MONITORUL OFICIAL AL ROMÂNIEI

Anul 190 (XXXIV) — Nr. 432

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Marți, 3 mai 2022

SUMAR

L E G I Ș I D E C R E T E

PARLAMENTUL ROMÂNIEI

C A M E R A D E P U T A Ț I L O R **S E N A T U L**

L E G E
pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 123/2007 privind unele măsuri pentru consolidarea cooperării judiciare cu statele membre ale Uniunii Europene în vederea facilitării aplicării de către România a Regulamentului (UE) 2018/1.727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului

Parlamentul României adoptă prezenta lege.

Art. I. — Ordonanța de urgență a Guvernului nr. 123/2007 privind unele măsuri pentru consolidarea cooperării judiciare cu statele membre ale Uniunii Europene, publicată în Monitorul Oficial al României, Partea I, nr. 751 din 6 noiembrie 2007, aprobată cu modificări prin Legea nr. 85/2008, cu modificările și completările ulterioare, se modifică și se completează după cum urmează:

1. **La articolul 4, după alineatul (2) se introduce un nou alineat, alineatul (2^1), cu următorul cuprins:**

„(2^1) Locul de muncă al magistratului de legătură român trimis în străinătate este la sediul Ministerului Justiției din statul în care este trimis în misiune.”

2. **La articolul 4, alineatul (3) se modifică și va avea următorul cuprins:**

„(3) Magistrații de legătură sunt selectați pe baza unui concurs de dosare, care să ateste o experiență practică în domeniul cooperării judiciare internaționale, și a unui interviu. La acest concurs se pot înscrie numai judecători, procurori sau personal de specialitate juridică asimilat, potrivit legii, judecătorilor și procurorilor, având o vechime în magistratură de cel puțin 12 ani.”

3. **La articolul 4, alineatul (5) se abrogă.**

4. **La articolul 5, alineatul (1) se modifică și va avea următorul cuprins:**

„(1) Magistratul de legătură are dreptul la pașaport diplomatic pe durata misiunii în străinătate și beneficiază în statul în care este trimis de drepturile salariale și de alte drepturi bănești corespunzătoare funcției diplomatice al cărei stagiu corespunde vechimii deținute în magistratură, potrivit legislației de salarizare în vigoare pentru personalul trimis în misiune permanentă în străinătate. Drepturile salariale și celelalte drepturi bănești se suportă din bugetul Ministerului Public, al Ministerului Justiției sau al Consiliului Superior al Magistraturii, după caz.”

5. **Denumirea titlului II se modifică și va avea următorul cuprins:**

„T I T L U L II

Dispoziții pentru facilitarea aplicării Regulamentului (UE) 2018/1.727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului”

6. **Articolul 6 se modifică și va avea următorul cuprins:**

„ARTICOLUL 6

Membrul național român la Eurojust

(1) În aplicarea dispozițiilor art. 7, 8 și 9 din Regulamentul (UE) 2018/1.727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului, denumit în continuare *Regulamentul Eurojust*, România desemnează și trimite un membru național la Eurojust.

(2) Membrul național român la Eurojust are locul de muncă la sediul Eurojust și competențele stabilite prin Regulamentul Eurojust.

(3) Membrul național român la Eurojust își desfășoară activitatea sub autoritatea ministrului justiției.”

7. **Articolul 7 se modifică și va avea următorul cuprins:**

„ARTICOLUL 7

Numirea

(1) Membrul național român la Eurojust este numit prin ordin al ministrului justiției, cu avizul consultativ al secției corespunzătoare a Consiliului Superior al Magistraturii.

(2) În aplicarea dispozițiilor art. 7 alin. (4) din Regulamentul Eurojust, membrul național român la Eurojust este numit dintre persoanele care au, potrivit Legii nr. 303/2004, republicată, cu modificările și completările ulterioare, statut de procuror sau judecător.

(3) Membrul național român la Eurojust este selectat de ministrul justiției dintre persoanele cu o vechime de cel puțin 12 ani în funcția de procuror sau judecător, cu experiență în domeniul justiției penale, cu precădere în domeniul cooperării judiciare internaționale în materie penală.

(4) În aplicarea dispozițiilor art. 7 alin. (5) din Regulamentul Eurojust, durata mandatului membrului național român la Eurojust este de cinci ani, care poate fi reînnoit o singură dată.”

8. **La articolul 8, alineatul (1) se modifică și va avea următorul cuprins:**

„(1) Membrul național român la Eurojust are dreptul la pașaport diplomatic și beneficiază de drepturile salariale și de alte drepturi bănești corespunzătoare funcției diplomatice al cărei stagiu corespunde vechimii deținute în magistratură,

potrivit legislației de salarizare în vigoare pentru personalul trimis în misiune permanentă în străinătate. Drepturile salariale și celelalte drepturi bănești se suportă din bugetul Ministerului Public, al Ministerului Justiției sau al Consiliului Superior al Magistraturii, după caz."

9. **Articolul 9 se modifică și va avea următorul cuprins:**

„ARTICOLUL 9

Încetarea mandatului membrului național român la Eurojust

(1) Mandatul membrului național român la Eurojust încetează:

a) la expirarea perioadei pe care a fost numit;

b) prin renunțare;

c) prin încetarea funcției de procuror sau judecător, în condițiile legii;

d) prin eliberare din funcție.

(2) Încetarea mandatului în cazurile prevăzute la alin. (1) lit. b)—d) se constată prin ordin al ministrului justiției.

(3) Ministerul Justiției va notifica încetarea mandatului și Secretariatului General al Consiliului Uniunii Europene, prin intermediul Ministerului Afacerilor Externe.

(4) La expirarea mandatului, postul de membru național român la Eurojust va fi considerat vacant. În caz de vacanță a postului membrului național român la Eurojust, supleantul său sau, în cazurile de vacanță a postului de supleant ori când acesta nu poate acționa în numele membrului național român la Eurojust sau nu îl poate înlocui, asistentul va exercita funcția respectivă până la data începerii mandatului noului membru desemnat sau până când supleantul membrului național român la Eurojust îl poate înlocui."

10. **Titlul articolului 10 și alineatul (1) se modifică și vor avea următorul cuprins:**

„ARTICOLUL 10

Raportul anual și informarea Parlamentului României

(1) Membrul național român la Eurojust prezintă ministrului justiției, până la data de 1 martie a fiecărui an pentru anul precedent, un raport referitor la activitatea Biroului român la Eurojust. Ministrul justiției transmite o copie a raportului de activitate Parlamentului României, procurorului general al Parchetului de pe lângă Înalta Curte de Casație și Justiție și Consiliului Superior al Magistraturii."

11. **Articolul 11 se modifică și va avea următorul cuprins:**

„ARTICOLUL 11

Supleantul și asistentul membrului național român la Eurojust

(1) În aplicarea dispozițiilor art. 7 alin. (2)—(10), art. 8 și 9 din Regulamentul Eurojust, România desemnează și trimite un supleant și cel puțin un asistent al membrului național român la Eurojust.

(2) Dispozițiile art. 7—9 se aplică în mod corespunzător supleantului și asistenților membrului național la Eurojust.

(3) Supleantul acționează în numele membrului național sau îl înlocuiește pe acesta, în funcție de organizarea activității Biroului român la Eurojust. În cazul în care membrul național este ales președinte sau vicepreședinte la Eurojust, supleantul îl poate înlocui pe membrul național în exercitarea competențelor ce îi revin în această calitate. Supleantul îl înlocuiește de drept pe membrul național în caz de absență fizică de la sediul Eurojust, boală, abținere, concediu sau vacanță a postului membrului național român la Eurojust.

(4) În cazul în care membrul național la Eurojust, supleantul sau asistentul acestuia este selecționat pentru a fi trimis magistrat de legătură la Eurojust în state terțe, consimțământul la numirea acestuia de către Eurojust este dat de ministrul justiției. Persoana trimisă magistrat de legătură este înlocuită în funcția sa, după caz, de ceilalți membri ai Biroului român la Eurojust și nu mai poate exercita atribuțiile prevăzute la art. 8 din Regulamentul Eurojust. Autoritățile române pot contacta în mod direct magistratul de legătură la Eurojust, inclusiv în cazul în care acesta este selectat din cadrul altor birouri naționale la Eurojust, cu excepția cazului în care România are un magistrat de legătură trimis în acel stat.

(5) În vederea coordonării și pentru îndeplinirea atribuțiilor ce îi revin, Biroul român la Eurojust menține legături strânse cu Biroul român de legătură la Europol."

12. **La articolul 11^1, alineatul (1) se modifică și va avea următorul cuprins:**

„(1) Fără a aduce atingere dispozițiilor art. 11, în cadrul administrației Eurojust sau pentru a-l asista pe membrul național pot fi detașați experți naționali, potrivit modalităților de aplicare adoptate de Colegiul Eurojust, în temeiul art. 66 din Regulamentul Eurojust."

13. **La articolul 12 alineatul (1), după litera a) se introduce o nouă literă, litera a^1), cu următorul cuprins:**

„a^1) directorul Direcției drept internațional și cooperare judiciară din Ministerul Justiției;".

14. **La articolul 12 alineatul (1), litera b) se modifică și va avea următorul cuprins:**

„b) șeful Serviciului de cooperare judiciară internațională, relații internaționale și programe din cadrul Parchetului de pe lângă Înalta Curte de Casație și Justiție;".

15. **La articolul 12, alineatul (2) se modifică și va avea următorul cuprins:**

„(2) Fără a aduce atingere principiului contactului direct dintre membrul național la Eurojust, supleantul sau asistentul acestuia și autoritățile judiciare ori autoritățile polițienești competente, corespondenții naționali constituie puncte de contact privilegiate ale acestuia."

16. **La articolul 13, alineatul (1) se modifică și va avea următorul cuprins:**

„(1) În aplicarea dispozițiilor art. 20 alin. (3) din Regulamentul Eurojust, Sistemul Național de Coordonare Eurojust este format din:

a) corespondenții naționali ai Eurojust;

b) un corespondent național pentru probleme legate de competența Parchetului European (EPPO), desemnat de procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție;

c) corespondentul național al Rețelei Judiciare Europene în materie penală și alte trei dintre punctele naționale de contact ale acestei rețele, dintre care un judecător și doi procurori;

d) punctele naționale de contact din Rețeaua echipelor comune de anchetă și membrii naționali sau punctele naționale de contact ale rețelelor înființate prin Decizia 2002/494/JAI a Consiliului din 13 iunie 2002 de înființare a unei rețele europene de puncte de contact cu privire la persoane vinovate

de genocid, crime împotriva umanității și crime de război, prin Decizia 2007/845/JAI a Consiliului din 6 decembrie 2007 privind cooperarea dintre oficiile de recuperare a creanțelor din statele membre în domeniul urmăririi și identificării produselor provenite din săvârșirea de infracțiuni sau a altor bunuri având legătură cu infracțiunile și prin Decizia 2008/852/JAI a Consiliului din 24 octombrie 2008 privind o rețea de puncte de contact de combatere a corupției."

17. **La articolul 13, alineatele (3) și (6)—(8) se abrogă.**

18. **Articolele 13[1], 14[2], 15, 16 și 21 se abrogă.**

Art. II. — Ordonanța de urgență a Guvernului nr. 123/2007 privind unele măsuri pentru consolidarea cooperării judiciare cu statele membre ale Uniunii Europene, publicată în Monitorul Oficial al României, Partea I, nr. 751 din 6 noiembrie 2007, aprobată cu modificări prin Legea nr. 85/2008, cu modificările și completările ulterioare, precum și cu cele aduse prin prezenta lege, se va republica în Monitorul Oficial al României, Partea I, dându-se textelor o nouă numerotare.

Această lege a fost adoptată de Parlamentul României, cu respectarea prevederilor art. 75 și ale art. 76 alin. (2) din Constituția României, republicată.

PREȘEDINTELE CAMEREI DEPUTAȚILOR
ION-MARCEL CIOLACU

PREȘEDINTELE SENATULUI
FLORIN-VASILE CÎȚU

București, 2 mai 2022.
Nr. 120.

PREȘEDINTELE ROMÂNIEI

D E C R E T
privind promulgarea Legii pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 123/2007 privind unele măsuri pentru consolidarea cooperării judiciare cu statele membre ale Uniunii Europene în vederea facilitării aplicării de către România a Regulamentului (UE) 2018/1.727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului

În temeiul prevederilor art. 77 alin. (1) și ale art. 100 alin. (1) din Constituția României, republicată,

Președintele României d e c r e t e a z ă:

Articol unic. — Se promulgă Legea pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 123/2007 privind unele măsuri pentru consolidarea cooperării judiciare cu statele membre ale Uniunii Europene în vederea facilitării aplicării de către România a Regulamentului (UE) 2018/1.727 al Parlamentului European și al Consiliului din 14 noiembrie 2018 privind Agenția Uniunii Europene pentru Cooperare în Materie de Justiție Penală (Eurojust) și de înlocuire și abrogare a Deciziei 2002/187/JAI a Consiliului și se dispune publicarea acestei legi în Monitorul Oficial al României, Partea I.

PREȘEDINTELE ROMÂNIEI
KLAUS-WERNER IOHANNIS

București, 2 mai 2022.
Nr. 561.

DECIZII ALE CURȚII CONSTITUȚIONALE

CURTEA CONSTITUȚIONALĂ

DECIZIA Nr. 901
din 16 decembrie 2021

referitoare la excepția de neconstituționalitate a dispozițiilor art. 20 alin. (2) și (3) din Legea nr. 19/2000 privind sistemul public de pensii și alte drepturi de asigurări sociale și ale art. 30 alin. (1) din Legea nr. 263/2010 privind sistemul unitar de pensii publice

Valer Dorneanu — președinte
Cristian Deliorga — judecător
Marian Enache — judecător
Daniel Marius Morar — judecător
Mona-Maria Pivniceru — judecător
Gheorghe Stan — judecător
Livia Doina Stanciu — judecător
Elena-Simina Tănăsescu — judecător
Varga Attila — judecător
Cosmin-Marian Văduva — magistrat-asistent

Cu participarea reprezentantului Ministerului Public, procuror Liviu Drăgănescu.

1. Pe rol se află soluționarea excepției de neconstituționalitate a prevederilor art. 20 alin. (2) și (3) din Legea nr. 19/2000 privind sistemul public de pensii și alte drepturi de asigurări sociale și ale art. 30 alin. (1) din Legea nr. 263/2010 privind sistemul unitar de pensii publice, excepție ridicată de Octavian Cebuc și Vasile Cîrstescu în Dosarul nr. 460/90/2016 al Tribunalului Vâlcea — Secția I civilă și care constituie obiectul Dosarului Curții Constituționale nr. 3.413D/2019.

2. La apelul nominal se constată lipsa părților, procedura de înștiințare fiind legal îndeplinită.

3. Cauza fiind în stare de judecată, președintele Curții acordă cuvântul reprezentantului Ministerului Public, care solicită menținerea jurisprudenței Curții Constituționale relevante.

C U R T E A,

având în vedere actele și lucrările dosarului, constată următoarele:

4. Prin Încheierea din 29 noiembrie 2019, pronunțată în Dosarul nr. 460/90/2016, **Tribunalul Vâlcea — Secția I civilă a sesizat Curtea Constituțională cu excepția de neconstituționalitate a dispozițiilor art. 20 alin. (2) și (3) din Legea nr. 19/2000 privind sistemul public de pensii și alte drepturi de asigurări sociale și ale art. 30 alin. (1) din Legea nr. 263/2010 privind sistemul unitar de pensii publice**, excepție ridicată de Octavian Cebuc și Vasile Cîrstescu într-o cauză având ca obiect cerere privind constatarea desfășurării activității în condiții speciale.

5. **În motivarea excepției de neconstituționalitate** se arată că prevederile criticate restrâng posibilitatea ca instanța să constate, pe baza probelor, existența unor meserii care se încadrează în condiții speciale și a unor societăți care au astfel de meserii și care nu sunt menționate în anexele nr. 2 și 3 la Legea nr. 263/2010. Dacă salariații beneficiază de prevederile legale referitoare la grupele de muncă, atunci ei trebuie să poată să aibă acces direct la justiție, și nu indirect, prin intermediul sindicatului, în cazul în care sunt nemulțumiți de faptul că nu au fost încadrați în astfel de condiții.

6. Autorii susțin că au aceleași meserii și activează în aceleași condiții grele, pe același tip de locomotive vechi și deteriorate, cu cei care dețin funcția de mecanic de locomotivă/mecanic ajutor/mecanic instructor la SNTFM CFR MARFĂ și se consideră discriminați față de aceștia deoarece nu sunt și ei încadrați în condiții speciale de muncă.

7. În plus, sunt discriminați și față de cei care au lucrat în grupa I de muncă, potrivit Ordinului ministrului muncii nr. 50/1990 și Legii nr. 3/1977. Astfel, aceste acte normative prevedeau stagii de cotizare pe baza cărora se putea ieși la pensie. Dar, sub regimul Legii nr. 19/2000 și al Legii nr. 263/2010, dacă societatea nu a obținut avizul de încadrare în condiții speciale de muncă, salariații acesteia, cum este și cazul autorilor, nu mai puteau beneficia de acest stagiu de cotizare, în ciuda faptului că au lucrat în aceleași condiții care, potrivit Ordinului nr. 50/1990 și Legii nr. 3/1977, atrăgeau aplicarea unui astfel de stagiu de cotizare. Autorii critică faptul că legiuitorul nu a impus obligația de a se verifica dacă toate locurile de muncă încadrate în grupa I de muncă se înscriu în condiții speciale, după 1 aprilie 2001, și a lăsat la voia societăților inițierea procedurii doar pentru anumite meserii/funcții. Din dorința de a nu achita contribuții mai mari la buget aferente condițiilor de muncă speciale, unele societăți nu au inițiat astfel de proceduri.

8. Autorii mai precizează că, având în vedere că se află în proces de recunoaștere în instanță a condițiilor speciale de muncă în care au lucrat, sunt discriminați față de cei care și-au câștigat deja în instanță o astfel de recunoaștere.

9. În sfârșit, autorii consideră că sunt discriminați față de cei care, lucrând în condiții similare cu ei, s-au pensionat în baza Legii nr. 3/1977, deoarece, la momentul la care au început să desfășoare activitate în condiții speciale, au avut reprezentarea că se vor pensiona în condițiile acestui act normativ, adică cu 5 ani mai devreme și cu o pensie mai mare. Or, schimbându-se, între timp, legislația, au pierdut aceste avantaje și arată că poate nu și-ar mai fi asumat să presteze activități în condiții periculoase, așa cum este siguranța circulației feroviare, dacă ar fi anticipat schimbarea condițiilor de pensionare.

10. Mai departe, autorii consideră că prevederile criticate sunt contrare și art. 135 din Constituție, deoarece împiedică înființarea unei societăți a cărei activitate să se desfășoare în condiții speciale, iar angajații să beneficieze de reducerea stagiului complet de cotizare prevăzută de Legea nr. 263/2010. Menționează că activitatea desfășurată de mecanicul ajutor de locomotivă este prevăzută în anexa nr. 2 la Legea nr. 263/2010 ca loc de muncă încadrat în condiții speciale, fiind, deci, îndeplinit acest criteriu, precum și faptul că, în anexa nr. 3 la Legea nr. 263/2010, sunt menționate numeroase societăți în care această meserie se desfășoară în condiții speciale.

11. **Tribunalul Vâlcea — Secția I civilă** apreciază că excepția este neîntemeiată, deoarece prevederile criticate se aplică, fără privilegii și discriminări, tuturor destinatarilor săi. Nici art. 21 din Constituție nu este încălcat, deoarece legiuitorul are atribuția exclusivă de a stabili criteriile de încadrare în condiții de muncă speciale, precum și procedura de urmat în acest sens. Arată că, potrivit Deciziei nr. 12 din 23 mai 2016, pronunțată în recurs în interesul legii, și Deciziei nr. 43 din 21 noiembrie 2016, pronunțată în dezlegarea unei chestiuni de drept, instanța supremă a statuat că instanța judecătorească este limitată în

posibilitatea de a analiza condițiile de muncă și de a statua cu privire la încadrarea acestora în condiții speciale. Dar, arată instanța, această limitare nu a fost dedusă din prevederile criticate de către autorii excepției, care stabilesc doar procedura administrativă de încadrare a locurilor de muncă în condiții speciale, ci din interpretarea întregii legislații care reglementează această materie.

12. 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 ridicate.

13. **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, prevederile legale criticate, raportate la prevederile Constituției, precum și Legea nr. 47/1992, reține următoarele:

14. Curtea Constituțională a fost legal sesizată și este competentă, potrivit prevederilor 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.

15. **Obiectul excepției de neconstituționalitate** îl constituie dispozițiile art. 20 alin. (2) și (3) din Legea nr. 19/2000 privind sistemul public de pensii și alte drepturi de asigurări sociale, publicată în Monitorul Oficial al României, Partea I, nr. 140 din 1 aprilie 2000, și ale art. 30 alin. (1) din Legea nr. 263/2010, publicată în Monitorul Oficial al României, Partea I, nr. 852 din 20 decembrie 2010. Prevederile criticate la data sesizării Curții Constituționale aveau următorul cuprins:

— Art. 20 alin. (2) și (3) din Legea nr. 19/2000: *„(2) Alte locuri de muncă în condiții speciale decât cele prevăzute la alin. (1) pot fi stabilite numai prin lege.*

(3) Metodologia și criteriile de încadrare a persoanelor în locuri de muncă în condiții speciale se vor stabili prin hotărâre a Guvernului, pe baza propunerii comune a Ministerului Muncii și Solidarității Sociale și a Ministerului Sănătății și Familiei, în urma consultării CNPAS.”;

— Art. 30 alin. (1) din Legea nr. 263/2010: *„(1) În sensul prezentei legi, locurile de muncă în condiții speciale sunt cele din:*

a) unitățile miniere, pentru personalul care își desfășoară activitatea în subteran cel puțin 50% din timpul normal de muncă în luna respectivă;

b) activitățile de cercetare, explorare, exploatare sau prelucrare a materiilor prime nucleare, zonele I și II de expunere la radiații;

c) abrogată;

d) aviația civilă, pentru personalul navigant prevăzut în anexa nr. 1;

e) activitățile și unitățile prevăzute în anexele nr. 2 și 3;

f) activitatea artistică desfășurată în profesiile prevăzute în anexa nr. 4.”

16. La data ridicării excepției de neconstituționalitate Legea nr. 19/2000 nu mai era în vigoare. Ținând, însă, seama de cele reținute de Curtea Constituțională în Decizia nr. 766 din 15 iunie 2011, publicată în Monitorul Oficial al României, Partea I, nr. 549 din 3 august 2011, excepția de neconstituționalitate a textelor normative din această lege este admisibilă.

17. În opinia autorilor excepției de neconstituționalitate, prevederile legale criticate încalcă art. 16 alin. (1) privind egalitatea în drepturi, art. 21 privind liberul acces la justiție și art. 135 privind proprietate privată din Constituție.

18. Examinând excepția de neconstituționalitate, Curtea observă că prevederile legale criticate au mai fost supuse controlului prin raportare la critici de neconstituționalitate similare celor formulate în prezenta cauză într-o cauză soluționată, deja, de către Curtea Constituțională, respectiv prin Decizia nr. 351 din 22 mai 2018, publicată în Monitorul Oficial al României, Partea I, nr. 889 din 22 octombrie 2018.

19. Curtea a observat că dispozițiile art. 20 alin. (2) și (3) din Legea nr. 19/2000 și ale art. 30 alin. (1) din Legea nr. 263/2010 au mai constituit obiect al controlului de constituționalitate (Decizia nr. 680 din 2 noiembrie 2017, publicată în Monitorul Oficial al României, Partea I, nr. 90 din 30 ianuarie 2018, paragrafele 57—66, și Decizia nr. 259 din 6 mai 2014, publicată în Monitorul Oficial al României, Partea I, nr. 536 din 18 iulie 2014). Astfel, Curtea a amintit că procedura încadrării unor locuri de muncă în condiții speciale a fost supusă unor condiții și termene prevăzute prin Hotărârea Guvernului nr. 1.025/2003 privind metodologia și criteriile de încadrare a persoanelor în locuri de muncă în condiții speciale, publicată în Monitorul Oficial al României, Partea I, nr. 645 din 10 septembrie 2003. Curtea a statuat că nu sunt discriminate persoanele care au avut deschis accesul către procedura reglementată de Hotărârea Guvernului nr. 1.025/2003, dar fie nu au obținut încadrarea locurilor de muncă în condiții speciale, fie nu au făcut demersurile necesare în termenul prevăzut de acest act normativ. Astfel, Curtea a reținut că, deși dispozițiile art. 30 alin. (1) lit. e) din Legea nr. 263/2010 nu sunt aplicabile acestei categorii de persoane, această soluție legislativă este justificată de faptul că la momentul la care Hotărârea Guvernului nr. 1.025/2003 a creat cadrul necesar încadrării locurilor de muncă în condiții speciale, cerințele legale prevăzute de acest act normativ nu au fost îndeplinite. În mod evident, aceste persoane se găsesc într-o situație diferită față de cei care au întrunit aceste cerințe și au obținut încadrarea locurilor de muncă în condiții speciale, regăsindu-se, în prezent, în ipoteza art. 30 alin. (1) lit. e) din Legea nr. 263/2010.

20. În plus, a statuat Curtea, între persoanele care anterior Legii nr. 19/2000 au lucrat în grupa I de muncă și cele care au fost încadrate ulterior în condiții speciale nu se poate pune un semn de egalitate, deși încadrarea locurilor de muncă în condiții speciale sau deosebite a avut ca temei rațiuni asemănătoare divizării activității în grupele I și a II-a de muncă, rațiuni ce țin de gradul de solicitare, precum și de factorii de risc prezenți și expunerea la aceștia, totuși, în urma aplicării metodologiilor de încadrare stabilite prin hotărârile Guvernului mai sus amintite, nu s-a realizat o suprapunere perfectă între locurile de muncă încadrate anterior Legii nr. 19/2000 în grupele I și a II-a de muncă și cele încadrate ulterior în condiții speciale ori deosebite. Astfel, unele activități și unități care anterior se regăseau în grupa I de muncă au fost încadrate în activități și unități în care se desfășoară activitatea în condiții speciale, în timp ce altele au fost încadrate în condiții deosebite, dacă au îndeplinit condițiile stabilite de art. 2 din Hotărârea Guvernului nr. 261/2001.

21. Mai departe, tot cu privire la situația persoanelor care au avut deschis accesul la procedura prevăzută prin Hotărârea Guvernului nr. 1.025/2003, dar care nu au făcut demersurile necesare în temenele legale, Curtea Constituțională a amintit cele reținute de Înalta Curte de Casație și Justiție prin Decizia nr. 12 din 23 mai 2016 privind examinarea recursului în interesul legii formulat de procurorul general al Parchetului de pe lângă Înalta Curte de Casație și Justiție având ca obiect posibilitatea constatării pe cale judiciară sau a obligării angajatorului la încadrarea activității desfășurate în condiții deosebite sau speciale de muncă, după 1 aprilie 2001, publicată în Monitorul Oficial al României, Partea I, nr. 904 din 10 noiembrie 2016, paragraful 90 și următoarele, și a apreciat că cele constatate de

instanța supremă pun în evidență faptul că, în cazul persoanelor care au avut acces la procedura reglementată de Hotărârea Guvernului nr. 1.025/2003, nu se poate vorbi de o obstrucționare a dreptului de acces liber la justiție.

22. În jurisprudența sa, Curtea Constituțională a analizat și situația persoanelor care susțin că desfășoară una dintre activitățile prevăzute în anexa nr. 2 la Legea nr. 263/2010, dar nu beneficiază de încadrarea locurilor de muncă în condiții speciale, deoarece acestea au fost constituite ulterior finalizării procedurii reglementate de Hotărârea Guvernului nr. 1.025/2003, iar legiuitorul nu a prevăzut o procedură care să permită actualizarea listelor prevăzute în anexele nr. 2 și 3 la Legea nr. 263/2010. Astfel, făcând din nou trimitere la evoluția reglementării în materia locurilor de muncă în condiții speciale, Curtea a amintit că dispozițiile art. 30 alin. (1) lit. e) din Legea nr. 263/2010 se referă la locuri de muncă care, potrivit legislației anterioare, au fost supuse unei evaluări ce a vizat nu doar caracteristicile activității, ci și condițiile concrete în care aceasta se desfășura în cadrul unei unități. Prin stabilirea unei limite temporale pentru procedura de încadrare a unor locuri de muncă în condiții speciale, precum și din reglementarea unei proceduri de reevaluare a acestei încadrări se desprinde intenția vădită a legiuitorului de a restrânge sfera locurilor de muncă încadrate în condiții deosebite sau speciale, prin normalizarea acestora și înlăturarea factorilor de risc pentru sănătatea salariaților, potrivit legislației privind protecția muncii. În acest sens a amintit și cele reținute de Înalta Curte de Casație și Justiție, în Decizia nr. 12 din 23 mai 2016, paragrafele 39 și 40, potrivit cărora „legislația națională adoptată, începând cu Legea nr. 19/2000, cu modificările și completările ulterioare, a urmat politica legislativă a Uniunii Europene de normalizare a condițiilor de lucru ale salariaților în sensul înlăturării, pe cât posibil, a condițiilor dăunătoare pentru sănătatea și securitatea acestora. În acest sens s-a dezvoltat, în baza Directivei Consiliului nr. 89/391/CEE privind introducerea de măsuri pentru promovarea îmbunătățirii securității și sănătății lucrătorilor la locul de muncă, o legislație care stabilește norme și garanții pentru sănătatea și securitatea angajatului, cuprinzând măsuri și acțiuni eșalonate în scopul eliminării locurilor de muncă în condiții deosebite, prin normalizarea condițiilor de muncă, limitându-se totodată posibilitatea angajatorului de a crea și dezvolta noi locuri de muncă periculoase. Aceasta este rațiunea pentru care legislația ce face obiectul procesului de unificare a interpretării pe calea prezentului recurs în interesul legii are aplicabilitate limitată în timp și cu privire la persoane, astfel că nu poate fi extinsă în ceea ce privește unități lucrative nou-create, care ar cuprinde locuri de muncă încadrabile în condiții deosebite sau speciale. La data de 31 decembrie 2002 s-a încheiat procesul de avizare pentru condițiile deosebite de muncă, respectiv la data de 30 iunie 2005, pentru nominalizarea locurilor de muncă în care se desfășoară activități încadrate în condiții speciale. Reînnoirea avizelor de încadrare a fost permisă doar atunci când, pe baza măsurilor adoptate de angajator, nu a fost posibilă normalizarea condițiilor de muncă.” Prin urmare, Curtea a apreciat că locurile de muncă înființate după încheierea procedurii reglementate de Hotărârea Guvernului nr. 1.025/2003 nu mai pot întruni, în mod obiectiv, aceleași criterii care au determinat, potrivit legislației anterioare, încadrarea în condiții speciale de muncă în grupa I a unor activități care nu beneficiau de o protecție suficientă a salariaților împotriva riscurilor implicate de desfășurarea respectivelor activități.

23. În sfârșit, Curtea a statuat, în ceea ce privește dispozițiile art. 135 din Constituție, invocate și de către autorii prezentei excepții, că dispozițiile art. 30 alin. (1) din Legea nr. 263/2010 nu au incidență asupra accesului liber al angajatorilor la o activitate economică ori asupra manifestării liberei inițiative.

24. Având în vedere cele anterior redate, precum și faptul că nu există motive pentru îndepărtarea de la soluția și motivarea din decizia menționată, considerentele acesteia își păstrează valabilitatea și în prezenta cauză.

25. Pentru considerentele expuse mai sus, în temeiul art. 146 lit. d) și al art. 147 alin. (4) din Constituție, 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 Octavian Cebuc și Vasile Cîrstescu în Dosarul nr. 460/90/2016 al Tribunalului Vâlcea — Secția I civilă și constată că dispozițiile art. 20 alin. (2) și (3) din Legea nr. 19/2000 privind sistemul public de pensii și alte drepturi de asigurări sociale și ale art. 30 alin. (1) din Legea nr. 263/2010 privind sistemul unitar de pensii publice sunt constituționale în raport cu criticile formulate.

Definitivă și general obligatorie.

Decizia se comunică Tribunalului Vâlcea — Secția I civilă și se publică în Monitorul Oficial al României, Partea I.

Pronunțată în ședința din data de 16 decembrie 2021.

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

Magistrat-asistent,
Cosmin-Marian Văduva

HOTĂRÂRI ALE GUVERNULUI ROMÂNIEI

GUVERNUL ROMÂNIEI

HOTĂRÂRE
privind suplimentarea pe anul 2022 a sumei prevăzute ca justă despăgubire, aprobată prin Hotărârea Guvernului nr. 736/2020 privind declanșarea procedurilor de expropriere a tuturor imobilelor proprietate privată care constituie coridorul de expropriere al lucrării de utilitate publică de interes național „Varianta de ocolire a municipiului Zalău, etapa 2, între DN1F, km 79+625— DJ 191C", precum și modificarea și completarea anexei nr. 2 la Hotărârea Guvernului nr. 736/2020

În temeiul art. 108 din Constituția României, republicată, precum și al art. 5 alin. (1), al art. 9 alin. (8), al art. 11 alin. (7) și al art. 32 alin. (2) din Legea nr. 255/2010 privind exproprierea pentru cauză de utilitate publică, necesară realizării unor obiective de interes național, județean și local, cu modificările și completările ulterioare,

Guvernul României adoptă prezenta hotărâre.

Art. I. — Se aprobă suplimentarea pe anul 2022 a sumei prevăzute ca justă despăgubire, aprobată prin Hotărârea Guvernului nr. 736/2020 privind declanșarea procedurilor de expropriere a tuturor imobilelor proprietate privată care constituie coridorul de expropriere al lucrării de utilitate publică de interes național „Varianta de ocolire a municipiului Zalău, etapa 2, între DN1F, km 79+625—DJ 191C", cu suma totală de 142,52 mii lei, care se alocă de la bugetul de stat, prin bugetul Ministerului Transporturilor și Infrastructurii, în conformitate cu Legea bugetului de stat pe anul 2022 nr. 317/2021, la capitolul 84.01 „Transporturi", subcapitolul 03 „Transport rutier", titlul 58 „Proiecte cu finanțare din fonduri externe nerambursabile aferente cadrului financiar 2014—2020", articolul 58.01 „Programe din Fondul European de Dezvoltare Regională — FEDR".

Art. II. — Anexa nr. 2 la Hotărârea Guvernului nr. 736/2020 privind declanșarea procedurilor de expropriere a tuturor imobilelor proprietate privată care constituie coridorul de expropriere al lucrării de utilitate publică de interes național „Varianta de ocolire a municipiului Zalău, etapa 2, între DN1F, km 79+625—DJ 191C", publicată în Monitorul Oficial al României, Partea I, nr. 814 din 3 septembrie 2020, se modifică și se completează, după cum urmează:

1. **Pozițiile nr. crt. 70 și 89 se modifică, în sensul actualizării, în condițiile legii, a elementelor de identificare, a titularilor de drepturi reale și a sumelor individuale aferente despăgubirilor, în conformitate cu anexa la prezenta hotărâre.**

2. **La pozițiile nr. crt. 70 și 89 se introduc imobilele proprietate privată reprezentând construcții situate pe terenurile supuse exproprierii în condițiile legii, care constituie coridorul de expropriere situat pe amplasamentul aprobat prin Hotărârea Guvernului nr. 736/2020.**

Art. III. — (1) Se aprobă declanșarea procedurii de expropriere pentru imobilele proprietate privată reprezentând construcții, prevăzute la art. II pct. 2, situate pe terenurile supuse exproprierii în condițiile legii, care constituie coridorul de expropriere situat pe amplasamentul aprobat prin Hotărârea Guvernului nr. 736/2020, expropriator fiind statul român, reprezentat de Ministerul Transporturilor și Infrastructurii, prin Compania Națională de Administrare a Infrastructurii Rutiere — S.A.

(2) Se aprobă lista cuprinzând imobilele proprietate privată reprezentând construcții, supuse exproprierii potrivit alin. (1), aflate pe raza localității Zalău, județul Sălaj, proprietarii sau deținătorii acestora, precum și sumele individuale aferente despăgubirilor, în conformitate cu anexa la prezenta hotărâre.

Art. IV. — (1) Suma aprobată potrivit art. I se utilizează în scopul acordării justelor despăgubiri estimate de expropriator pentru imobilele prevăzute la art. II, în conformitate cu anexa la prezenta hotărâre.

(2) Sumele individuale estimate de expropriator prevăzute la alin. (1) se virează de către Ministerul Transporturilor și Infrastructurii într-un cont de trezorerie deschis pe numele Companiei Naționale de Administrare a Infrastructurii Rutiere — S.A., în termen de cel mult 30 de zile de la data aprobării cererii de deschidere de credite, conform prevederilor art. 4 alin. (8) din Normele metodologice de aplicare a Legii nr. 255/2010 privind exproprierea pentru cauză de utilitate publică, necesară realizării unor obiective de interes național, județean și local, aprobate prin Hotărârea Guvernului nr. 53/2011, cu completările ulterioare, la dispoziția proprietarilor/deținătorilor de imobile proprietate privată care constituie coridorul de expropriere al lucrării de utilitate publică de interes național „Varianta de ocolire a municipiului Zalău, etapa 2, între DN1F, km 79+625— DJ 191C", în vederea efectuării plății despăgubirilor în cadrul procedurilor de expropriere, în condițiile legii.

Art. V. — Ministerul Transporturilor și Infrastructurii, prin Compania Națională de Administrare a Infrastructurii Rutiere — S.A., răspunde de realitatea datelor din anexa la prezenta hotărâre, de modul de utilizare, în conformitate cu prevederile legale, a sumei alocate potrivit prevederilor prezentei hotărâri, precum și de corectitudinea datelor înscrise în documentele care au stat la baza stabilirii acesteia.

PRIM-MINISTRU
NICOLAE-IONEL CIUCĂ

Contrasemnează:
Viceprim-ministru,
ministrul transporturilor și infrastructurii,
Sorin Mihai Grindeanu
Ministrul finanțelor,
Adrian Câciu

București, 28 aprilie 2022.
Nr. 567.

LISTA

cuprinzând imobilele proprietate privată care constituie coridorul de expropriere al lucrării de utilitate publică de interes național „Varianta de ocolire a municipiului Zalău, etapa 2, între DN1F, km 79+625—DJ 191C”, aflate pe raza municipiului Zalău, județul Sălaj, proprietarii sau deținătorii acestora, precum și sumele individuale aferente despăgubirilor

Nr. crt.	Nr. crt. Hotărârea Guvernului nr. 736/2020	Județul	Unitatea administrativ-teritorială	Numele și prenumele proprietarului/ deținătorului imobilului	Tarlaua	Parcela	Categoria de folosință	Intravilan/ Extravilan	Număr cadastral	Număr carte funciară	Suprafața totală (mp)	Suprafața terenului de expropriat (mp)	Suprafața de expropriat — construcții (mp/ml/mc)	Valoarea de despăgubire a imobilului conform Legii nr. 255/2010 (lei)
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1	70	Sălaj	Zalău	Ignat Iuliu	—	—	Pășune	Extravilan	63046	63046	7.500,00	3.338,00	—	6.309,00
											—	—	123 mp CA — anexă agricolă cu regim de înălțime P + M	90.636,00
											—	—	Fântână cu hidrofor acoperită și alimentată de la panouri solare	4.156,80
											—	—	27 mp — platformă betonată	7.944,00
2	89	Sălaj	Zalău	Șandor Jozsef, Șandor Mihaela	36	P718	Curți-construcții/ Livadă	Extravilan	53801	53801	5.070,00	106	—	334,96
												1.527,00	—	5.512,47
												—	Fântână	2.720,90
												—	Fântână	1.700,85
												—	Fosă	2.053,90
												—	213,15 ml împrejmuire	35.967,40

ACTE ALE BĂNCII NAȚIONALE A ROMÂNIEI

BANCA NAȚIONALĂ A ROMÂNIEI

REGULAMENT
privind cadrul de desfășurare a testelor de reziliență cibernetică TIBER-RO

Având în vedere prevederile art. 2 alin. (2) lit. b) și ale art. 22 alin. (1) și (2) din Legea nr. 312/2004 privind Statutul Băncii Naționale a României, ale art. 404, 407 și ale art. 408 alin. (1) din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea nr. 227/2007, cu modificările și completările ulterioare,

luând în considerare metodologia TIBER–EU dezvoltată la nivelul Băncii Centrale Europene, prin care se stabilește cadrul european de testare a rezilienței cibernetice a instituțiilor financiare, prin realizarea unor teste controlate, care simulează atacuri de natură cibernetică ale unor entități avansate și persistente, pe baza informațiilor privind amenințările și vulnerabilitățile specifice entității testate,

în temeiul art. 48 alin. (2) din Legea nr. 312/2004 privind Statutul Băncii Naționale a României și ale art. 405 lit. c) și e) și art. 420 alin. (1) din Ordonanța de urgență a Guvernului nr. 99/2006 privind instituțiile de credit și adecvarea capitalului, aprobată cu modificări și completări prin Legea nr. 227/2007, cu modificările și completările ulterioare,

Banca Națională a României emite următorul regulament:

CAPITOLUL I
Obiect, domeniu de aplicare și definiții

Art. 1. — (1) Prezentul regulament stabilește cadrul de testare a rezilienței cibernetice, prin desfășurarea unor atacuri cibernetice simulate, cu grad ridicat de complexitate și bazate pe informații despre vulnerabilitățile și amenințările la care entitățile sunt supuse în realitate, denumit în continuare *cadrul TIBER-RO*.

(2) Prezentul regulament se aplică administratorilor de infrastructuri ale pieței financiare aflați în aria de monitorizare a Băncii Naționale a României, denumită în continuare *BNR*, precum și instituțiilor de credit desemnate drept participanți critici la infrastructurile pieței financiare.

(3) Instituțiile participante la infrastructurile pieței financiare, care nu sunt desemnate participanți critici, pot să realizeze testul TIBER-RO în mod voluntar.

Art. 2. — În înțelesul prezentului regulament, termenii și expresiile de mai jos au următoarele semnificații:

a) *active informaționale* — date sau alte cunoștințe care au valoare pentru instituție, inclusiv sisteme ale tehnologiei informației și comunicațiilor, configurațiile acestora, alte infrastructuri, precum și conexiunile cu alte sisteme externe și interne;

b) *actor statal* — unitate de luptă cibernetică sau grup susținut de către un stat care amenință cibernetic o entitate testată;

c) *amenințare cibernetică* — potențial atac, desfășurat cu precădere cu mijloace informatice de către atacatori avansați din punct de vedere tehnologic și persistenți, inclusiv grupări de crimă organizată sau actori statali, care afectează confidențialitatea, integritatea sau disponibilitatea resurselor care susțin funcțiile critice ale entității testate;

d) *colectare de informații în mod activ* — tehnică de obținere a informațiilor despre activele informaționale ale entităților testate, prin angajarea în interacțiune directă cu sistemele informatice și cu personalul entităților testate și prin evaluarea răspunsului acestora la diverși stimuli;

e) *colectare de informații în mod pasiv* — tehnică de obținere a informațiilor despre activele informaționale ale entităților testate fără a interacționa direct cu acestea;

f) *CTI (Cyber Threat Intelligence)* — procesul prin care sunt colectate, analizate și interpretate date și informații, în scopul identificării atacurilor cibernetice și a autorilor acestora și cunoașterii unor elemente esențiale legate de modul de operare, motivele, intențiile, resursele și capabilitățile acestora;

g) *echipa albastră (Blue Team) — BT* — întreg personalul entității testate care sprijină îndeplinirea funcțiilor critice ale acesteia, cu excepția personalului echipei albe, ale căror capacități de prevenire, detectare și răspuns sunt testate, fără a fi informat în prealabil despre desfășurarea testului;

h) *echipa albă (White Team) — WT* — echipa desemnată de către entitatea testată pentru elaborarea documentului Sfera de cuprindere a testului achiziția furnizorilor Threat Intelligence și Red Team și coordonarea testului, fiind singura structură din cadrul entității care cunoaște toate detaliile legate de test și care va reprezenta entitatea în relația cu BNR, cu furnizorul Threat Intelligence și cu furnizorul Red Team;

i) *echipa roșie (Red Team) — RT* — echipa externă din cadrul furnizorului Red Team care efectuează atacul simulat asupra entității testate în scopul de a testa reziliența cibernetică a acesteia;

j) *echipa TI (Threat Intelligence)* — echipa din cadrul furnizorului Threat Intelligence care, pe baza analizei de tip Cyber Threat Intelligence și Targeted cyber threat intelligence, elaborează raportul Threat Intelligence la adresa entității testate;

k) *entitate sau instituție testată* — are semnificația prevăzută la art. 1 alin. (2) sau, după caz, alin. (3) din prezentul regulament;

l) *funcții critice* — funcțiile entității testate, necesare pentru funcționarea unei infrastructuri a pieței financiare sau pentru participarea acesteia la infrastructuri ale pieței financiare, care necesită anumite resurse de personal, informații, procese și tehnologii și care, dacă ar fi afectate, ar putea avea un impact negativ semnificativ asupra: stabilității financiare, siguranței și solidității entității, clienților entității sau pieței în care activează entitatea;

m) *furnizor RT* — persoana juridică contractată de către entitatea testată pentru a furniza servicii de testare cibernetică utilizând o echipă de tip Red Team;

n) *furnizor TI* — persoana juridică contractată de către entitatea testată pentru a furniza servicii de informații de tip Cyber Threat Intelligence și Targeted cyber threat intelligence, utilizând o echipă de Threat Intelligence;

o) *participant critic* — entitate definită în art. 2 pct. 53 din Regulamentul Băncii Naționale a României nr. 3/2018 privind monitorizarea infrastructurilor pieței financiare și a instrumentelor de plată, cu modificările și completările ulterioare;

p) *raport de test* — raport formal prevăzut la art. 28 din prezentul regulament;

q) *raport TI* — raportul de amenințări și vulnerabilități de natură cibernetică la adresa entității testate, care conține analiza de tip Targeted cyber threat intelligence specifică entității testate, în contextul informațiilor de tip Cyber Threat Intelligence despre amenințările specifice naționale de natură cibernetică, luând în

considerare activitățile de tip Advanced Persistent Threat la nivelul sectorului financiar bancar, într-o perioadă de minimum 12 luni înaintea desfășurării testului TIBER-RO;

r) *reziliență cibernetică* — capacitatea unei entități de a anticipa amenințările cibernetice, de a rezista la atacurile cibernetice, de a limita amploarea consecințelor unui atac cibernetic și de a relua activitatea după astfel de atacuri;

s) *sfera de cuprindere a testului* — document formal care include elementele prevăzute la art. 20 alin. (1) din prezentul regulament;

t) *Targeted cyber threat intelligence* — informații cu privire la amenințări și vulnerabilități de natură cibernetică de tip Cyber Threat Intelligence, care vizează cel puțin, dar fără a se limita la acestea: (i) descrierea generală a atacurilor de tip Advanced Persistent Threat care pot ataca entitățile testate; (ii) vulnerabilitățile resurselor care sprijină funcțiile critice ale entităților testate; (iii) tacticile, tehnicile și procedurile utilizate în atacurile de tip Advanced Persistent Threat, prin care acestea ar putea exploata vulnerabilitățile entităților testate.

CAPITOLUL II
Dispoziții generale

SECȚIUNEA 1
Condiții generale

Art. 3. — (1) Entitățile prevăzute la art. 1 alin. (2) realizează testul TIBER-RO cel puțin o dată la 3 ani, în condițiile stabilite prin prezentul regulament.

(2) În vederea asigurării și menținerii unui cadru solid de gestionare a riscurilor pe toată durata desfășurării testului TIBER-RO, entitatea stabilește proceduri, procese și controale adecvate, vizând inclusiv operațiunile desfășurate de furnizorul TI și furnizorul RT, pentru a identifica, monitoriza și gestiona în mod cuprinzător toată gama de riscuri asociate acestui test.

(3) În aplicarea alin. (1), entitățile asigură respectarea cerințelor de desfășurare a testului TIBER-RO, inclusiv prin contractele încheiate cu furnizorii TI și cu furnizorii RT.

Art. 4. — (1) Testele de tip TIBER-RO, denumite în continuare *teste*, vizează:

a) funcțiile critice ale entității testate;

b) infrastructura informatică de producție, informațiile, procedurile, personalul și serviciile externalizate, utilizate de entitate, care susțin funcțiile critice ale entității testate.

(2) Testele simulează, într-un mod controlat, atacuri de natură cibernetică ale unor atacatori avansați din punct de vedere tehnologic și persistenți, inclusiv grupări de crimă organizată sau actori statali, care pot afecta disponibilitatea, integritatea și confidențialitatea resurselor care susțin funcțiile critice ale entității testate, folosind instrumente, metode și tehnici specifice acestor atacatori, cu scopul de a verifica și îmbunătăți reziliența cibernetică a entității testate.

Art. 5. — (1) BNR monitorizează testele pe tot parcursul desfășurării acestora, urmărind să fie respectate cerințele prezentului regulament, iar, în caz contrar, poate solicita întreruperea procesului de testare sau implementarea unor măsuri de remediere pentru a se asigura conformitatea cu prevederile prezentului regulament.

(2) În sensul alin. (1), BNR furnizează îndrumare WT pe toată durata desfășurării testului, avizează întreaga documentație întocmită de către WT, furnizorii TI și furnizorii RT cu privire la test, precum și documentul prevăzut la art. 31 alin. (4) din prezentul regulament și monitorizează implementarea măsurilor stabilite în planurile de remediere.

(3) Entitățile testate transmit BNR orice informații solicitate de aceasta pentru monitorizarea efectuării testelor TIBER-RO.

SECȚIUNEA a 2-a
Etapele testului

Art. 6. — Demararea testelor se realizează prin transmiterea unei solicitări de către entitatea care urmează să facă obiectul testării către BNR, conform anexei nr. 1 la prezentul regulament.

Art. 7. — Testul se desfășoară în următoarele etape succesive:

a) stabilirea perioadei de desfășurare a testului și stabilirea WT de către entitatea care urmează să facă obiectul testării;

b) stabilirea și documentarea sferei de cuprindere a testului de către WT și aprobarea acesteia de către consiliul de administrație al entității care urmează să facă obiectul testării;

c) selectarea furnizorului TI și a furnizorului RT de către WT și contractarea serviciilor acestora;

d) elaborarea de către furnizorul TI a raportului TI la adresa entității testate, pe baza sferei de cuprindere a testului, în colaborare cu WT și, dacă este cazul, și cu furnizorul RT;

e) elaborarea de către furnizorul RT a planului de testare a entității testate, pe baza raportului TI, în colaborare cu WT și furnizorul TI;

f) aplicarea de către furnizorul RT a planului de testare a entității testate, în colaborare cu WT și, dacă este cazul, și cu furnizorul TI;

g) finalizarea testului, care implică:

(i) întocmirea de către furnizorul RT a raportului de test;

(ii) întocmirea de către structura responsabilă de securitatea cibernetică a entității testate a raportului de acțiune al BT;

(iii) efectuarea exercițiului de reconstituire a testului, cu participarea tuturor părților implicate;

(iv) elaborarea de către furnizorul RT a unui rezumat al rezultatelor testării, transmis BNR;

(v) elaborarea de către WT a unui plan de remediere, în colaborare cu structura responsabilă de securitatea cibernetică a entității testate, în baza recomandărilor din Raportul de test, aprobat de către consiliul de administrație al entității testate.

Art. 8. — (1) Toate documentele întocmite în legătură cu procesul de testare, precum și comunicările aferente trebuie să fie în limba română sau în limba engleză și sunt confidențiale, cu un regim de diseminare controlat, bazat pe principiul „necesității de a cunoaște”.

(2) Pe parcursul întregului proces trebuie folosit un nume de cod, stabilit de către WT, pentru a păstra confidențialitatea entității testate.

(3) Raportul de test și raportul de acțiune al BT sunt păstrate de către entitatea testată și sunt consultate de reprezentanții BNR exclusiv la fața locului.

(4) Entitatea testată informează semestrial BNR cu privire la îndeplinirea măsurilor stabilite prin Planul de remediere, dar nu mai târziu de 15 zile de la începutul fiecărui semestru.

SECȚIUNEA a 3-a
Limitări ale testelor de tip TIBER-RO

Art. 9. — Cadrul contractual încheiat de către entitățile testate cu furnizorii TI și RT trebuie să cuprindă cel puțin:

a) obligația furnizorilor TI și RT de păstrare a confidențialității cu privire la toate datele dobândite de aceștia în procesul de efectuare a testelor;

b) Interdicția de:

(i) a distruge echipamentele entității testate;

(ii) a modifica necontrolat datele, programele informatice sau configurațiile sistemelor informatice ale entității testate;

(iii) a periclita continuitatea funcțiilor critice ale entității testate;

(iv) a dezvălui, în afara cadrului stabilit prin acest regulament, informațiile privind amenințările și vulnerabilitățile specifice entității testate și/sau rezultatele testului.

Art. 10. — (1) Până la finalizarea testului, informațiile referitoare la test sunt cunoscute exclusiv de către WT, consiliul de administrație al entității, furnizorul TI, furnizorul RT și BNR.

(2) În cazul în care BNR constată, prin orice mijloace, că există informații referitoare la test care au ajuns la cunoștința BT înainte de finalizarea testului, BNR va informa, în scris, entitatea cu privire la obligația de a relua testul de la început.

(3) În cazul în care BNR constată că testul nu se desfășoară cu un control adecvat sau că cerințele prezentului regulament nu sunt respectate, informează imediat WT și solicită aplicarea cu celeritate a măsurilor de remediere necesare. Dacă situația de neconformitate persistă, BNR solicită entității întreruperea testului până la remedierea deficiențelor constatate.

Art. 11. — (1) Testarea se realizează doar de către furnizorii TI și RT și membrii echipelor TI și RT care îndeplinesc cerințele prevăzute în anexa nr. 2, contractați în prealabil, cu respectarea specificațiilor testului.

(2) Pentru asigurarea obiectivității procesului de testare, entitatea poate să utilizeze același furnizor TI sau RT pentru realizarea a cel mult două teste consecutive.

SECȚIUNEA a 4-a

Cerințe aplicabile WT

Art. 12. — (1) Membrii WT dețin o gamă adecvată de competențe tehnice, cunoștințe, experiență și un nivel ierarhic ridicat și au responsabilități în cel puțin unul dintre următoarele domenii:

a) operarea funcțiilor critice ale entității;

b) continuitatea activității entității;

c) gestionarea riscurilor operaționale și de securitate informatică ale entității;

d) procesul de achiziție de servicii pentru entitate;

e) furnizarea de asistență juridică referitoare la contractele de prestări servicii și legislația aferentă funcționării entității.

(2) În aplicarea alin. (1), în funcție de structura și modul de organizare a entității, WT trebuie să fie alcătuită din minimum 3 și maximum 7 persoane care dețin una dintre următoarele funcții sau echivalent sau aparțin uneia dintre următoarele categorii de personal:

a) COO (Chief Operating Officer) — coordonatorul funcției care se ocupă de supervizarea operațiunilor curente ale organizației;

b) CIO (Chief Information Officer) — coordonatorul funcțiilor de gestionare, implementare și utilizare a tehnologiilor informatice;

c) CTO (Chief technology officer) — coordonatorul funcției care se ocupă de dezvoltările și implementările tehnologice în organizație;

d) CISO (Chief Information Security Officer) — coordonatorul funcției care se ocupă de securitatea informațiilor.

Art. 13. — (1) WT este coordonată de un manager, ce raportează direct către consiliul de administrație al entității, reprezintă entitatea în relația cu BNR și cu restul entităților participante la testare și este împuternicit să semneze orice documente și contracte în numele entității în scopul derulării testului.

(2) Coordonatorul WT:

a) trebuie să dețină abilități de coordonare și experiență în funcționarea entității și a infrastructurii acesteia (inclusiv a activității referitoare la tehnologia informației și comunicațiilor și a operațiunilor comerciale desfășurate);

b) este preferabil să dețină experiență în colaborarea cu alte departamente relevante ale entității (de exemplu: operațional, juridic, achiziții, comercial, securitate fizică, fraudă etc.) și în testarea rezilienței cibernetice, preferabil în testarea de tip RT.

(3) Prin excepție de la prevederile alin. (2) lit. b), în situația în care coordonatorul WT nu deține unele dintre respectivele abilități, acestea trebuie să fie asigurate de alți membri ai WT.

Art. 14. — WT are următoarele responsabilități:

a) implementează procedurile, procesele și controalele stabilite la art. 3 alin. (2) și (3);

b) elaborează sfera de cuprindere a testului și desfășoară procesul de contractare a furnizorului TI și a furnizorului RT, urmărind implementarea tuturor măsurilor necesare pentru gestionarea riscurilor și păstrarea confidențialității informațiilor;

c) în scopul asigurării îndeplinirii criteriilor de bună reputație, onestitate și integritate, solicită furnizorilor TI și RT caziere judiciare sau documente similare care să ateste lipsa antecedentelor penale ale furnizorilor contractați, ale coordonatorilor și ale membrilor echipei TI și, respectiv, ale membrilor RT;

d) avizează raportul TI, planul de testare, raportul de test, raportul de acțiune al BT;

e) monitorizează continuu respectarea de către echipa TI și de către RT a documentației de test, colaborează permanent cu BNR și asigură buna desfășurare a testului;

f) elaborează planul de remediere și îl înaintează spre aprobare consiliului de administrație al entității.

SECȚIUNEA a 5-a

Cerințe aplicabile furnizorilor TI și furnizorilor RT aferente cadrului contractual cu entitatea testată

Art. 15. — Furnizorul TI trebuie să utilizeze metodologii bine fundamentate pentru documentarea și recunoașterea amenințărilor, precum și să fie capabil să explice evoluția acestora și modul în care conduc la rezultate eficace în cadrul testelor RT. Metodologiile trebuie să fie întocmite astfel încât să demonstreze entității că furnizorul TI este în măsură:

a) să obțină un context util pentru efectuarea analizei privind amenințările;

b) să documenteze situația actuală a entității din punctul de vedere al riscurilor cibernetice;

c) să documenteze și să fundamenteze pregătirea atacului;

d) să colaboreze cu celelalte părți implicate în testare;

e) să aibă o viziune comprehensivă asupra sectorului financiar în care entitatea operează;

f) să realizeze evaluări și analize privind riscurile;

g) să își operaționalizeze metodologiile într-un mod clar, transparent și flexibil.

Art. 16. — (1) Furnizorul TI trebuie să elaboreze raportul TI, pornind de la sfera de cuprindere a testului, și să îl transmită către furnizorul RT, WT și BNR pentru revizuire.

(2) Furnizorul TI trebuie să colaboreze cu WT și cu furnizorul RT pe toată durata testării, prin oferirea de asistență pentru furnizorul RT în stabilirea scenariilor de atac și actualizarea informațiilor obținute pe măsură ce atacul RT avansează.

(3) Raportul TI nu trebuie să fie condiționat de experiența furnizorului RT și de capacitatea RT de a-l pune în aplicare.

(4) Furnizorul TI și furnizorul RT pot fi aceeași persoană juridică, dar personalul echipei TI trebuie să fie diferit de personalul RT.

(5) Furnizorul TI și furnizorul RT, respectiv personalul implicat în desfășurarea testelor trebuie să dispună de o bună reputație, onestitate și integritate.

Art. 17. — Furnizorul RT trebuie să utilizeze metodologii bine fundamentate de management al riscului și:

a) să obțină un set de informații relevante pentru a asigura penetrarea sistemelor informatice ale entității testate, bazându-se pe informațiile din raportul TI și pe cele obținute utilizând metodele de colectare de informații utilizate de către atacatorii cibernetici;

b) să înregistreze și raporteze WT toate acțiunile întreprinse în cadrul testării;

c) să aibă o viziune cuprinzătoare asupra sectorului financiar în care entitatea testată operează;

d) să elaboreze și să execute planul de testare a entității testate, pornind de la raportul TI și având în vedere sfera de cuprindere a testului;

e) să colaboreze cu WT și cu furnizorul TI în etapa de elaborare a planului de testare, pe întreaga durată a testării și în etapa de încheiere;

f) să aplice, dacă este cazul, și alte scenarii de atac, identificate în colaborare cu furnizorul TI și aprobate de către WT;

g) să urmeze o metodologie de testare etică și riguroasă;

h) să ia toate măsurile necesare pentru ca funcțiile critice ale entității testate să nu fie perturbate;

i) să informeze WT, furnizorul TI și BNR, ori de câte ori i se solicită sau consideră că este cazul, cu privire la progresul din timpul testării și referitor la obiectivele ce urmează a fi atinse în timpul testului;

j) să elaboreze și să transmită raportul de test către WT și furnizorul TI pentru revizuire;

k) să participe la exercițiul de reconstituire a testului.

Art. 18. — (1) Cerințele prevăzute de prezentul regulament în legătură cu furnizorii TI și furnizorii RT sunt integrate în cadrul contractual încheiat de către entitățile testate cu aceștia.

(2) Cadrul contractual dintre entitățile testate și furnizorii TI și RT trebuie să includă clauze privind confidențialitatea și protecția datelor cu caracter personal și să prevadă garanții adecvate pentru respectarea cerințelor legislației incidente în domeniul datelor cu caracter personal.

CAPITOLUL III
Desfășurarea testului TIBER-RO

SECȚIUNEA 1
Inițierea testului

Art. 19. — (1) După primirea solicitării prevăzute la art. 6, BNR solicită entității care face obiectul testării să stabilească WT și furnizează entității informații relevante cu privire la: procesul de testare, rolurile și responsabilitățile părților implicate, precum și orice alte informații necesare pentru derularea testului, în conformitate cu cerințele prezentului regulament.

(2) BNR poate solicita ajustarea perioadei de realizare a testului pentru a asigura eficiența monitorizării acestuia.

Art. 20. — (1) În vederea testării, WT documentează sfera de cuprindere a testului, identificând cel puțin următoarele:

a) funcțiile critice ale entității testate;

b) toate resursele de personal, informații, tehnologii și proceduri care contribuie la furnizarea funcțiilor critice ale entității testate, inclusiv acele sisteme/procese/servicii externalizate către terți;

c) țintele și obiectivele pe care echipa RT trebuie să le atingă în timpul testului.

(2) Obiectivele testului trebuie să fie formulate în sensul de a demonstra că integritatea, confidențialitatea sau disponibilitatea resurselor care susțin funcțiile critice ale entității testate pot fi afectate de un atacator, fără să afecteze buna funcționare a entității.

(3) Documentul privind sfera de cuprindere a testului este aprobat de către consiliul de administrație al entității testate.

Art. 21. — (1) WT achiziționează serviciile furnizorilor TI și furnizorilor RT după ce verifică îndeplinirea de către aceștia a cerințelor din prezentul regulament.

(2) WT prezintă BNR toate documentele și informațiile necesare din care rezultă că furnizorii TI și furnizorii RT și, respectiv, coordonatorii și membrii echipelor TI și RT contractați pentru derularea testului îndeplinesc cerințele minime prevăzute în prezentul regulament.

SECȚIUNEA a 2-a
Realizarea testului

Art. 22. — Furnizorul TI realizează o analiză exactă a amenințărilor și vulnerabilităților specifice entității testate evaluate, pe baza sferei de cuprindere a testului, a celor mai noi informații referitoare la vulnerabilitățile și amenințările de natură cibernetică la nivel internațional și/sau asupra sectorului financiar național, precum și pe baza raționamentului profesional.

Art. 23. — (1) În urma analizei amenințărilor și vulnerabilităților specifice entității testate, furnizorul TI elaborează raportul TI, pe care furnizorul RT îl va folosi în faza de testare.

(2) Etapa de analiză și elaborare a raportului TI trebuie să fie una corespunzătoare complexității entității testate, nu mai mică de 5 săptămâni, iar colectarea de informații trebuie să se desfășoare exclusiv în mod pasiv, pentru a nu alerta BT.

(3) WT pune la dispoziția furnizorului TI rezumatele rapoartelor de test, elaborate la testele anterioare de tip TIBER, dacă există.

(4) WT poate sprijini furnizorul TI, la cererea acestuia, cu informații care, într-un scenariu realist, ar putea fi obținute într-o perioadă rezonabilă de timp de un atacator avansat și persistent, în scopul de a reduce timpul necesar furnizorului TI pentru a formula un raport TI comprehensiv.

Art. 24. — (1) Pe baza raportului TI, furnizorul RT elaborează planul de testare a entității testate, care detaliază minimum trei scenarii de atac cibernetic, cu identificarea tacticilor, tehnicilor și procedurilor ce vor fi utilizate pentru a atinge țintele și obiectivele stabilite în sfera de cuprindere a testului.

(2) WT pune la dispoziția furnizorului RT rezumatele rapoartelor de test, elaborate la testele anterioare de tip TIBER.

(3) Scenariile de atac cibernetic trebuie să includă două scenarii de atac similare cu cele suferite anterior de instituții financiare și un scenariu nou, care să utilizeze elemente din mai multe atacuri reale.

(4) Suplimentar celor stabilite la alin. (3) vor fi incluse și scenariile executate cu succes în cadrul ultimului test de tip TIBER, realizat de către entitate conform prezentului regulament.

(5) Planul de testare trebuie să includă și modalități de acces fizic în cadrul entității testate și posibilitatea de a introduce în rețeaua entității testate dispozitive de către RT, respectiv orice obiect care în urma conectării cu infrastructura tehnică a entității testate favorizează atingerea obiectivelor de atac ale RT.

Art. 25. — (1) Testarea se realizează în mod controlat și documentat de către RT, cu respectarea planului de testare a entității testate, urmând toate fazele descrise în plan și utilizând doar personalul stabilit în contract.

(2) La cererea RT, WT poate decide să acorde sprijin echipei RT, prin furnizarea unor informații sau a unui cont de utilizator și/sau a unui echipament instalat în cadrul entității testate, în vederea depășirii unor obstacole într-un timp rezonabil de către echipa RT, având în vedere faptul că un atacator avansat și persistent ar fi avut suficient timp și resurse la dispoziție pentru a accesa infrastructura entității testate.

Art. 26. — RT trebuie să realizeze testarea etapizat, pe o perioadă de cel puțin 10 săptămâni de la momentul începerii testării efective, pentru a limita probabilitatea de detecție de către echipa BT, și trebuie să informeze imediat WT, prin canalele de comunicare agreate, în legătură cu atingerea fiecărui obiectiv.

Art. 27. — În situația în care BT detectează atacul cibernetic simulat în cursul testării și intenționează să alerteze cu privire la acest incident partenerii externi, autoritățile de resort sau alte entități ori să informeze publicul, WT trebuie să împiedice escaladarea incidentului, să păstreze confidențialitatea testului față de BT și să informeze imediat RT și BNR.

SECȚIUNEA a 3-a
Finalizarea testului și rapoartele de testare

Art. 28. — În cel mult 10 zile lucrătoare de la momentul finalizării testului și comunicării acestui fapt, în scris, către BNR de către WT, furnizorul RT, în colaborare cu furnizorul TI, elaborează raportul de test, în care include:

a) rezumatul testului;

b) obiectivele atinse și recomandările privind măsurile urgente care trebuie întreprinse de entitate în vederea întăririi rezilienței cibernetice;

c) lista cu toate acțiunile efectuate de către furnizorul RT în cadrul testului. Pentru fiecare acțiune, furnizorul RT documentează cel puțin, dar fără a se limita la acestea:

(i) tacticile, tehnicile și procedurile de atac utilizate;

(ii) vulnerabilitățile vizate sau exploatate;

(iii) condițiile necesare atacatorului pentru a îndeplini obiectivul de atac;
(iv) modul de declanșare a acțiunii pe echipamentele entității testate;
(v) efectul acțiunii pe dispozitivele din sistemul informatic al entității testate;
(vi) toate modificările efectuate în timpul acțiunii pe dispozitivele din sistemul informatic al entității testate;
(vii) modul în care se poate detecta acțiunea și/sau eventualele faze intermediare ale acțiunii pe dispozitivele din sistemul informatic al entității testate;
(viii) modul în care se poate/pot preveni acțiunea și/sau eventualele faze intermediare ale acțiunii pe dispozitivele din sistemul informatic al entității testate;
(ix) modul de răspuns indicat pentru BT în cazul acțiunii și/sau al eventualelor faze intermediare ale acțiunii pe dispozitivele din sistemul informatic al entității testate.

Art. 29. — (1) BT este informată de către WT despre test și, pe baza raportului de test, realizează raportul de acțiune al BT, care documentează toate acțiunile întreprinse de către BT, aflate în strânsă legătură cu acțiunile de atac efectuate de RT și descrise în raportul de test.

(2) Raportul de acțiune al BT este elaborat în colaborare cu RT și vizat de către WT.

Art. 30. — După finalizarea rapoartelor prevăzute la art. 28 și 29 se creează o echipă din care fac parte reprezentanți ai BT și reprezentanți ai RT, care vor participa la exercițiul de reconstituire a testului și vor colabora pentru a identifica:

a) dacă toate acțiunile RT au generat în sistemul informatic al entității testate înregistrări în jurnalele de sistem sau alte informații relevante pentru a indica un posibil atac în desfășurare, astfel încât BT să declanșeze procedurile de răspuns la incidente;

b) dacă toate acțiunile RT au generat alerte în sistemele de detecție și de prevenție implementate în sistemul informatic al entității testate, astfel încât BT să fie informată despre un posibil atac în desfășurare și să declanșeze procedurile de răspuns la incidente;

c) dacă măsurile de răspuns la incidente ale BT au fost eficiente și eficace;

d) dacă RT ar fi acționat în mod diferit, cât de adecvate ar fi fost măsurile luate de BT;

e) modalități de îmbunătățire a metodelor de detecție și răspuns pentru BT.

Art. 31. — (1) În baza recomandărilor din raportul de test se va realiza, în cel mult 30 de zile de la finalizarea testului, un plan de remediere, elaborat de către WT, care va fi remis, pentru punct de vedere BNR, în cel mult 10 zile de la finalizarea acestuia.

(2) Ulterior consultării BNR, planul de remediere va fi supus aprobării consiliului de administrație al entității testate, care va adresa toate deficiențele identificate în timpul testării și va stabili termenele de implementare a măsurilor de remediere.

(3) Entitatea are obligația să implementeze măsurile din planul de remediere la termenele stabilite.

(4) Conducerea entității testate va elabora un atestat privind realizarea testării conform cerințelor din prezentul regulament, care va fi remis, pentru aviz, către BNR și care va include informații referitoare la furnizorul TI și furnizorul RT.

(5) Entitatea informează BNR referitor la stadiul de implementare a planului de remediere, conform prevederilor art. 8 alin. (4).

CAPITOLUL IV
Măsuri și sancțiuni

Art. 32. — În situația în care BNR constată că cerințele prezentului regulament nu sunt respectate, poate stabili măsuri de remediere și termene de implementare entităților prevăzute la art. 1 alin. (2), în temeiul art. 407 din Ordonanța de urgență a Guvernului nr. 99/2006, aprobată cu modificări și completări prin Legea nr. 227/2007, cu modificările și completările ulterioare.

Art. 33. — În situația în care BNR constată că nu sunt respectate măsurile stabilite de către BNR și/sau că măsurile de remediere prevăzute în planul de remediere nu sunt implementate corespunzător, în termenele de implementare stabilite, BNR poate aplica sancțiuni entităților prevăzute la art. 1 alin. (2), în conformitate cu prevederile art. 408 din Ordonanța de urgență a Guvernului nr. 99/2006, aprobată cu modificări și completări prin Legea nr. 227/2007, cu modificările și completările ulterioare.

Art. 34. — Dispozițiile art. 32 și 33 nu se aplică instituțiilor menționate la art. 1 alin. (3).

CAPITOLUL V
Dispoziții finale

Art. 35. — Testările TIBER-RO pot fi inițiate începând cu 30 de zile de la data intrării în vigoare a prezentului regulament, dar nu mai târziu de 3 ani de la data intrării în vigoare a prezentului regulament.

Art. 36. — Anexele nr. 1 și 2 fac parte integrantă din prezentul regulament.

Art. 37. — Prezentul regulament se publică în Monitorul Oficial al României, Partea I, și intră în vigoare la data publicării.

Președintele Consiliului de administrație al Băncii Naționale a României,
Mugur Constantin Isărescu

București, 12 aprilie 2022.
Nr. 6.

ANEXA Nr. 1

Solicitare testare TIBER-RO

Data cererii	
Denumirea	
Sediul social	
Numele și datele persoanei de contact	
Perioada propusă pentru realizarea testării	

ANEXA Nr. 2

Cerințe, certificări și calificări aplicabile furnizorilor TI și RT

I. **Cerințe aplicabile furnizorilor TI**

A. Furnizorul TI (la nivel de persoană juridică) trebuie:

1. să prezinte cel puțin 3 referințe de la instituții din domeniul financiar, din țară sau din străinătate, pentru care a furnizat rapoarte de amenințări și vulnerabilități;

2. să dispună de o asigurare de răspundere civilă în vigoare pentru activitățile care au fost convenite în contract și/sau care decurg din conduite incorecte, neglijență etc.

B. Coordonatorul echipei TI trebuie:

1. să dețină cel puțin 5 ani de experiență în domeniul furnizării rapoartelor de amenințări și vulnerabilități, din care cel puțin 3 ani pentru domeniul financiar;

2. să prezinte un curriculum vitae actualizat din care să reiasă experiența în domeniu și cel puțin 3 referințe de la instituții financiare privind rapoartele de amenințări și vulnerabilități furnizate;

3. preferabil, să fie certificat cu cel puțin una dintre calificările prevăzute la pct. III;

4. în cazul în care cerința prevăzută la pct. 3 nu este îndeplinită, coordonatorul echipei TI trebuie să fie certificat cu cel puțin una dintre calificările prevăzute la pct. IV.

C. Membrii echipei TI trebuie:

1. să dispună de cel puțin 2 ani de experiență în domeniul furnizării rapoartelor de amenințări și vulnerabilități;

2. să prezinte un curriculum vitae actualizat din care să reiasă experiența în domeniu;

3. să fie certificați cu cel puțin una dintre calificările prevăzute la pct. IV;

4. echipa TI trebuie să aibă o compoziție multidisciplinară, vizând o gamă variată de abilități (de exemplu, OSINT — informații din surse deschise, HUMINT — informații din surse umane și cunoștințe geopolitice).

II. **Cerințe aplicabile furnizorilor RT**

A. Furnizorul RT (la nivel de persoană juridică) trebuie:

1. să prezinte cel puțin 5 referințe de la instituții din domeniul financiar, din țară sau din străinătate, privind teste de penetrare executate, preferabil de tip echipă RT;

2. să dispună de o asigurare de răspundere civilă în vigoare pentru activitățile care au fost convenite în contract și/sau care decurg din conduite incorecte, neglijență etc.

B. Coordonatorul RT trebuie:

1. să dețină cel puțin 5 ani de experiență în domeniul realizării testelor de penetrare a infrastructurii informatice, din care cel puțin 3 ani în domeniul financiar;

2. să prezinte un curriculum vitae actualizat din care să reiasă experiența în domeniu și cel puțin 3 referințe de la instituții financiare privind testele de penetrare realizate;

3. să fie certificat cu cel puțin una dintre calificările prevăzute la pct. III.

C. Membrii RT trebuie:

1. să dispună de cel puțin 2 ani de experiență în domeniul realizării testelor de penetrare a infrastructurii informatice, în domeniul financiar;

2. să prezinte un curriculum vitae actualizat din care să reiasă experiența în domeniu;

3. să fie certificați cu cel puțin una dintre calificările prevăzute la pct. IV;

4. RT trebuie să aibă o compoziție multidisciplinară, vizând o gamă variată de abilități (de exemplu, cunoștințe de afaceri, teste de penetrare, recunoaștere, informații despre amenințări, gestionarea riscurilor, inginerie socială, analiză a vulnerabilităților sau combinații ale acestora).

III. **Certificări ale coordonatorilor echipei TI sau ale coordonatorilor RT:**

Organism de certificare	Calificarea
CREST	CREST Certified Threat Intelligence Manager (CCTIM)
CREST	CREST Certified Simulated Attack Manager (CCSAM)
Offensive Security	Offensive Security Certified Expert (OSCE)
eLearnSecurity	eLearnSecurity Certified Penetration Tester eXtreme (eCPTX)

IV. **Calificări ale membrilor echipei TI sau ale membrilor RT:**

Organism de certificare	Calificarea
CREST	CREST Certified Simulated Attack Specialist (CCSAS)
ISACA	CSX Penetration & Vulnerability Tester Pathway
	CSX-P — Cybersecurity Practitioner Certification
(ISC)2	Certified Information Systems Security Professional (CISSP)
	Systems Security Certified Practitioner (SSCP)
SANS Institute — GIAC	GIAC Penetration Tester (GPEN)
	GIAC Web Application Penetration Tester (GWAPT)
	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)
	GIAC Mobile Device Security Analyst (GMOB)
	GIAC Assessing and Auditing Wireless Networks (GAWN)

Organism de certificare	Calificarea
Offensive Security	Offensive Security Certified Professional (OSCP)
	Offensive Security Wireless Professional (OSWP)
	Offensive Security Exploitation Expert (OSEE)
	Offensive Security Web Expert (OSWE)
eLearnSecurity	eLearnSecurity Certified Professional Penetration Tester (eCPPT)
	eLearnSecurity Web Application Penetration Tester (eWPT)
	eLearnSecurity Web Application Penetration Tester eXtreme (eWPTX)
	eLearnSecurity Mobile Application Penetration Tester (eMAPT)
	eLearnSecurity Certified eXploit Developer (eCXD)
Altele	EC-Council Certified Security Analyst (ECSA)
	Licensed Penetration Tester (LPT)
	Certified Ethical Hacker (CEH)

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, e-mail: concursurifp@ramo.ro, convocariaga@ramo.ro
Pentru publicări, încărcați actele pe site, la: https://www.monitoruloficial.ro/brp/

MONITORUL OFICIAL

5 948493 454410

Monitorul Oficial al României, Partea I, nr. 432/3.V.2022 conține 16 pagini. Prețul: 4 lei **ISSN** 1453—4495