de altfel, și jurisprudența Curții Europene a Drepturilor Omului prin care s-a statuat că „dreptul la un tribunal” nu este absolut, acest drept putând fi subiectul unor limitări atât timp cât nu este atinsă însăși substanța sa (Hotărârea din 28 mai 1985, pronunțată în Cauza *Ashingdane împotriva Regatului Unit,* paragraful 57). De asemenea, prin Hotărârea din 11 octombrie 2007, pronunțată în Cauza *Larco și alții împotriva României*, paragrafele 54 și 58, Curtea Europeană a Drepturilor Omului a statuat că obligația de a plăti în fața instanțelor civile o taxă judiciară corespunzătoare cererilor formulate nu poate fi considerată o limitare a dreptului de acces la o instanță sau o încălcare a dreptului la un proces echitabil.

16. Referitor la pretinsa neconstituționalitate a prevederilor art. 42 din Ordonanța de urgență a Guvernului nr. 80/2013, în jurisprudența amintită, Curtea Constituțională a observat că acestea statuează cu privire la faptul că persoanele fizice pot beneficia de scutiri, reduceri, eșalonări sau amânări pentru plata taxelor judiciare de timbru, în condițiile Ordonanței de urgență a Guvernului nr. 51/2008 privind ajutorul public judiciar în materie civilă, publicată în Monitorul Oficial al României, Partea I, nr. 327 din 25 aprilie 2008, iar, în mod excepțional, instanța poate acorda aceste facilități fiscale în alte cazuri în care apreciază că, față de datele referitoare la situația economico-financiară a persoanei juridice, plata taxei judiciare de timbru la valoarea datorată ar fi de natură să afecteze în mod semnificativ activitatea curentă a acesteia. Curtea nu a reținut însă pretinsa neconstituționalitate a acestor dispoziții din Ordonanța de urgență a Guvernului nr. 80/2013, ca urmare a faptului că aceste prevederi legale lasă la aprecierea instanței de judecată stabilirea ajutorului public judiciar, deoarece, pe de o parte, dispozițiile art. 8 alin. (1) și (2) din Ordonanța de urgență a Guvernului nr. 51/2008 reglementează criteriile în funcție de care beneficiul de ajutor public judiciar în formele prevăzute la art. 6 din aceasta se avansează de către stat fie în întregime, fie în proporție de 50%, iar, pe de altă parte, alin. (3) al aceluiași articol are în vedere și alte cazuri în care ajutorul public judiciar se poate acorda, proporțional cu nevoile solicitantului (a se vedea în acest sens Decizia nr. 713 din 27 octombrie 2015, publicată în Monitorul Oficial al României, Partea I, nr. 955 din 23 decembrie 2015).

17. Totodată, Curtea a observat că plata taxelor judiciare de timbru este o condiție legală pentru începerea proceselor civile, iar obligația la plata anticipată a acestor taxe este justificată. De altfel, contribuția justițiabilului poate fi recuperată la cererea acestuia, în temeiul art. 453 din Codul de procedură civilă, de la partea care pierde. Așadar, regula este cea a timbrării acțiunilor în justiție, excepțiile fiind posibile numai în măsura în care sunt stabilite de legiuitor. Astfel, potrivit dispozițiilor art. 90 din Codul de procedură civilă, cel care nu este în stare să facă față cheltuielilor pe care le presupune declanșarea și susținerea unui proces civil, fără a primejdui propria sa întreținere sau a familiei sale, poate beneficia de asistență judiciară, în condițiile legii speciale privind ajutorul public judiciar (Decizia nr. 533 din 9 octombrie 2014, publicată în Monitorul Oficial al României, Partea I, nr. 837 din 17 noiembrie 2014).

18. Cu privire la pretinsa încălcare a dispozițiilor art. 16 din Constituție, Curtea a constatat că legiuitorul a adoptat reglementări care vizează și acele situații în care partea nu poate face față cheltuielilor unui proces din cauza lipsei mijloacelor materiale. În acest sens sunt prevederile Ordonanței de urgență a Guvernului nr. 51/2008 și ale art. 42 din Ordonanța de urgență a Guvernului nr. 80/2013, prin care se instituie

posibilitatea instanței de judecată de a acorda scutiri, reduceri, eșalonări sau amânări pentru plata taxelor judiciare de timbru, la solicitarea justificată a părților interesate. Față de această împrejurare, având în vedere faptul că principiul egalității presupune ca la situații egale să se aplice un tratament juridic egal, fără nicio discriminare pe criterii arbitrare, și, în același timp, presupune și dreptul la diferențiere în tratament juridic, dacă situațiile în care se află cetățenii sunt diferite, nu se poate reține pretinsa discriminare pe criteriul averii, întrucât există mijloace legale prin care se asigură protecția drepturilor fundamentale, legiuitorul adoptând mecanisme de protecție a persoanelor vulnerabile din punct de vedere financiar, ceea ce constituie o garanție a accesului liber la justiție.

19. În ceea ce privește pretinsa încălcare a dispozițiilor art. 21 alin. (4) din Constituție, potrivit cărora *„Jurisdicțiile speciale administrative sunt facultative și gratuite”*, Curtea constată că autorul excepției pornește de la o premisă greșită, apreciind că procedura prevăzută de Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor ar reglementa o procedură jurisdicțională administrativă. Astfel, referitor la susținerile potrivit cărora jurisdicția în materia contravențională ar trebui să fie gratuită, astfel cum este jurisdicția administrativă, prin Decizia nr. 232 din 19 aprilie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 505 din 5 iulie 2016, Curtea a subliniat că acest aspect ține de voința legiuitorului, care este liber să acorde scutiri de la plata taxelor de timbru în considerarea anumitor situații specifice, fiind, așadar, la latitudinea legiuitorului să stabilească scutiri de taxe ori impozite sau, dimpotrivă, să instituie asemenea taxe.

20. Curtea învederează faptul că în materie contravențională, potrivit art. 19 din Ordonanța de urgență a Guvernului nr. 80/2013, plângerea împotriva procesului-verbal de constatare și sancționare a contravenției, precum și calea de atac împotriva hotărârii pronunțate se taxează cu 20 lei. De asemenea, potrivit art. 36 din Ordonanța Guvernului nr. 2/2001, astfel cum a fost modificat prin art. 53 din Ordonanța de urgență a Guvernului nr. 80/2013, „Pentru plângerea împotriva procesului-verbal de constatare și sancționare a contravenției, pentru recursul formulat împotriva hotărârii judecătorești prin care s-a soluționat plângerea, precum și pentru orice alte cereri incidente se percep taxele judiciare de timbru prevăzute de lege.” În acest context, Curtea a reținut că taxa instituită prin Ordonanța de urgență a Guvernului nr. 80/2013 este una fixă și nu depinde în niciun fel de tipul contravenției împotriva căreia se depune plângerea și nici de cuantumul amenzii (a se vedea Decizia nr. 265 din 4 iunie 2020, publicată în Monitorul Oficial al României, Partea I, nr. 728 din 12 august 2020). Față de această împrejurare, Curtea a reținut că o atare soluție legislativă este justificată atât timp cât legiuitorul optează, în materie contravențională, pentru sistemul unei taxe fixe, și nu la valoare (a se vedea, spre exemplu, Decizia nr. 510 din 5 decembrie 2013, publicată în Monitorul Oficial al României, Partea I, nr. 94 din 6 februarie 2014, și Decizia nr. 232 din 19 aprilie 2016, publicată în Monitorul Oficial al României, Partea I, nr. 505 din 5 iulie 2016), neputându-se reține, astfel, încălcarea principiului accesului liber la justiție.

21. În fine, referitor la constituționalitatea prevederilor art. 43 din Ordonanța de urgență a Guvernului nr. 80/2013, prin Decizia nr. 801 din 6 decembrie 2018, precitată, Curtea a reținut că încheierea prin care se soluționează cererea de acordare a facilităților la plata taxei judiciare de timbru se comunică solicitantului și părții adverse, dacă este cazul, aceștia putând formula cerere de reexaminare, ce va fi soluționată în camera de consiliu de un alt complet, instanța pronunțându-se prin încheiere irevocabilă. Instanța de judecată încuviințează acordarea ajutorului judiciar printr-o încheiere motivată, fără ca textul de lege să prevadă caracterul irevocabil al acestei încheieri, iar soluționarea cererii de reexaminare se face pe baza unor criterii obiective și presupune verificarea anumitor înscrisuri din care să rezulte starea materială a solicitantului și a familiei sale. În acest mod, legiuitorul nu a restrâns dreptul de acces liber la justiție sau dreptul la apărare, ci a asigurat celeritatea soluționării cererii prin care se contestă modul de acordare a facilităților la plata taxei judiciare de timbru. Curtea a avut în vedere și dispozițiile art. 17 alin. (1) din Ordonanța de urgență a Guvernului nr. 51/2008, potrivit cărora „Orice persoană interesată va putea sesiza oricând instanța care a încuviințat ajutorul public judiciar, prezentând dovezi cu privire la situația reală a celui căruia i s-a încuviințat cererea; ajutorul public judiciar nu se suspendă în cursul noilor cercetări”. Așadar, având în vedere că situația materială a celui care a solicitat acordarea ajutorului judiciar se poate modifica pe parcursul procesului, precum și luând în considerare eventualele cazuri în care solicitantul ar fi de rea-credință, legea a prevăzut, prin dispozițiile art. 17 alin. (1) din Ordonanța de urgență a Guvernului nr. 51/2008, posibilitatea persoanelor interesate de a se adresa instanței tocmai pentru a se restabili situația legală.

22. Întrucât nu au intervenit elemente noi, de natură să determine reconsiderarea jurisprudenței Curții Constituționale, atât soluția, cât și considerentele cuprinse în deciziile menționate își păstrează valabilitatea și în cauza de față.

23. Având în vedere cele mai sus menționate, Curtea apreciază că nu poate fi reținută nici critica privind încălcarea dispozițiilor cuprinse în art. 1 alin. (5) din Legea fundamentală.

24. Pentru considerentele expuse mai sus, în temeiul art. 146 lit. d) și al art. 147 alin. (4) din Constituție, precum și al art. 1—3, al art. 11 alin. (1) lit. A.d) și al art. 29 din Legea nr. 47/1992, cu unanimitate de voturi,

CURTEA CONSTITUȚIONALĂ

În numele legii

DECIDE:

Respinge, ca neîntemeiată, excepția de neconstituționalitate ridicată de Kasai Marec în Dosarul nr. 25.561/325/2017 al Tribunalului Timiș — Secția de contencios administrativ și fiscal și constată că prevederile art. 42 și art. 43 din Ordonanța de urgență a Guvernului nr. 80/2013 privind taxele judiciare de timbru sunt constituționale în raport cu criticile formulate.

Definitivă și general obligatorie.

Decizia se comunică Tribunalului Timiș — Secția de contencios administrativ și fiscal și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 8 iunie 2021.

PREȘEDINTELE CURȚII CONSTITUȚIONALE
prof. univ. dr. **VALER DORNEANU**

Magistrat-asistent,
Ingrid Alina Tudora

ORDONANȚE ALE GUVERNULUI ROMÂNIEI

GUVERNUL ROMÂNIEI

ORDONANȚĂ DE URGENȚĂ
privind înființarea Directoratului Național de Securitate Cibernetică

Provocările, riscurile și amenințările de securitate din spațiul cibernetic s-au intensificat în ultimii ani, iar securitatea cibernetică a devenit o necesitate ce implică abordări integrate, cuprinzătoare, adoptarea de strategii de securitate cibernetică, noi și permanente, investiții financiare semnificative și adaptări organizaționale rapide și ambițioase.

Având în vedere faptul că amenințările cibernetice nu au o adresă clară națională a unui expeditor, nu sunt blocate la granițele statale, au un profund caracter asimetric, întrucât, cu resurse relativ limitate, un individ sau un grup de indivizi, afiliați sau nu cu structuri guvernamentale, pot genera incidente cu efecte perturbatoare semnificative cu impact destabilizator la nivel statal sau al unui sector economic,

ținând cont de faptul că atât statele membre ale Uniunii Europene, cât și multe alte state, inclusiv NATO în anul 2016, au recunoscut spațiul cibernetic ca fiind un spațiu de confruntare și domeniu operațional, alături de domeniile terestru, aerian, cosmic și maritim,

considerând că, pentru asigurarea unui nivel ridicat de securitate a rețelelor și sistemelor informatice care stau la baza furnizării serviciilor esențiale la nivelul României ca stat membru al Uniunii Europene, implementarea Directivei UE 2016/1.148 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 este vitală pentru activitățile economice și societale și, în special, pentru funcționarea pieței interne,

ca urmare a evaluării de către Comisia Europeană a activității de implementare a Directivei UE 2016/1.148 la nivelul României, unde au fost constatate întârzieri și neconformități în abordarea națională,

ca urmare a Regulamentului (UE) 2021/887 al Parlamentului European și al Consiliului din 20 mai 2021 de înființare a Centrului de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică și a Rețelei de centre naționale de coordonare, găzduit în România,

având în vedere obligațiile naționale ce revin României din Strategia de securitate cibernetică a Uniunii Europene pentru deceniul digital, având la bază Comunicarea comună către Parlamentul European și Consiliu JOIN(2020) 18 final din 16 decembrie 2020,

motivat de faptul că în primul rând transformarea digitală expune statul, societatea, economia și cetățenii unor amenințări și atacuri cibernetice asimetrice caracterizate prin costuri scăzute și prin faptul că atacatorul deține inițial avantaje,

motivat de necesitatea dezvoltării capabilităților de răspuns care trebuie să evolueze în același timp cu atacurile cibernetice, atât prin prevenție, cât și prin reacție și intervenție specializată, de înaltă pregătire și adaptată noilor tipuri de atacuri cibernetice,

motivat de necesitatea consolidării rezilienței cibernetice, în contextul creșterii frecvenței și a complexității atacurilor cibernetice împotriva infrastructurilor ce susțin servicii esențiale pentru societatea și economia românească ce pot conduce la situații extraordinare de blocare a unor infrastructuri vitale dintr-o arie largă de domenii publice și private,

având ca obiectiv gestionarea amenințărilor cibernetice, în măsura în care riscurile asociate sunt foarte reale și semnificative, pentru prevenirea nesiguranței, a pierderilor economice sau a impactului asupra activităților,

mai mult, pentru o prezență mai activă a României pe harta mondială a statelor cu capacități de reacție și intervenție ridicate și, nu în ultimul rând, pentru ca România să devină un pol/nod de influență cibernetică regional/global și, implicit, pentru consolidarea imaginii internaționale a țării,

țintind ca noua instituție să devină o instituție de anvergură internațională care să poziționeze ferm România ca un lider recunoscut în securitatea cibernetică,

apreciind că cele de mai sus constituie premisele unei situații de urgență și extraordinare a cărei reglementare nu poate fi amânată,

în temeiul art. 115 alin. (4) din Constituția României, republicată,

Guvernul României adoptă prezenta ordonanță de urgență.

ARTICOLUL 1

Înființarea Directoratului

(1) Se înființează Directoratul Național de Securitate Cibernetică, denumit în continuare *DNSC*, organ de specialitate al administrației publice centrale, în subordinea Guvernului și în coordonarea prim-ministrului, cu personalitate juridică, finanțat integral din bugetul de stat, prin bugetul Secretariatului General al Guvernului.

(2) Centrul Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO se desființează la data intrării în vigoare a prezentei ordonanțe de urgență.

(3) La data intrării în vigoare a prezentei ordonanțe de urgență, DNSC preia activitățile, atribuțiile și personalul Centrului Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO, cu menținerea drepturilor salariale avute la data preluării.

(4) DNSC are sediul central în municipiul București, Strada Italiană nr. 22, sectorul 2, în imobilul proprietate a statului român și aflat în administrarea CERT-RO, potrivit Hotărârii Guvernului nr. 1.005/2020 privind transmiterea unui imobil aflat în domeniul public al statului din administrarea Ministerului Transporturilor, Infrastructurii și Comunicațiilor în administrarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO, cu destinația de sediu al CERT-RO, și pentru modificarea Hotărârii Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO.

(5) DNSC are calitatea de membru permanent în Consiliul Operativ de Securitate Cibernetică, denumit în continuare *COSC*.

(6) DNSC are responsabilități privind securitatea cibernetică a spațiului cibernetic național civil.

(7) DNSC are în structura internă compartimente funcționale, precum și alte structuri în subordinea sa, fără personalitate juridică.

(8) DNSC înființează structuri regionale și județene, fără personalitate juridică.

ARTICOLUL 2

Concepte, definiții și termeni

În înțelesul prezentei ordonanțe de urgență, termenii și expresiile de mai jos au următoarele semnificații:

a) *CSIRT* — echipă de răspuns la incidente de securitate cibernetică — entitate organizațională specializată care dispune de capacitatea necesară pentru prevenirea, analiza, identificarea și reacția la incidentele cibernetice;

b) *comunitatea CSIRT din România* — ansamblul echipelor CSIRT care funcționează în cadrul autorităților și instituțiilor publice ori al altor persoane juridice de drept public sau privat din România și care relaționează cu Directoratul Național de Securitate Cibernetică pe baza unor proceduri și protocoale de cooperare;

c) *spațiul cibernetic* — mediul virtual, astfel cum este definit în Strategia de securitate cibernetică a României și Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, aprobat prin Hotărârea Guvernului nr. 271/2013;

d) *spațiul cibernetic național civil* — spațiul cibernetic național care exclude infrastructurile cibernetice aflate, conform prevederilor legale, în administrarea sau responsabilitatea instituțiilor din sistemul național de apărare, ordine publică și securitate națională, precum și cele care vehiculează informații clasificate;

e) *securitate cibernetică* — stare de normalitate, astfel cum este definită în Strategia de securitate cibernetică a României și Planul de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică, aprobat prin Hotărârea Guvernului nr. 271/2013;

f) *amenințare cibernetică* — orice circumstanță, eveniment sau acțiune potențială care ar putea cauza daune sau perturbări la nivelul rețelelor și al sistemelor informatice, precum și la nivelul utilizatorilor unor astfel de sisteme și al altor persoane sau care poate avea un alt fel de impact negativ asupra acestora;

g) *serviciile publice de tip preventiv* — acele servicii oferite de Directoratul Național de Securitate Cibernetică care constau în:

1. anunțuri privind evenimente în domeniu;

2. anunțuri privind amenințări nou-identificate pe plan național și internațional;

3. cercetare și informare privind noutățile tehnologice în domeniu;

4. realizarea, la cerere, de auditări și evaluări de securitate sau teste de penetrare;

5. identificarea vulnerabilităților și punerea la dispoziție de situații actualizate privind încercările de intruziune și servicii de localizare a surselor atacurilor, pe baza informațiilor transmise de furnizorii de rețele și servicii de comunicații electronice;

6. diseminarea informațiilor de securitate cibernetică;

h) *serviciile publice de tip reactiv* — acele servicii oferite de Directoratul Național de Securitate Cibernetică care constau în:

1. alerte și atenționări privind apariția unor activități premergătoare atacurilor;

2. gestiunea incidentelor la nivel național, în cooperare cu celelalte echipe CSIRT;

3. diseminarea rezultatelor investigațiilor incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii Directoratului Național de Securitate Cibernetică;

i) *serviciile publice de consultanță pentru managementul securității cibernetice* — acele servicii oferite de Directoratul Național de Securitate Cibernetică care constau în:

1. analize de risc aplicate la nivel local și la nivel național privind infrastructurile cibernetice de interes național;

2. planificarea asigurării funcționării continue și a recuperării în caz de dezastre;

3. atestarea managementului securității cibernetice și a incidentelor cibernetice;

4. autorizarea echipelor de tip CSIRT și atestarea auditorilor de securitate informatică specifice domeniului securității rețelelor și sistemelor informatice;

j) *sistem de alertă timpurie și informare în timp real privind incidentele cibernetice* — ansamblul de proceduri și sisteme tehnice care au rolul de a identifica premisele de apariție a incidentelor cibernetice și de a avertiza în cazul producerii acestora. Sistemul include și conexiuni de date ce vor transporta informații referitoare la incidentele cibernetice identificate de senzori dedicați, precum și informații statistice referitoare la valorile de trafic înregistrate în nodurile de rețea ale infrastructurilor cibernetice ce asigură funcționalități de utilitate publică ori asigură servicii ale societății informaționale;

k) *criza cibernetică* — o stare de fapt care reprezintă o amenințare reală sau o deteriorare a unei infrastructuri cibernetice, de natură să creeze daune rețelelor și sistemelor informatice care furnizează servicii esențiale, digitale sau de interes național;

l) *produs de securitate cibernetică* — un element sau un grup de elemente care asigură securitatea unei rețele sau a unui sistem informatic;

m) *serviciu de securitate cibernetică* — un serviciu care asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea, nonrepudierea unei rețele sau a unui sistem informatic.

ARTICOLUL 3

Responsabilități și principii

(1) Principala responsabilitate a DNSC este asigurarea securității cibernetice a spațiului cibernetic național civil, în colaborare cu instituțiile și autoritățile competente.

(2) DNSC este autoritatea competentă la nivel național pentru spațiul cibernetic național civil, precum și pentru gestionarea riscurilor și a incidentelor de securitate cibernetică.

(3) În exercitarea calității de autoritate competentă la nivel național, DNSC se consultă și cooperează cu:

a) Serviciul Român de Informații — privind asigurarea securității cibernetice a spațiului cibernetic național civil a cărei afectare aduce atingere securității naționale;

b) Ministerul Apărării Naționale — privind asigurarea securității cibernetice a spațiului cibernetic național civil a cărei afectare aduce atingere apărării țării;

c) Ministerul Afacerilor Interne, Serviciul de Informații Externe, Serviciul de Telecomunicații Speciale și Serviciul de Protecție și Pază — privind asigurarea securității cibernetice a spațiului cibernetic național civil a cărei afectare aduce atingere domeniului acestora de activitate și responsabilitate;

d) Administrația Prezidențială — privind asigurarea securității spațiului cibernetic național civil a cărei afectare aduce atingere infrastructurilor cibernetice din domeniul de activitate și responsabilitate al acesteia sau celor destinate Consiliului Suprem de Apărare a Țării, denumit în continuare *CSAT*,

administrate potrivit cadrului legislativ specific și hotărârilor adoptate de acesta în condițiile legii.

(4) Pentru îndeplinirea responsabilităților sale, DNSC se consultă și cooperează, după caz, cu:

a) instituțiile publice prevăzute la alin. (3);

b) Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în cazul incidentelor care au ca rezultat încălcarea securității datelor cu caracter personal, în condițiile legii;

c) Autoritatea Națională pentru Administrare și Reglementare în Comunicații, atunci când incidentele au ca rezultat afectarea securității ori funcționării rețelelor publice de comunicații electronice ori când pentru administrarea unui incident sunt necesare măsuri ce intră în aria de activitate și responsabilitate a acesteia;

d) Oficiul Registrului National al Informațiilor Secrete de Stat, în cazul incidentelor și atacurilor cibernetice asupra sistemelor informatice și de comunicații care vehiculează informații clasificate;

e) Ministerul Afacerilor Externe, în cazul unor incidente și atacuri cibernetice care afectează interese pe plan extern ale României;

f) organele de urmărire penală, în condițiile legii.

(5) În vederea atingerii obiectivelor și funcțiilor, DNSC aplică următoarele principii:

a) principiul legalității — atât DNSC, cât și personalul instituției acționează cu respectarea prevederilor legale în vigoare și a tratatelor și convențiilor internaționale la care România este parte;

b) principiul egalității — beneficiarii activităților desfășurate de către DNSC vor fi tratați în mod egal, într-o manieră nediscriminatorie, corelativ cu obligația DNSC de autoritate națională, de a trata în mod egal pe toți beneficiarii, fără discriminare, pe criteriile prevăzute de legislația în domeniul de competență;

c) principiul transparenței — în procesul elaborării de propuneri de acte normative, DNSC va informa și va supune consultării și dezbaterii publice proiectele de acte normative și va permite accesul persoanelor juridice și fizice la datele și informațiile de interes public, în condițiile Legii nr. 544/2001 privind liberul acces la informațiile de interes public, cu modificările și completările ulterioare. În același timp, beneficiarii DNSC au dreptul de a obține informații de la instituție, iar instituția are obligația de a pune la dispoziția beneficiarilor informații, din oficiu sau la cerere, în limitele legii;

d) principiul proporționalității — activitatea DNSC trebuie să fie corespunzătoare cu legislația națională și să satisfacă interesul public, precum și echilibrată din punctul de vedere al efectelor asupra persoanelor fizice și juridice;

e) principiul imparțialității — personalul DNSC își exercită atribuțiile legale fără subiectivism, indiferent de propriile convingeri sau interese;

f) principiul continuității — activitatea DNSC se exercită fără întreruperi, cu respectarea prevederilor legale;

g) principiul neutralității tehnologice — în activitatea specifică de reglementare, testare și evaluare, DNSC nu favorizează o anumită marcă sau tehnologie și nu impune sau discriminează în favoarea utilizării unui anumit tip de tehnologie;

h) principiul solidarității internaționale — în relațiile cu partenerii din Uniunea Europeană și celelalte state sau organizații, DNSC promovează cooperarea între state în vederea rezolvării cât mai eficiente a provocărilor globale în domeniul securității cibernetice;

i) principiul sincronizării — măsurile și cerințele de securitate impuse de DNSC vor ține cont de evoluția fenomenului securității cibernetice la nivelul Uniunii Europene;

j) principiul satisfacerii interesului public — DNSC, precum și personalul instituției urmăresc satisfacerea interesului public înaintea celui individual sau de grup. Interesul public național este prioritar față de interesul public local;

k) principiul conștientizării — în activitatea sa de informare a persoanelor fizice și juridice, precum și a cetățenilor, DNSC prezintă noi cunoștințe și informații cu privire la vulnerabilitățile, riscurile și atacurile cibernetice, pe înțelesul tuturor, folosind diverse metode de atragere a interesului grupurilor-țintă.

(6) În îndeplinirea atribuțiilor sale, DNSC urmărește atingerea obiectivelor, luând în acest sens măsuri rezonabile, cu respectarea principiilor prevăzute la alin. (5).

(7) Responsabilitățile DNSC nu aduc atingere legislației în vigoare referitoare la sistemul național de apărare, ordine publică și securitate națională, la infrastructurile critice naționale și la informațiile clasificate.

ARTICOLUL 4

Obiective

Principalele obiective ale DNSC sunt:

a) asigurarea securității, confidențialității, integrității, disponibilității, rezilienței elementelor din spațiul cibernetic național civil, în cooperare cu instituțiile care au competențe și atribuții în domeniu;

b) asigurarea cadrului de strategii, politici și reglementări care să susțină implementarea viziunii naționale în domeniul securității cibernetice;

c) crearea cadrului național de cooperare între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni și abordări realiste, comune și coerente privitor la securitatea cibernetică a României;

d) crearea și operarea unei platforme naționale de colaborare care să permită schimbul de informații între constituenți, instituții ale statului, mediul academic și mediul privat în domeniul incidentelor, vulnerabilităților și crizelor de natură cibernetică;

e) crearea cadrului național de certificare în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu;

f) crearea cadrului național de instruire în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu;

g) promovarea și susținerea pe plan internațional a strategiei naționale în domeniul securității cibernetice;

h) crearea cadrului național destinat evaluării noilor tehnologii și impactului acestora asupra securității cibernetice a României;

i) dezvoltarea capacității de atragere de fonduri de finanțare pentru realizarea obiectivelor instituționale;

j) elaborarea și coordonarea planului de management al crizelor de securitate cibernetică la nivel național, în cooperare cu instituțiile care au competențe și atribuții în domeniul managementului crizelor, precum și prin colaborare cu ceilalți membri permanenți din COSC.

ARTICOLUL 5

Funcții și atribuții

În îndeplinirea obiectivelor, DNSC exercită următoarele funcții și atribuții:

a) Strategie și planificare

1. realizează politica Guvernului în domeniul securității cibernetice și stabilește la nivel național strategiile și politicile publice în domeniul securității cibernetice;

2. asigură elaborarea și diseminarea politicilor publice de prevenire și contracarare a incidentelor din cadrul infrastructurilor cibernetice din spațiul cibernetic civil național;

3. participă la elaborarea strategiei naționale de securitate cibernetică în cooperare cu instituțiile din Sistemul Național de Apărare, Ordine Publică și Securitate Națională, denumit în continuare *SNAOPSN*, cu competențe în domeniu, și coordonează implementarea acesteia, asigurând inclusiv monitorizarea acțiunilor întreprinse, a măsurilor implementate și evaluarea rezultatelor obținute;

4. elaborează și coordonează aplicarea planului de management al crizelor de securitate cibernetică la nivel național pe timp de pace, în cooperare cu instituțiile care au competențe și atribuții în domeniul managementului crizelor;

5. elaborează și coordonează implementarea strategiei naționale de instruire în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu;

6. elaborează și coordonează implementarea strategiei naționale de cooperare între instituții din domeniul public, privat, de educație și cercetare, pentru asigurarea unei viziuni și abordări realiste, comune și coerente privitor la securitatea cibernetică a României, inclusiv din perspectiva pregătirii și menținerii resursei umane în România;

7. elaborează propuneri privind modificarea cadrului legislativ în domeniul securității cibernetice, pe care le înaintează către Guvernul României;

8. asigură sprijin autorităților publice în elaborarea și implementarea strategiilor naționale sectoriale, care includ componente de securitate cibernetică;

9. sprijină participarea instituțiilor statului român și a altor părți interesate în proiecte naționale și internaționale din domeniul securității cibernetice, în vederea îndeplinirii obiectivelor strategiei naționale de securitate cibernetică;

b) Funcția de autoritate competentă la nivel național de reglementare, supraveghere și control — asigură reglementarea și gestionarea securității cibernetice a României și a spațiului cibernetic național civil, astfel:

1. monitorizează implementarea strategiei și politicilor naționale și sectoriale în domeniul securității cibernetice;

2. elaborează cadrul normativ și instituțional în domeniul securității cibernetice, inițiază și, respectiv, avizează proiecte de acte normative în domeniul său de competență, pe care le supune spre aprobare, în condițiile legii;

3. exercită atribuțiile stabilite prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare;

4. elaborează regulamente, norme, cerințe, ghiduri și recomandări, în domeniul de competență, care se aprobă prin decizia directorului DNSC și se publică, după caz, în Monitorul Oficial al României sau pe site-ul instituției;

5. îndeplinește atribuțiile de autoritate națională pentru furnizorii de servicii de găzduire/hosting, de servicii tip cloud, de servicii de identificare electronică, de servicii de încredere pentru tranzacțiile electronice și furnizorii de rețele de distribuție de conținut;

6. stabilește standardele și reglementările în domeniul securității cibernetice la nivel național, cu excepția domeniilor prevăzute la art. 20 alin. (1), care devin obligatorii odată cu publicarea în Monitorul Oficial al României, Partea I, și verifică implementarea acestora prin acțiuni de control;

7. gestionează și administrează evidențe privind persoanele fizice și juridice care intră sub incidența actelor normative care reglementează domeniul securității cibernetice, conform atribuțiilor instituției;

c) Funcția de CSIRT național

1. asigură coordonarea activităților la nivel național de detecție, protecție și răspuns la atacuri cibernetice, precum și desfășurarea de activități de supraveghere, monitorizare, identificare, analiză, investigare și de răspuns la incidente de securitate cibernetică, prin echipa CSIRT națională, pentru infrastructurile cibernetice aflate în domeniul de competență, așa cum vor fi definite prin regulamentul de organizare și funcționare al DNSC;

2. exercită și atribuțiile de CSIRT național stabilite prin Legea nr. 362/2018, cu modificările și completările ulterioare;

3. coordonează răspunsul la incidente de securitate cibernetice la nivel național pentru domeniul său de competență;

4. monitorizează, identifică, analizează și răspunde la amenințările de securitate cibernetică din spațiul cibernetic național civil;

5. derulează activități de investigare a incidentelor cibernetice care vizează sau utilizează spațiul cibernetic național civil, în conformitate cu competențele legale, utilizând, după caz, metode tehnice care presupun inclusiv analiza metadatelor corespunzătoare conexiunilor de rețea puse la dispoziția DNSC de către posesorii acestora;

6. evaluează riscurile de securitate cibernetică la nivel național și emite avertizări, buletine de informare și de prognoză;

7. derulează activități de identificare și analiză a amenințărilor, inclusiv în cooperare cu mediul public, privat și academic, în scopul implementării unui nivel ridicat de securitate cibernetică;

8. derulează activități tehnice specifice de identificare a vulnerabilităților site-urilor cu conținut în limba română și emite avertizări de securitate;

9. dezvoltă sisteme și instrumente de identificare, analiză și prognoză privind incidentele cibernetice, în baza cărora stabilește impactul la nivel național și transfrontalier al incidentelor și informează autoritățile relevante la nivel național, precum și autoritățile similare din alte state potențial afectate. În acest sens, DNSC cooperează cu instituțiile din sistemul național de apărare, ordine publică și securitate națională, precum și cu mediul privat și mediul academic;

10. asigură colectarea, în condițiile legii, analiza și schimbul de informații privind riscurile și vulnerabilitățile de securitate ale rețelelor și sistemelor informatice, precum și ale produselor și serviciilor de securitate cibernetică;

11. oferă servicii publice de tip preventiv, de tip reactiv și de consultanță pentru managementul securității cibernetice;

12. implementează, gestionează și coordonează Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică, denumită în continuare *PNRISC*;

d) Funcția de CSIRT guvernamental

1. monitorizează implementarea măsurilor de securitate cibernetică la nivelul instituțiilor Guvernului României, în colaborare și coordonare cu instituțiile statului care au competențe și atribuții în domeniu;

2. sprijină instituțiile statului care au competențe și atribuții în domeniu în exercitarea atribuțiilor legate de securitatea cibernetică;

e) Funcția de coordonare, implementare, îndrumare și sprijin a CSIRT-urilor sectoriale

1. asigură sau participă la asigurarea funcției de CSIRT sectorial pentru toate sectoarele specificate de Legea nr. 362/2018, cu modificările și completările ulterioare, în colaborare și coordonare cu instituțiile statului care au competențe și atribuții în domeniu și cu autoritățile de reglementare din sectoarele implicate;

2. în cooperare cu instituțiile sau organizațiile care coordonează și/sau reglementează domenii de activitate ce pot fi afectate de incidente de securitate cibernetică, dezvoltă echipe CSIRT sectoriale sau participă la completarea capabilităților echipelor constituite la nivel sectorial, subsectorial ori al instituțiilor sau organizațiilor;

f) Funcția de echipă de răspuns la incidente de securitate cibernetică pentru produse și servicii informatice utilizate în cadrul sectorului guvernamental

1. asigură identificarea, evaluarea și gestionarea riscurilor asociate vulnerabilităților de securitate cibernetică din produsele, soluțiile, componentele și/sau serviciile informatice ale sectorului guvernamental;

2. asigură infrastructura și procesele necesare pentru primirea, investigarea și raportarea, publică sau către instituțiile statului care au competențe și atribuții în domeniu, a informațiilor privind vulnerabilitățile de securitate cibernetică ale produselor, soluțiilor, componentelor și/sau serviciilor informatice ale sectorului guvernamental;

g) Funcția de alertare, prevenire, conștientizare și instruire

1. asigură informarea și pregătirea la nivel național a populației, precum și a tuturor entităților care fac parte din spațiul cibernetic civil național, inclusiv a operatorilor economici din sectoarele stabilite în baza Legii nr. 362/2018, cu modificările și completările ulterioare, și din sectorul public cu privire la riscurile de securitate din spațiul cibernetic civil;

2. promovează dezvoltarea unui comportament adecvat în spațiul cibernetic național civil pentru persoanele fizice și juridice prin conștientizarea efectelor consecințelor atacurilor cibernetice și a modalității de semnalare a acestora;

3. emite informări privind obligațiile care derivă din calitatea de administrator, furnizor sau utilizator al rețelelor și sistemelor informatice, privind răspunsul în fața unor posibile atacuri cibernetice, privind conștientizarea cetățenilor și instituțiilor publice și private despre necesitatea semnalării sau notificării atacurilor cibernetice;

4. dezvoltă cadrul național de conștientizare a populației în cooperare cu mediul public, privat și academic în scopul asigurării unei abordări eficiente a pregătirii populației privind modalitățile de comportament, reacție și reziliență cibernetică în mediul online;

5. desfășoară și participă la campanii și acțiuni de prevenire și conștientizare a cauzelor și consecințelor atacurilor cibernetice asupra rețelelor și sistemelor informatice civile, la nivel internațional, național și regional;

h) Funcția de cooperare și colaborare

1. asigură cadrul de cooperare în vederea derulării de activități specifice asigurării securității cibernetice, cercetării, schimbului de informații, instruirii, educației, conștientizării, elaborării de proiecte, precum și a oricăror altor activități necesare pentru asigurarea securității cibernetice a României, conform competențelor legale;

2. asigură reprezentarea României în formatele de cooperare internațională pe domeniile de competență, în cooperare cu alte autorități competente ale statului, în interesul asigurării cooperării interinstituționale, informării reciproce și susținerii unei poziții unitare la nivel internațional;

3. sprijină efortul național, instituțiile și autoritățile competente ale statului, precum și inițiativele de cooperare în cadrul organizațiilor internaționale din care România face parte — în special în cadrul Uniunii Europene (UE), al Organizației Națiunilor Unite (ONU), al Organizației pentru Securitate și Cooperare în Europa (OSCE) și al Organizației Tratatului Atlanticului de Nord (NATO);

4. în colaborare cu alte autorități competente, universități, centre de cercetare și operatori economici, participă la dezvoltarea de soluții tehnologice de securitate cibernetică de interes, care pot avea o dublă utilizare civilă și militară;

5. înființează, coordonează și gestionează Platforma Națională de Cooperare în Domeniul Securității Cibernetice, denumită în continuare *PNCDSC*, între instituțiile de stat, mediul privat, mediul academic și organizații nonguvernamentale, în scopul asigurării unui cadru național unitar de expertiză, cercetare, informare și orice alte acțiuni conexe domeniului de competență;

6. participă în grupuri de cooperare, de lucru sau de specialitate și în rețele de cooperare, forumuri și organizații din domeniul securității cibernetice constituite la nivel național, european și internațional;

7. dezvoltă relații de parteneriat cu alte structuri naționale sau internaționale cu competențe și responsabilități în domeniul securității cibernetice, în acest sens încheind memorandumuri și protocoale de cooperare cu persoane de drept public sau privat, naționale sau străine;

8. cooperează cu instituțiile din SNAOPSN, precum și din COSC în vederea asigurării securității cibernetice la nivelul României;

9. cooperează cu Ministerul Cercetării, Inovării și Digitalizării, precum și cu Centrul de competențe european industrial, tehnologic și de cercetare în materie de securitate cibernetică pe domeniile de competență;

10. sprijină participarea instituțiilor statului român și a altor părți interesate în proiecte naționale și internaționale din domeniul securității cibernetice;

i) Funcția de autoritate națională de certificare privind securitatea cibernetică — are calitatea de organism național și asigură mecanismele naționale privind evaluarea, certificarea și acreditarea produselor, serviciilor și proceselor în domeniul securității cibernetice.

1. DNSC este autoritate națională de certificare în domeniul securității cibernetice pentru spațiul cibernetic civil. În această calitate, certifică din punctul de vedere al securității cibernetice tehnologii, produse și servicii;

2. stabilește norme, cerințe tehnice, standarde și proceduri pentru implementarea Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică);

3. înființează și gestionează Registrul Național al Activelor, Produselor și Serviciilor de Securitate Cibernetică, denumit în continuare *RNAPSSC*;

4. autorizează laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice;

5. cooperează cu instituțiile naționale și internaționale în domeniul standardizării și acreditarii produselor, serviciilor și proceselor în domeniul securității cibernetice;

j) Funcția de asigurare a conformității și abordării unitare a securității cibernetice în cadrul infrastructurilor cibernetice

1. avizează din punct de vedere al securității cibernetice proiectele finanțate din fonduri publice sau pentru care s-au solicitat garanții guvernamentale care implică rețele și sisteme informatice care intră sub incidența Legii nr. 362/2018. Avizarea se realizează prin raportare la cerințele și normele tehnice din domeniul securității cibernetice adoptate la nivel național și internațional;

2. verifică și validează conformitatea implementării măsurilor de securitate cibernetică în proiectele de la pct. 1;

k) Funcția de reprezentare — asigură, în numele României, reprezentarea în organismele și organizațiile naționale, regionale, europene și internaționale, ca autoritate națională pentru domeniul său de activitate, în conformitate cu cadrul normativ în vigoare.

l) Funcția de cercetare-dezvoltare

1. consolidează, sprijină și promovează potențialul național de cercetare, dezvoltare și inovare al activităților, proceselor și tehnologiilor de vârf de securitate cibernetică, pe baza

capacităților individuale și colective ale sectorului public și privat, ale mediului academic și ale industriei;

2. desfășoară și participă la activități de cercetare-dezvoltare în domeniul securității cibernetice și elaborează proceduri și recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea științifică și dezvoltarea tehnologică;

3. elaborează studii și cercetări privind problematica securității cibernetice a produselor, serviciilor și infrastructurilor cibernetice;

4. elaborează și actualizează cadrul metodologic, procedural și de bune practici cu privire la activitatea de cercetare științifică în domeniul securității cibernetice, prin consultare cu instituțiile care au atribuții și competențe în domeniu;

5. planifică și desfășoară activități de cercetare științifică în domeniile de competență, cooperând la nivel central și teritorial cu instituții din mediul public, privat și academic, precum și cu persoane fizice;

6. dezvoltă relații pe linie de cercetare științifică cu universități, institute de cercetare, edituri, biblioteci și specialiști în domeniu din țară și din străinătate;

7. promovează inițiativa științifică, dezvoltarea și inovarea în domenii specifice securității cibernetice, cu scopul de a sprijini și proteja interesele naționale în acest domeniu;

m) Funcția de analiză și prognoză — evaluează și analizează evoluțiile din domeniul securității cibernetice și emite avertizări, analize, buletine de informare și de prognoză.

n) Funcția de identificare, evaluare, monitorizare și atenuare a riscurilor cibernetice la nivel național

o) Funcția de centru național de gestionare a crizelor de natură cibernetică pe timp de pace

1. la nivelul DNSC se constituie Centrul Național de Gestionare a Crizelor de Securitate Cibernetică, denumit în continuare *CNGCSC*, din care fac parte reprezentanți din cadrul instituțiilor și autorităților competente, cu responsabilități în domeniul securității cibernetice;

2. împreună cu instituțiile din SNAOPSN, CNGCSC, asigură procesarea și analiza datelor și informațiilor referitoare la atacurile cibernetice care vizează spațiul național cu potențial impact major în sfera rețelelor și sistemelor informatice, prin produse analitice, destinate fundamentării deciziei de nivel strategic sau care să constituie suportul operațional pentru managementul crizelor cibernetice;

3. prin colaborare cu ceilalți membri permanenți din COSC, CNGCSC, asigură managementul crizelor cibernetice cauzate de atacuri cibernetice, în colaborare cu instituțiile statului care au competențe și atribuții în domeniul de gestionare a crizelor care afectează buna funcționare a statului;

p) Funcția de evaluare a securității cibernetice a noilor tehnologii

1. evaluează din punctul de vedere al securității cibernetice sisteme de control industrial, sisteme informatice și rețele complexe, produse și servicii, precum și noile tehnologii;

2. evaluează riscurile identificate, precum și impactul acestora asupra securității cibernetice a României;

q) Funcția de evaluare și certificare

1. evaluează, testează și certifică produse și servicii de securitate cibernetică, pentru nevoi proprii sau la solicitarea instituțiilor din SNAOPSN și/sau a Guvernului;

2. stabilește reguli, prescripții sau caracteristici pentru activități sau pentru rezultatele acestora din domeniul securității cibernetice, pentru asigurarea unei abordări unitare la nivel național în scopul realizării unui nivel ridicat al securității cibernetice;

3. în colaborare cu organismele specializate, participă la elaborarea, aprobarea și adoptarea de standarde în domeniul de competență, pe care le pune la dispoziția publicului;

4. participă la lucrările comitetelor tehnice naționale și internaționale pentru punerea în aplicare a standardelor și specificațiilor tehnice acceptate la nivel internațional, aplicabile securității rețelelor și a sistemelor informatice, fără a impune sau discrimina în favoarea utilizării unui anumit tip de tehnologie;

r) Funcția de educație și pregătire în domeniul securității cibernetice

1. dezvoltă parteneriate cu ministere de resort, cu școli, licee, colegii și universități, cu mediul privat, precum și cu parteneri internaționali, în scopul creării cadrului național de educație și pregătire în domeniul securității cibernetice care să ofere resursa umană necesară statului român pentru asigurarea securității cibernetice;

2. promovează școlarizarea, educarea și formarea profesională a elevilor și studenților cu privire la securitatea cibernetică în vederea asigurării implementării și utilizării noilor tehnologii în viața de zi cu zi;

3. desfășoară acțiuni, exerciții și colocvii de pregătire și instruire;

4. inițiază și coordonează, în colaborare cu reprezentanți ai mediului public, privat și academic, înființarea și dezvoltarea de centre de excelență în domeniul securității cibernetice, centrale și regionale, având ca scop pregătirea resursei umane calificate pentru nevoile naționale, desfășurarea de activități de cercetare-dezvoltare în domeniul securității cibernetice, precum și orice alte activități necesare asigurării unui nivel ridicat de securitate cibernetică în România. Aceste activități pot include, fără a se limita la, pregătirea resursei umane din alte state;

5. certifică, la cerere, centre de excelență, programe de școlarizare, educare și formare profesională în domeniul securității cibernetice;

s) Funcția de management al proiectelor și serviciilor pentru activități se realizează fără a aduce atingere activităților prevăzute la lit. b) și lit. q), după cum urmează:

1. întocmește, conduce, execută și participă la identificarea, coordonarea și implementarea de proiecte de interes comun, cu finanțare internă sau externă, atât pe cont propriu, cât și în parteneriat, și facilitează accesul instituțiilor, operatorilor economici și persoanelor abilitate la aceste proiecte;

2. pe durata derulării activităților specifice proiectelor prevăzute la pct. 1, poate crea sau participa în structuri fără personalitate juridică, departamente, secții, laboratoare ori alte structuri legale sau organizatorice necesare realizării obiectivelor, funcțiilor și atribuțiilor sale, cu respectarea prevederilor legale în vigoare.

ARTICOLUL 6

Conducere

(1) Conducerea DNSC este asigurată de directorul DNSC și cinci adjuncți ai directorului DNSC, care au rang de secretar de stat, respectiv subsecretari de stat.

(2) Directorul DNSC și cei cinci adjuncți ai directorului DNSC sunt numiți și eliberați din funcție prin decizie a prim-ministrului, cu avizul CSAT.

(3) Directorului DNSC și celor cinci adjuncți ai directorului DNSC le sunt aplicabile regimul incompatibilităților și al conflictului de interese aplicabil funcțiilor de secretar de stat și subsecretar de stat, astfel cum este prevăzut de cartea I titlul IV din Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu modificările și completările ulterioare.

(4) Durata mandatului directorului DNSC este de 5 ani, cu posibilitatea prelungirii o singură dată, nu mai mult de 5 ani.

(5) Mandatul directorului DNSC încetează în următoarele situații:

a) în situația imposibilității de a-și îndeplini mandatul mai mult de 120 de zile calendaristice consecutive dintr-un interval de 140 de zile;

b) în caz de condamnare penală prin hotărâre judecătorească definitivă, pentru care nu a intervenit reabilitarea;

c) în situația retragerii avizului CSAT;

d) prin demisie;

e) prin deces;

f) la expirarea perioadei mandatului.

(6) Dacă funcția de director DNSC devine vacantă, în condițiile alin. (5) lit. a)—e) se procedează la numirea unei noi persoane pentru această funcție pentru durata rămasă din mandat, în condițiile prevederilor alin. (3).

(7) În caz de vacanță a funcției de director DNSC, până la desemnarea și numirea, în condițiile legii, a unui nou director, pentru durata rămasă din mandat, interimatul va fi asigurat de unul din adjuncții directorului DNSC.

ARTICOLUL 7

Reprezentare

(1) Directorul DNSC reprezintă instituția în raporturile cu alte autorități și instituții publice, organizații nonguvernamentale, precum și cu orice persoane juridice și fizice din țară și din străinătate.

(2) Directorul DNSC este ordonator terțiar de credite în condițiile legii.

(3) În exercitarea atribuțiilor sale, directorul DNSC emite decizii și ordine.

(4) Deciziile și ordinele cu caracter normativ se publică în Monitorul Oficial al României, Partea I.

(5) Deciziile și ordinele emise în exercitarea atribuțiilor prevăzute de lege, inclusiv cele adoptate în conformitate cu prevederile Legii nr. 362/2018, pot fi atacate în contencios administrativ, în condițiile legii.

(6) DNSC transmite Comisiei Europene informații cu privire la implementarea normativelor europene ce intră în domeniile de competență ale instituției, conform termenelor stabilite sau la solicitarea expresă a Comisiei Europene.

ARTICOLUL 8

Atribuții ale conducerii DNSC

(1) Directorul DNSC are următoarele atribuții principale:

a) supune spre aprobare prim-ministrului, cu avizul CSAT, strategia de dezvoltare instituțională a DNSC, programe de activitate și cooperare și planul anual de activitate ale DNSC;

b) aprobă planurile de investiții ale DNSC;

c) convoacă și prezidează reuniunile Comitetului director al DNSC;

d) stabilește amplasarea sediilor structurilor regionale și județene ale DNSC, structuri fără personalitate juridică;

e) stabilește, prin decizie internă, atribuțiile specifice fiecărui compartiment funcțional din cadrul DNSC;

f) aprobă regulamentul intern al DNSC;

g) aprobă, în condițiile legii, încadrarea, promovarea, precum și modificarea sau încetarea raporturilor de muncă ale personalului DNSC;

h) prezintă anual în CSAT raportul de activitate al DNSC;

i) supune spre aprobare CSAT actele de organizare ale DNSC, respectiv statul de funcții, structura organizatorică și regulamentul de organizare și funcționare, precum și orice modificare a acestora.

(2) Directorul DNSC poate delega adjuncților săi atribuțiile prevăzute la alin. (1).

(3) În lipsa directorului DNSC, atribuțiile sale se exercită de către adjunctul directorului DNSC desemnat prin decizie a directorului DNSC.

(4) Dacă atât directorul DNSC, cât și adjuncții directorului DNSC sunt absenți sau în imposibilitate temporară de a-și exercita prerogativele, reprezentarea DNSC se asigură de către o persoană cu funcție de conducere desemnată prin decizie a directorului DNSC.

ARTICOLUL 9

Comitetul director

(1) În activitatea sa, conducerea DNSC este sprijinită de Comitetul director al DNSC, ce funcționează în baza unui statut elaborat de către DNSC, aprobat de prim-ministru, cu avizul CSAT.

(2) Comitetul director este format din câte un reprezentant al:

a) Administrației Prezidențiale;

b) prim-ministrului;

c) Ministerului Afacerilor Interne;

d) Ministerului Apărării Naționale;

e) Ministerului Afacerilor Externe;

f) Ministerului Finanțelor;

g) Ministerului Muncii și Protecției Sociale;

h) Ministerului Cercetării, Inovării și Digitalizării;

i) Ministerului Educației;

j) Serviciului Român de Informații;

k) Serviciului de Informații Externe;

l) Serviciului de Telecomunicații Speciale;

m) Serviciului de Protecție și Pază;

n) Autorității Naționale pentru Administrare și Reglementare în Comunicații;

o) Oficiului Registrului Național al Informațiilor Secrete de Stat.

(3) Membrii Comitetului director sunt desemnați de către conducerea instituțiilor menționate la alin. (2).

(4) Directorul DNSC și adjuncții directorului DNSC sunt membri de drept ai Comitetului director.

(5) Comitetul director are următoarele atribuții și competențe:

a) avizează strategiile de dezvoltare ale DNSC și propunerile de politici publice elaborate de DNSC, destinate prevenirii și contracarării incidentelor din cadrul infrastructurilor cibernetice;

b) avizează proiectul bugetului anual, planul anual de activitate și raportul anual de activitate ale DNSC;

c) urmărește desfășurarea în condiții de eficiență economică și performanță profesională a activității DNSC;

d) formulează recomandări privind obiectivele din planul anual de activitate al DNSC;

e) formulează recomandări privind punctele de vedere naționale ce trebuie susținute de reprezentanții DNSC în formatele de cooperare internaționale;

f) analizează activitatea DNSC pe baza rapoartelor de activitate prezentate de către directorul DNSC;

g) avizează actele de organizare ale DNSC, precum și orice modificare a acestora, respectiv statul de funcții, structura organizatorică și regulamentul de organizare și funcționare;

h) sprijină conducerea DNSC în îndeplinirea obiectivelor instituționale asumate prin prezentul act normativ și prin regulamentul de organizare și funcționare.

(6) Comitetul director își desfășoară activitatea în cadrul unor întâlniri trimestriale, în ședințe ordinare, sau ori de câte ori este nevoie, în ședințe extraordinare.

(7) În exercitarea atribuțiilor sale, Comitetul director emite avize și recomandări, precum și decizii de numire și revocare a membrilor Comitetului de reglementare, care se adoptă cu votul majorității simple a membrilor prezenți la ședință.

(8) Secretariatul Comitetului director este asigurat de către DNSC.

ARTICOLUL 10

Comitetul de reglementare

(1) Se înființează Comitetul de reglementare cu rol de garant al obiectivității, transparenței, neutralității, echidistanței, nediscriminării și legalității activităților de reglementare desfășurate de DNSC, acordând, în acest scop, sprijin de specialitate, prin îndrumări și recomandări, în ceea ce privește asigurarea respectării principiilor obiectivității, transparenței, neutralității, echidistanței, nediscriminării și legalității în activitatea de reglementare a DNSC.

(2) Comitetul de reglementare are un rol consultativ și are următoarea componență:

a) trei membri din cadrul DNSC, desemnați prin decizie a directorului DNSC;

b) câte un membru din instituțiile prevăzute la art. 9 alin. (2).

(3) Numirea și revocarea membrilor Comitetului de reglementare se fac de către Comitetul director la propunerea instituțiilor menționate la alin. (2).

(4) Unul dintre membrii DNSC desemnați conform alin. (2) lit. a) convoacă și prezidează reuniunile Comitetului de reglementare.

(5) Membrii Comitetului de reglementare trebuie să îndeplinească următoarele condiții:

a) să fie cetățeni români, cu domiciliul stabil în România, cu o bună reputație etică și profesională, atestată de către instituțiile care au făcut nominalizarea, printr-o scrisoare de recomandare;

b) să fie absolvenți de studii superioare și cu pregătire profesională în domeniul tehnic, economic sau juridic, având o vechime în muncă de minimum 10 ani;

c) să aibă o experiență de minimum 5 ani în funcții de conducere în domeniul securității cibernetice, rețelelor și sistemelor informatice sau din SNAOPSN.

(6) Durata mandatului membrilor Comitetului de reglementare este de 3 ani.

(7) În cazul imposibilității definitive de exercitare a mandatului de către unul dintre membri, instituțiile menționate la alin. (2) desemnează o nouă persoană în condițiile alin. (3) și (5) pentru perioada rămasă din mandat.

(8) Se consideră imposibilitate definitivă de exercitare a mandatului orice împrejurare care creează o indisponibilizare cu o durată mai mare de 90 de zile consecutive.

(9) Activitatea Comitetului de reglementare se desfășoară în baza statutului Comitetului de reglementare, elaborat de către DNSC cu avizul CSAT.

(10) Secretariatul Comitetului de reglementare este asigurat de DNSC prin compartimentul funcțional care gestionează activitatea de reglementare.

ARTICOLUL 11

Finanțare

(1) Finanțarea cheltuielilor curente și de capital ale DNSC se asigură integral din bugetul de stat, prin bugetul Secretariatului General al Guvernului.

(2) DNSC stabilește și încasează:

a) cuantumul tarifelor pentru servicii din activitățile prevăzute la art. 22 alin. (1) lit. l), art. 32 alin. (2) lit. c) și e) și la art. 33 alin. (2) lit. c) și e) din Legea nr. 362/2018, cu modificările și completările ulterioare, stabilite prin decizie a directorului DNSC care se publică în Monitorul Oficial al României, Partea I;

b) cuantumul tarifelor pentru înscrierea în Registrul național al activelor, produselor și serviciilor de securitate cibernetică;

c) cuantumul tarifelor pentru autorizarea laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice;

d) cuantumul tarifelor pentru avizarea, verificarea și validarea conformității privind securitatea cibernetică;

e) cuantumul tarifelor pentru certificarea securității cibernetice a soluțiilor, produselor și serviciilor de tehnologia informației și comunicațiilor, inclusiv a noilor tehnologii;

f) venituri din servicii de specialitate;

g) venituri din furnizare de produse și componente din domeniul securității cibernetice sau conexe acestuia;

h) venituri din drepturi de proprietate intelectuală și licențe;

i) venituri din comisioane pentru parteneriate și proiecte;

j) alte venituri, a căror natură este aprobată prin hotărâre a Guvernului.

(3) Resursele prevăzute la alin. (2) se fac venit la bugetul de stat. Sumele încasate potrivit alin. (2) se virează în conturile corespunzătoare de venituri bugetare, în termen de cel mult două zile lucrătoare de la încasare.

ARTICOLUL 12

Analiza activității DNSC

(1) Activitatea DNSC este analizată de CSAT pe baza raportului anual, care se prezintă pentru anul anterior, precum și a rapoartelor specifice întocmite la solicitarea CSAT.

(2) Raportul anual de activitate se depune la CSAT, până la data de 31 martie, după avizare de către Comitetul director.

(3) DNSC elaborează rapoarte, analize și informări cu privire la securitatea cibernetică a spațiului cibernetic național, a infrastructurilor cibernetice de interes național, a rețelelor și sistemelor informatice din domeniile de competență pe care le prezintă prim-ministrului, președintelui, CSAT, COSC și instituțiilor cu atribuții în SNAOPSN, precum și Comitetului director.

ARTICOLUL 13

Personalul instituției

(1) Personalul DNSC este format din personal contractual propriu și personal detașat din SNAOPSN, încadrat pe funcții conform statului de funcții al DNSC.

(2) Statul de funcții, structura organizatorică și regulamentul de organizare și funcționare al DNSC, precum și orice modificare a acestora se aprobă de către CSAT. Statul de funcții cuprinde și funcțiile prevăzute a se încadra cu personal provenit inclusiv din SNAOPSN.

(3) Numărul maxim de posturi este de 1.250, care include structurile centrale, regionale și județene, exclusiv demnitarii și posturile aferente cabinetelor demnitarilor.

(4) Pe lângă funcțiile prevăzute de Legea-cadru nr. 153/2017 privind salarizarea personalului plătit din fonduri publice, cu modificările și completările ulterioare, statul de funcții al DNSC conține și funcții specifice de conducere și de execuție după cum urmează:

a) funcții de conducere: manager superior securitate cibernetică, manager securitate cibernetică, coordonator superior securitate cibernetică, coordonator securitate cibernetică;

b) funcții de execuție (studii superioare): expert securitate cibernetică, expert preluare, analiză primară și răspuns la incidente securitate cibernetică, expert investigații digitale și analiză malware, expert dezvoltare, implementare și administrare infrastructuri securitate cibernetică, expert analiză surse deschise, riscuri și amenințări securitate cibernetică, expert accesare fonduri, implementare și administrare proiecte securitate cibernetică, expert legal politici, standardizare de securitate cibernetică, expert evaluare și impact financiar securitate cibernetică, expert politici, strategii și cooperare securitate cibernetică, expert dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică;

c) funcții de execuție (studii medii): asistent securitate cibernetică, asistent preluare, analiză primară și răspuns la incidente securitate cibernetică, asistent investigații digitale și analiză malware, asistent dezvoltare, implementare și administrare infrastructuri securitate cibernetică, asistent analiză surse deschise, riscuri și amenințări securitate cibernetică, asistent accesare fonduri, implementare și administrare proiecte securitate cibernetică, asistent legal politici, standardizare de securitate cibernetică, asistent evaluare și impact financiar securitate cibernetică, asistent politici, strategii și cooperare securitate cibernetică, asistent dezvoltare competențe, aptitudini și cunoștințe specifice de securitate cibernetică.

ARTICOLUL 14

Încadrarea și promovarea personalului

Personalul DNSC este angajat pe bază de concurs sau examen organizat în condițiile legii, în conformitate cu structura organizatorică, iar salarizarea funcțiilor specifice de conducere și de execuție din cadrul DNSC se stabilește potrivit art. 28 din Legea-cadru nr. 153/2017, cu modificările și completările ulterioare, prin asimilare cu funcțiile și salariile de bază prevăzute în anexele la Legea-cadru și aplicabile categoriei de personal respective, cu avizul Ministerului Muncii și Protecției Sociale și al Ministerului Finanțelor, în termen de 45 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență.

ARTICOLUL 15

Patrimoniu

(1) La data intrării în vigoare a prezentei ordonanțe de urgență DNSC preia patrimoniul, arhiva și creditele bugetare angajate, inclusiv pe întreg anul în curs, în limita creditelor de angajament și în scopurile pentru care au fost aprobate Centrului Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO, care se desființează.

(2) DNSC se subrogă în toate drepturile și obligațiile CERT-RO, inclusiv în litigiile aflate pe rolul instanțelor judecătorești, și dobândește calitatea procesuală a acestuia.

(3) Predarea-preluarea patrimoniului se efectuează în baza situațiilor financiare întocmite potrivit prevederilor art. 28 alin. (11) din Legea contabilității nr. 82/1991, republicată, cu modificările și completările ulterioare, și a protocolului de predare-preluare întocmit în termen de 30 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență. Protocolul de predare-preluare cuprinde și creditele bugetare, creditele de angajament și execuția bugetară pe anul în curs.

ARTICOLUL 16

Cooperare

(1) DNSC cooperează cu organizații și organisme internaționale pe domeniile sale de competență.

(2) DNSC reprezintă România la nivelul instituțiilor Uniunii Europene și la nivelul altor foruri internaționale pentru domeniile de competență.

(3) Pentru asigurarea unei capacități adecvate de identificare, evaluare și adoptare a unor măsuri de management al riscului și/sau de răspuns la incidente și atacuri cibernetice, DNSC dezvoltă schimburi de informații și transfer de expertiză cu instituțiile și autoritățile cu responsabilități în domeniu, promovează și susține cooperarea între sectorul public și cel privat, precum și cooperarea cu mediile neguvernamentale și comunitatea academică.

(4) DNSC poate face parte ca membru cotizant în organizații și organisme naționale și internaționale, pe domeniile sale de competență.

ARTICOLUL 17

Atribuții în situații de criză cibernetică pe timp de pace

(1) Atribuțiile specifice, modul de organizare și funcționare a CNGCSC se stabilesc prin Regulamentul de organizare și funcționare a CNGCSC, care se elaborează de către DNSC în termen de 180 de zile de la intrarea în vigoare a prezentei ordonanțe de urgență și se aprobă de către directorul DNSC, după consultarea celorlalți membri permanenți din COSC.

(2) Conducerea DNSC va dispune măsurile necesare pentru asigurarea capacității operaționale a instituției, inclusiv a CNGCSC pentru gestionarea de criză cibernetică pe timp de pace.

ARTICOLUL 18

Autorizarea laboratoarelor civile

(1) În implementarea Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică), produsele și serviciile de securitate cibernetică utilizate în cadrul rețelelor și sistemelor informatice sunt testate, evaluate și certificate de operatori economici care au calitatea de laboratoare civile autorizate. Funcționarea laboratoarelor civile autorizate ce efectuează activități de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice este condiționată de obținerea prealabilă a unei autorizații din partea DNSC.

(2) Acordarea, prelungirea, suspendarea sau retragerea autorizației prevăzute la alin. (1) se efectuează în baza regulamentului de autorizare și verificare a laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice, elaborat de DNSC și aprobat prin hotărâre a Guvernului. Valabilitatea autorizației este de maximum 3 ani.

(3) Cererea pentru obținerea autorizației de funcționare a laboratoarelor civile prevăzute la alin. (1) însoțită de documentația stabilită prin regulamentul prevăzut la alin. (2) se transmite către DNSC în format fizic sau prin mijloace electronice.

(4) În termen de 10 zile de la primirea cererii solicitantului, DNSC îl informează pe acesta dacă documentația este completă sau solicită informații suplimentare relevante.

(5) În termen de maximum 60 de zile de la data primirii tuturor informațiilor solicitate, DNSC eliberează autorizația de

funcționare a laboratorului de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice sau informează solicitantul asupra deciziei sale negative.

(6) DNSC justifică în mod corespunzător orice decizie prin care refuză autorizația de funcționare a laboratorului de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.

(7) Laboratoarele civile prevăzute la alin. (1) se supun controlului desfășurat de către DNSC în vederea stabilirii gradului de respectare a obligațiilor ce le revin în temeiul prezentei ordonanțe de urgență.

ARTICOLUL 19

Activitatea de verificare a laboratoarelor civile

(1) DNSC exercită controlul activității desfășurate de către laboratoarele civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.

(2) DNSC verifică îndeplinirea obligațiilor de către laboratoarele civile în baza regulamentului de autorizare și verificare prevăzut la art. 18 alin. (2).

(3) Următoarele fapte constituie contravenții dacă nu au fost săvârșite în astfel de condiții încât să fie considerate infracțiuni potrivit legii:

a) utilizarea titulaturii de laborator civil autorizat, fără o autorizație acordată de către DNSC, în temeiul art. 18 alin. (1);

b) furnizarea de rapoarte sau certificate de testare, evaluare sau certificare de către laboratoare civile neautorizate sau fără autorizație valabilă în temeiul art. 18 alin. (1);

c) refuzul laboratorului civil de a se supune controlului declanșat de DNSC în temeiul art. 18 alin. (7).

(4) Prin derogare de la dispozițiile art. 8 alin. (2) lit. a) din Ordonanța Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, contravențiile prevăzute la alin. (3) se sancționează astfel:

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

b) pentru operatorii economici cu o cifră de afaceri netă de peste 1.000.000 lei, cu amendă în cuantum de până la 5% din cifra de afaceri netă, iar, în cazul săvârșirii unei noi contravenții, în termen de 6 luni, de la data săvârșirii primei contravenții, limita maximă a amenzii este de 10% din cifra de afaceri netă.

(5) Cifra de afaceri netă prevăzută la alin. (4) lit. b) este cea înregistrată de operatorul economic în ultimul exercițiu financiar.

(6) În vederea individualizării sancțiunii prevăzute la alin. (4), DNSC va lua în considerare gradul de pericol social concret al faptei și perioada de timp în care obligația legală a fost încălcată.

(7) Pentru persoanele fizice autorizate, întreprinderile individuale și întreprinderile familiale, cifrei de afaceri prevăzute la alin. (4) lit. b) îi corespunde totalitatea veniturilor realizate de respectivii operatori economici în exercițiul financiar anterior sancționării.

(8) Pentru entitățile nou-înființate și pentru entitățile care nu au înregistrat cifra de afaceri în exercițiul financiar anterior sancționării, amenda prevăzută la alin. (4) se stabilește în cuantum de minimum 1 și maximum 25 de salarii minime brute pe economie.

(9) În măsura în care prezenta ordonanță de urgență nu prevede altfel, contravențiilor prevăzute la alin. (3) li se aplică dispozițiile Ordonanței Guvernului nr. 2/2001 privind regimul juridic al contravențiilor, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare.

(10) Constatarea contravențiilor prevăzute la alin. (3) se realizează de către personalul de control din cadrul DNSC, iar aplicarea sancțiunii corespunzătoare se face prin decizia directorului DNSC.

(11) Decizia prevăzută la alin. (10) trebuie să cuprindă următoarele elemente: datele de identificare ale contravenientului, data săvârșirii faptei, descrierea faptei contravenționale și a împrejurărilor care au fost avute în vedere la individualizarea sancțiunii, indicarea temeiului legal potrivit căruia se stabilește și se sancționează contravenția, sancțiunea aplicată, termenul și modalitatea de plată a amenzii, termenul de exercitare a căii de atac și instanța de judecată competentă.

(12) Dacă este cazul, directorul DNSC sesizează Consiliul Concurenței cu privire la existența unor posibile fapte sau acte anticoncurențiale.

(13) Prin derogare de la prevederile art. 13 din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, aplicarea sancțiunii potrivit alin. (4) se prescrie în termen de un an de la data săvârșirii faptei. În cazul încălcărilor care durează în timp sau al celor constând în săvârșirea, în baza aceleiași rezoluții, la intervale diferite de timp, a mai multor acțiuni sau inacțiuni, care prezintă, fiecare în parte, conținutul aceleiași contravenții, prescripția începe să curgă de la data constatării sau de la data încetării ultimului act ori fapt săvârșit, dacă acest moment intervine anterior constatării.

(14) Prin derogare de la dispozițiile art. 14 alin. (1) din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002 cu modificările și completările ulterioare, decizia prevăzută la alin. (10) se comunică contravenientului în termen de 15 zile de la data emiterii deciziei.

(15) Odată cu decizia prevăzută la alin. (10), contravenientului i se comunică și înștiințarea de plată, care conține mențiunea privind obligativitatea achitării amenzii în termen de 30 de zile de la data comunicării deciziei.

(16) Decizia prevăzută la alin. (10) constituie titlu executoriu, fără vreo altă formalitate. Acțiunea în contencios administrativ în condițiile alin. (18) suspendă executarea numai în ceea ce privește achitarea amenzii, până la pronunțarea de către instanța de judecată a unei hotărâri definitive.

(17) Sumele provenite din amenzile aplicate în conformitate cu dispozițiile prezentului articol se fac venit integral la bugetul de stat. Executarea se realizează în conformitate cu dispozițiile legale privind executarea silită a creanțelor fiscale. În vederea punerii în executare a sancțiunii, DNSC comunică din oficiu organelor de specialitate ale Agenției Naționale de Administrare Fiscală decizia prevăzută la alin. (10), după expirarea termenului prevăzut în înștiințarea de plată sau după rămânerea definitivă a hotărârii judecătorești prin care s-a soluționat acțiunea în contencios administrativ.

(18) Prin derogare de la dispozițiile art. 7 din Legea contenciosului administrativ nr. 554/2004, cu modificările și completările ulterioare, și de la dispozițiile art. 32 alin. (1) din Ordonanța Guvernului nr. 2/2001, aprobată cu modificări și completări prin Legea nr. 180/2002, cu modificările și completările ulterioare, deciziile adoptate potrivit prezentei ordonanțe de urgență pot fi atacate în contencios administrativ

la Curtea de Apel București, fără parcurgerea procedurii prealabile, în termen de 30 de zile de la comunicarea acestora.

(19) În exercitarea atribuțiilor prevăzute la art. 5 lit. i) DNSC sesizează Consiliul Concurenței cu privire la existența unor posibile fapte sau acte anticoncurențiale.

(20) Prevederile art. 19 intră in vigoare în termen de 30 de zile de la data publicării prezentei ordonanțe de urgență.

ARTICOLUL 20

Dispoziții tranzitorii și finale

(1) Prezenta ordonanță de urgență nu se aplică domeniilor de activitate din responsabilitatea instituțiilor de apărare, ordine publică și securitate națională, infrastructurilor critice naționale și infrastructurilor ce vehiculează informații clasificate.

(2) Lista bunurilor proprietate publică a statului, precum și lista bunurilor imobile proprietate privată a statului, preluate în administrare de către DNSC, se vor aproba prin hotărâre a Guvernului, în termen de 30 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență.

(3) Reîncadrarea personalului preluat potrivit art. 1 alin. (3) în structura organizatorică a DNSC se realizează în termenele și cu procedura prevăzute de lege.

(4) De la data aprobării de către CSAT a statului de funcții, organigramei și regulamentului de organizare și funcționare a DNSC se va demara procedura de ocupare a posturilor vacante în noua structură organizatorică, cu încadrare în prevederile bugetare anuale aprobate.

(5) În termen de 180 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență se va aproba, prin hotărâre a Guvernului, regulamentul de autorizare și verificare a laboratoarelor civile de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice.

(6) Normele metodologice de organizare și funcționare a registrului prevăzut la art. 5 lit. i) pct. 3 se aprobă în termen de 120 de zile de la data intrării în vigoare a prezentei ordonanțe de urgență, prin ordin al directorului DNSC care se publică în Monitorul Oficial al României, Partea I.

(7) Normele privind modalitățile de avizare, verificare și validare din punctul de vedere al securității cibernetice prevăzute la art. 5 lit. j) pct. 1 și 2 se aprobă în termen de 180 de zile de la intrarea în vigoare a prezentei ordonanțe de urgență, la propunerea directorului DNSC, prin ordin al secretarului general al Guvernului, care se publică în Monitorul Oficial al României, Partea I.

(8) Prin derogare de la dispozițiile art. 27 alin. (3) din Legea nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, cu modificările și completările ulterioare, pe durata stării de alertă se pot desfășura și concursuri sau examene pentru ocuparea posturilor vacante sau temporar vacante din structura organizatorică a DNSC.

(9) În tot cuprinsul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, publicată în Monitorul Oficial al României, Partea I, nr. 21 din 9 ianuarie 2019, cu modificările și completările ulterioare, sintagmele „Centrul Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO” și „Secretariatul General al Guvernului” se înlocuiesc cu sintagma „Directoratul Național de Securitate Cibernetică”, sintagma „CERT-RO” cu sintagma „DNSC”, iar sintagma „secretarul general al Guvernului” cu sintagma „directorul DNSC”.

(10) La data intrării în vigoare a prezentei ordonanțe de urgență se abrogă Hotărârea Guvernului nr. 494/2011 privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică — CERT-RO, publicată în Monitorul Oficial al României, Partea I, nr. 388 din 2 iunie 2011, cu modificările și completările ulterioare.

PRIM-MINISTRU
FLORIN-VASILE CÎȚU

Contrasemnează:
Secretarul general al Guvernului,
Tiberiu Horațiu Gorun
Directorul general al Centrului Național de Răspuns
la Incidente de Securitate Cibernetică — CERT-RO,
Dan Cîmpean
p. Ministrul muncii și protecției sociale,
Mihnea-Claudiu Drumea,
secretar de stat
Ministrul apărării naționale,
Nicolae-Ionel Ciucă
Ministrul afacerilor interne,
Lucian Nicolae Bode
Ministrul cercetării, inovării și digitalizării, interimar,
Tánczos Barna
p. Ministrul educației,
Gigel Paraschiv,
secretar de stat
p. Ministrul afacerilor externe,
Cornel Feruță,
secretar de stat
Ministrul finanțelor,
Dan Vîlceanu

București, 22 septembrie 2021.
Nr. 104.

★

R E C T I F I C Ă R I

În anexa nr. 16 la Ordinul ministrului justiției nr. 4.300/C/2021 privind actualizarea numărului posturilor de notar public pentru anul 2021 destinate schimbărilor de sedii ale birourilor notariale, publicat în Monitorul Oficial al României, Partea I, nr. 847 și 847 bis din 6 septembrie 2021, se face următoarea rectificare:

— la coloana „Camera Notarilor Publici", la nr. crt. 2, în loc de: *„Brașov"* se va citi: *„Bacău",* iar la nr. crt. 3, în loc de: *„Bacău"* se va citi: *„Brașov"*.

★

În anexa nr. 16 la Ordinul ministrului justiției nr. 4.301/C/2021 privind actualizarea pentru anul 2021 a numărului posturilor de notar public destinate persoanelor care au cel puțin 6 ani vechime în funcții de specialitate juridică și care vor promova concursul de dobândire a calității de notar public, publicat în Monitorul Oficial al României, Partea I, nr. 851 și 851 bis din 7 septembrie 2021, se face următoarea rectificare:

— la coloana „Camera Notarilor Publici", la nr. crt. 2, în loc de: *„Brașov"* se va citi: *„Bacău",* iar la nr. crt. 3, în loc de: *„Bacău"* se va citi: *„Brașov"*.

★

În anexa nr. 16 la Ordinul ministrului justiției nr. 4.302/C/2021 privind actualizarea pentru anul 2021 a numărului posturilor de notar public destinate notarilor stagiari care vor promova examenul de definitivat, publicat în Monitorul Oficial al României, Partea I, nr. 852 și 852 bis din 7 septembrie 2021, se face următoarea rectificare:

— la coloana „Camera Notarilor Publici", la nr. crt. 2, în loc de: *„Brașov"* se va citi: *„Bacău"*, iar la nr. crt. 3, în loc de: *„Bacău"* se va citi: *„Brașov"*.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

„Monitorul Oficial" R.A., Str. Parcului nr. 65, sectorul 1, București; 012329
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro

Adresa Biroului pentru relații cu publicul este:
Str. Parcului nr. 65, intrarea A, sectorul 1, București; 012329.
Tel. 021.401.00.73, fax 021.401.00.71 și 021.401.00.72,
e-mail: pierderiacte@ramo.ro, concursurifp@ramo.ro, convocariaga@ramo.ro

MONITORUL OFICIAL

5 948493 328582

Monitorul Oficial al României, Partea I, nr. 918/24.IX.2021 conține 16 pagini. Prețul: 3,20 lei **ISSN** 1453—4495