GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2024

Chișinău

Cu privire la aprobarea proiectului de lege pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică)

Guvernul HOTĂRĂȘTE:

Se aprobă şi se prezintă Parlamentului spre examinare proiectul de lege pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică).

Prim-ministru **DORIN RECEAN**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării Dumitru ALAIBA

Ministrul justiției Veronica Mihailov-Moraru

Proiect

PARLAMENTUL REPUBLICII MOLDOVA

LEGE
pentru modificarea unor acte normative

(modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică)

Parlamentul adoptă prezenta lege organică.

Art. I. – Legea nr. 1456/1993 cu privire la activitatea farmaceutică (republicată în Monitorul Oficial al Republicii Moldova, 2005, nr. 59-61 art. 200), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 3 se completează cu alineatul (5), cu următorul cuprins:

„(5) Întreprinderile și instituțiile farmaceutice, identificate ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”

2. Articolul 9 se completează cu alineatul (3) cu următorul cuprins:

„(3) Persoanele care efectuează investigații în vederea creării medicamentelor noi, identificate ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”

3. Articolul 16 se completează cu alineatul (5) cu următorul cuprins:

„(5) Supravegherea și controlul de stat al respectării de către întreprinderile și instituțiile farmaceutice a obligațiilor stabilite la art. 3 alin. (5), precum și de către persoanele care efectuează investigații în vederea creării medicamentelor noi a obligațiilor stabilite la art. 9 alin. (3), se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

Art. II. – Articolul 4 din Legea ocrotirii sănătății nr. 411/1995 (Monitorul Oficial al Republicii Moldova, 1995, nr. 34. art. 373), cu modificările ulterioare, se completează cu alineatele (8) și (9), cu următorul cuprins:

„(8) Prestatorii de servicii medicale, identificați în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică ca furnizori de servicii, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative

de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.

(9) Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor prevăzute la alin. (8) se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică."

Art. III. – Codul navigației maritime comerciale al Republicii Moldova, aprobat prin Legea nr. 599/1999 (Monitorul Oficial al Republicii Moldova, 2001, nr. 1-4, art. 2), cu modificările ulterioare, se completează cu art. 9^1 cu următorul cuprins:

„Articolul 9^1. Asigurarea securității rețelelor și sistemelor informatice în navigația maritimă comercială

(1) Persoanele juridice care desfășoară activitatea de navigație maritimă comercială pentru transportul de mărfuri și/sau de pasageri, căpităniile porturilor, administrațiile porturilor maritime și întreprinderile și unitățile economice menționate la art. 80 alin. (2), precum și persoanele juridice care operează serviciul de trafic maritim, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia."

Art. IV. – Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, se modifică după cum urmează:

1. La articolul 3, noțiunea „securitate cibernetică" va avea următorul cuprins:

„*securitate cibernetică* – astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică";

2. La articolul 10, alineatul (1) va avea următorul cuprins:

„(1) În scopul asigurării securității sistemelor și resurselor informaționale de stat, autoritățile publice, instituțiile publice și alte entități de stat sunt responsabile de realizarea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere în aplicare a acesteia și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice."

3. La articolul 22, litera e) va avea următorul cuprins:

„e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene;”

Art. V. – Legea comunicațiilor electronice nr. 241/2007 (republicată în Monitorul Oficial al Republicii Moldova, 2017, nr. 399-410, art. 679), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 21 va avea următorul cuprins:

„**Art. 21.** – (1) În scopul asigurării securității și integrității rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, furnizorii sunt responsabili de realizarea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere în aplicare a acesteia și de alte acte normative care stabilesc cerințele specifice de asigurare a securității cibernetice.

(2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.

(3) În exercitarea supravegherii și controlului respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă în temeiul acestei legi informează, în termen de 5 zile, Agenția despre încălcările depistate și eventualele sancțiuni aplicate.”

2. Articolul 22 se abrogă.

Art. VI. – Punctul 1 din anexa la Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător (Monitorul Oficial al Republicii Moldova, 2012, nr. 181-184, art. 595), cu modificările ulterioare, se completează cu poziția 13^1 cu următorul cuprins:

13^1	Agenția pentru Securitate Cibernetică	Supravegherea și controlul de stat al respectării de către furnizorii de servicii a obligațiilor privind asigurarea securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative pentru punerea acesteia în aplicare

Art. VII. – Legea nr. 171/2012 privind piața de capital (Monitorul Oficial al Republicii Moldova, 2012, nr. 193-197, art. 665), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 41 se completează cu alineatele (9) și (10) cu următorul cuprins:

„(9) Societățile de investiții, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor care le revin conform acestei legi, a

actelor normative de punere a acesteia în aplicare și a altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(10) Supravegherea și controlul de stat al modului în care societățile de investiții îndeplinesc obligațiile prevăzute la alin. (9) se realizează de către autoritatea competentă în domeniul securității cibernetice la nivel național în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică".

2. Articolul 62 se completează cu alineatele (4) și (5) cu următorul cuprins:

„(4) Operatorii de piață, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor care le revin conform acestei legi, conform actelor normative de punere a acesteia în aplicare și conform altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(5) Supravegherea și controlul de stat al modului în care operatorii de piață îndeplinesc obligațiile respective se realizează de către autoritatea competentă în domeniul securității cibernetice la nivel național în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică."

Art. VIII. – Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova (Monitorul Oficial al Republicii Moldova, 2013, nr. 238-242, art. 672), cu modificările ulterioare, se completează cu articolul 37^1, cu următorul cuprins:

„**Articolul 37^1.** Asigurarea securității cibernetice

(1) Persoanele juridice care prestează servicii de transport de încărcături și/sau de pasageri și bagaje în domeniul transportului naval intern al Republicii Moldova și administrațiile portuare de stat ale transportului naval intern, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia."

Art. IX. – Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare (Monitorul Oficial al Republicii Moldova, 2014, nr. 60-65, art. 123), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 9 se completează cu litera e) cu următorul cuprins:

„e) autoritatea competentă la nivel național să exercite supravegherea și controlul de stat a respectării legislației în domeniul securității cibernetice.";

2. Articolul 9^1 se completează cu alineatul (4) cu următorul cuprins:

„(4) Supravegherea și controlul de stat al respectării de către operatori a obligațiilor stabilite la art. 15 alin. (3)[1] se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

3. Articolul 15 se completează cu alineatul (3)[1], cu următorul cuprins:

„(3)[1] Operatorii, identificați ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”

Art. X. – Articolul 14 din Legea comunicațiilor poștale nr. 36/2016 (Monitorul Oficial al Republicii Moldova, 2016, nr. 114-122, art. 225), cu modificările ulterioare, se completează cu alineatul (7)[2] cu următorul cuprins:

„(7)[2] Furnizorii de servicii poștale, identificați ca furnizori de servicii în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru realizarea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice pe care aceștia le utilizează la prestarea serviciilor. Supravegherea și controlul de stat al modului în care sunt îndeplinite obligațiile stabilite de prezentul alineat se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

Art. XI. – Legea nr. 209/2016 privind deșeurile (Monitorul Oficial al Republicii Moldova, 2016, nr. 459-471, art. 916), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 18 se completează cu alineatul (6) cu următorul cuprins:

„(6) Persoanele juridice care desfășoară activități de gestionare a deșeurilor, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru realizarea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice pe care aceștia le utilizează la prestarea serviciilor.”

2. Articolul 31 se completează cu alineatul (5) cu următorul cuprins:

„(5) Supravegherea și controlul de stat al modului în care persoanele juridice care desfășoară activități de gestionare a deșeurilor realizează obligațiile stabilite la art. 18 alin. (6) se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

Art. XII. – Articolul 16 din Legea nr. 102/2017 cu privire la dispozitivele medicale (Monitorul Oficial al Republicii Moldova, 2017, nr. 244-251, art. 389), cu modificările ulterioare, se completează cu alineatele (1^1) și (1^2), cu următorul cuprins:

„(1^1) Producătorii de dispozitive medicale, identificați ca furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.

(1^2) Supravegherea și controlul de stat al respectării de către producătorii de dispozitive medicale a obligațiilor stabilite la alin. $(1)^1$ se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

Art. XIII. – Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului (Monitorul Oficial al Republicii Moldova, 2017, nr. 364-370, art. 614), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 3 se completează cu noțiunile „obiectiv al infrastructurii critice” și „operator” cu următorul cuprins:

„*obiectiv al infrastructurii critice* – obiectiv de importanță vitală din domeniul administrației publice, tehnologiei informației și comunicațiilor electronice și poștale, de infrastructură, energetică, din sfera social-economică, sănătății, cultural-educativă, industrială, ecologică, din sistemul informațional al țării în ansamblu, din infrastructura complexului militar și de apărare al organelor de forță, de perturbarea sau distrugerea căruia poate provoca un impact negativ pentru siguranța, securitatea, bunăstarea socială și economică a statului, pierderi de servicii esențiale, pericol pentru viața, sănătatea oamenilor și efecte negative asupra mediului;

operator – ministerele, alte autorități sau instituții publice și persoanele juridice, indiferent de tipul de proprietate și forma juridică de organizare, care au în gestiunea lor obiective incluse în Nomenclatorul național al infrastructurii critice;”.

2. Articolul 20 se completează cu alineatele $(2)^1$ și $(2)^2$ cu următorul cuprins:

„$(2)^1$ Supravegherea și controlul de stat al respectării de către operatorii obiectivelor de infrastructură critică a obligațiilor de asigurare a securității cibernetice, prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia, se realizează de către autoritatea competentă în temeiul legii respective.

$(2)^2$ Autoritatea competentă în domeniul securității cibernetice informează, în termen de 5 zile, Centrul Antiterorist despre încălcările legislației constatate în

cadrul controlului exercitat asupra operatorilor obiectivelor de infrastructură critică privind modul în care aceștia respectă obligațiile de asigurare a securității cibernetice stabilite de actele normative menționate la alineatul (2)[1].”

Art. XIV. – Articolul 21 din Legea 174/2017 cu privire la energetică (republicată în Monitorul Oficial al Republicii Moldova, 2023, nr. 480-482, art. 849), cu modificările ulterioare, se modifică după cu urmează:

1. la alineatul (4) cuvintele „în conformitate cu prezenta lege și legile sectoriale” se substituie cu cuvintele „în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi”;

2. se completează cu alineatele (7)[1] și (7)[2], cu următorul cuprins:

„(7)[1] Întreprinderile energetice, identificate ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabile pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(7)[2] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.”

Art. XV. – Legea nr. 202/2017 privind activitatea băncilor (Monitorul Oficial al Republicii Moldova, 2017, nr. 434-439, art. 727), cu modificările ulterioare, se completează cu articolul 38[2], cu următorul cuprins:

„**Articolul 38[2]**. Gestionarea riscurilor de tehnologie a informației și a comunicațiilor (TIC), de securitate a informației și de continuitate a activității

(1) Fiecare bancă trebuie să dispună de personal, sisteme și servicii eficiente aferente tehnologiei informației și a comunicațiilor (TIC) ce asigură, de o manieră proporțională cu natura, amploarea și complexitatea riscurilor inerente activităților și modelului de afaceri, desfășurarea activităților băncii. În acest scop, banca stabilește roluri și responsabilități, aprobă și pune în aplicare o strategie TIC și de securitate a informației și planuri de acțiuni în vederea atingerii obiectivelor acesteia.

(2) Banca trebuie să stabilească un cadru de administrare a continuității activității, capabil să asigure capacitatea de a funcționa în mod continuu, cu asigurarea protejării tuturor informațiilor critice, inclusiv în vederea limitării pierderilor în cazul unei întreruperi severe a activității. În acest scop, banca va identifica riscurile de continuitate la care este expusă și va aproba și va pune în aplicare planuri de asigurare a continuității activității.

(3) Banca trebuie să dispună de un cadru de administrare a riscurilor aferente TIC și de securitate a informației care să conțină procese și proceduri pentru a asigura identificarea, analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al băncii.

(4) Banca trebuie să dispună de un cadru de administrare a securității informației care trebuie să definească principiile, normele și modalitățile de protejare a confidențialității, integrității și disponibilității datelor și informației băncii și ale clienților acesteia, instituind în baza acestuia măsuri pentru diminuarea nivelurilor riscurilor TIC și de securitate a informației la care este expusă.

(5) Banca trebuie să stabilească procese de revizuire a riscurilor, de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității.

(6) Cerințe specifice privind punerea în aplicare a alin. (1)-(5) se stabilesc în actele normative ale Băncii Naționale.

(7) În măsura în care gestionarea riscurilor TIC, de securitate a informației și de continuitate a activității nu este reglementată de dispozițiile prezentei legi și a actului normativ menționat la alineatul (6), acestea se completează cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și de actele normative de punere a acesteia în aplicare.

(8) Supravegherea și controlul modului în care băncile realizează obligațiile stabilite de prezentul articol se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Banca Națională a Moldovei, în conformitate cu actul normativ prevăzut la alineatul (6) și actele normative de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică.”

Art. XVI. – Articolul 8 din Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate (Monitorul Oficial al Republicii Moldova, 2018, nr. 295-308, art. 452), cu modificările ulterioare, se completează cu alineatul (4) cu următorul cuprins:

„(4) Realizarea obligației stabilite la alineatul (3) nu scutește participanții la schimbul de date, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, de realizarea obligațiilor de notificare stabilite de această lege.”

Art. XVII. – Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar (Monitorul Oficial al Republicii Moldova, 2018, nr. 441-447, art. 715), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 17 alineatul (2) se completează cu litera b^2) cu următorul cuprins:

„b^2) pentru personalul Agenției pentru Securitate Cibernetică – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific;”.

2. La anexa nr. 3, notele la tabelul 2 se completează cu punctul 17 cu următorul cuprins:

„**17.** Clasele de salarizare pentru funcțiile publice de conducere și de execuție din cadrul Direcției răspuns la incidente și crize cibernetice a Agenției pentru Securitate Cibernetică se majorează față de cele stabilite în tabel pentru aceste funcții, după cum urmează:

- cu 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”;

- cu 25 de clase succesive – pentru funcțiile publice de execuție.”

Art. XVIII. – Legea nr. 277/2018 privind substanțele chimice (Monitorul Oficial al Republicii Moldova, 2019, nr. 49-58, art. 109), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 11 se completează cu alineatul (5) cu următorul cuprins:

„(5) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 12 alin. (6) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.”

2. Articolul 12 se completează cu alineatul (6) cu următorul cuprins:

„(6) Furnizorul unei substanțe sau al unui amestec, identificat ca furnizor de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, este responsabil pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.”

Art. XIX. – Legea nr. 306/2018 privind siguranța alimentelor (Monitorul Oficial al Republicii Moldova, 2019, nr. 59-65, art. 120), cu modificările ulterioare, se modifică după cum urmează:

1. Articolul 7 se completează cu alineatul $(13)^1$ cu următorul cuprins:

„$(13)^1$ Întreprinderile din domeniul alimentar, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor privind asigurarea securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice.”

2. Articolul 8 se completează cu alineatul $(9)^1$, cu următorul cuprins:

„$(9)^1$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 7 alin. $(13)^1$ se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.”

Art. XX. – Articolul 22 din Legea nr. 192/2019 privind securitatea aeronautică (Monitorul Oficial al Republicii Moldova, 2019, nr. 400-406, art. 356), cu modificările ulterioare, se modifică după cum urmează:

1. Alineatul (1) va avea următorul cuprins:

„(1) Pentru asigurarea securității cibernetice în domeniul aviației civile sunt responsabili operatorii aeronautici, entitățile aeronautice, autoritatea administrativă de implementare și realizare a politicilor în domeniul aviației civile și autoritatea competentă în domeniul securității cibernetice în limitele stabilite de cadrul normativ.”

2. Se completează cu alineatele (3) și (4) cu următorul cuprins:

„(3) Operatorii aeronautici și entitățile aeronautice, identificați ca furnizori de servicii în temeiul Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(4) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (3) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.”

Art. XXI. – Codul transportului feroviar al Republicii Moldova nr. 19/2022 (Monitorul Oficial al Republicii Moldova, 2022, nr. 45-52, art. 57) se modifică după cum urmează:

1. Articolul 26 se completează cu alineatul $(1)^1$ cu următorul cuprins:

„$(1)^1$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la art. 89 alin. $(3)^1$ se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.”

2. Articolul 89 se completează cu alineatul $(3)^1$ cu următorul cuprins:

„$(3)^1$ Administratorul infrastructurii și întreprinderile feroviare, identificați ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de această lege, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.”

Art. XXII. – Articolul 39 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere (Monitorul Oficial al Republicii Moldova, 2022, nr. 170-176, art. 317) va avea următorul cuprins:

„**Articolul 39.** Asigurarea securității cibernetice de către prestatorii de servicii de încredere

(1) În scopul asigurării securității rețelelor și a sistemelor informatice utilizate la prestarea serviciilor de încredere, prestatorii de servicii de încredere sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de Legea nr. 48/2023 privind securitatea cibernetică, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

(2) Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alin. (1) se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și actele normative de punere în aplicare a acesteia.

(3) În exercitarea supravegherii și controlului respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă în temeiul acestei legi informează, în termen de 5 zile, organul de supraveghere și control despre încălcările depistate și eventualele sancțiuni aplicate.”

Art. XXIII. – Prezenta lege intră în vigoare la data de 1 ianuarie 2025, cu excepția prevederilor art. XVII care intră în vigoare la data publicării legii.

Președintele Parlamentului

Notă informativă
la proiectul de lege pentru modificarea unor acte normative
(aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică)

1. Denumirea autorului și, după caz, a participanților la elaborarea proiectului
Proiectul a fost elaborat de Ministerul Dezvoltării Economice și Digitalizării, cu suportul proiectului „Asistență rapidă Republicii Moldova în domeniul securității cibernetice” finanțat de Comisia Europeană și implementat de Academia de Guvernare Electronică din Estonia.
2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite
1. Condițiile ce au impus elaborarea proiectului de act normativ La data de 16 martie 2023 Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, care urmează să intre în vigoare la data de 1 ianuarie 2025. Legea are ca obiectiv general să asigure legalitatea în spațiul cibernetic prin reglementarea principalelor elemente indispensabile implementării unui model de guvernanță eficient la nivel național în vederea protecției și asigurării securității rețelelor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Un instrument juridic esențial asumat în procesul reglementării acestui domeniu a constituit legislația Uniunii Europene, inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană, prin Legea respectivă asigurându-se, deși doar parțial, armonizarea cadrului normativ național la prevederile Directivei NIS2[1] și, implicit, a unor elemente esențiale ale Directivei NIS1[2]. Modul de realizare a procesului de armonizare este reflectat în tabelul[3] de concordanță, parte a dosarului de însoțire a proiectului Legii privind securitatea cibernetică, prezentat Parlamentului de către Guvern. Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal: ***a)*** stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliul coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu; ***b)*** desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național; ***c)*** reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile; ***d)*** stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ce privește obligațiile de implementare a măsurilor de securitate și în ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și împuternicirea autorității

[1] ***Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului*** din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148;
[2] ***Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului*** din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;
[3] https://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/6386/language/ro-RO/Default.aspx

competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

e) determinarea cadrului normativ primar pentru identificarea persoanelor juridice ca fiind furnizori de servicii esențiale, împuternicire atribuită de asemenea autorității respective, ca parte componentă a funcției de supraveghere, etc.

Potrivit prevederilor Legii privind securitatea cibernetică, Guvernul este învestit cu competență de intervenție, de diferită natură (normativă, organizatorică și tehnică), pe un șir de chestiuni în vederea punerii în aplicare a prevederilor acesteia, dintre care în mod special ținem să le evidențiem pe cele care sunt pertinente obiectului de reglementare a proiectului propus spre avizare și anume:

a) aprobarea listei sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare și care vor cădea sub incidența prevederilor legii și a cadrul metodologic de identificare a acestora (art. 4 alin. (2));

b) desemnarea/constituirea, reglementarea modului de organizare și funcționare, a structurii și efectivului-limită a entității care va exercita funcțiile autorității competente (art. 7 alin. (1));

c) modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 18 alin. (5));

d) modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 19 alin. (5)).

În același context, trebuie de remarcat că și articolul 23 din Legea nr. 48/2023 cuprinde norme juridice cu caracter tranzitoriu care stabilesc un set de sarcini Guvernului, orientate spre organizarea executării prevederilor Legii. Una dintre aceste sarcini rezidă în obligația Guvernului să elaboreze și să prezinte Parlamentului un proiect de lege pentru modificarea unor acte normative (legi), în vederea aducerii în concordanță cu Legea menționată a cadrului normativ relevant.

2. Finalitățile urmărite

După cum s-a menționat mai sus proiectul de lege are ca obiectiv general să aducă în concordanță cu Legea privind securitatea cibernetică prevederile legale existente. În acest context finalitățile urmărite prin adoptarea actului normativ sunt determinate de diferitele categorii de intervenții legislative propuse în proiect și constau în principal în următoarele:

a) asigurarea interconexiunii dintre normele Legii privind securitatea cibernetică și cele cuprinse în legile sectoriale care reglementează activitatea viitorilor furnizori de servicii și eliminarea/revizuirea unor prevederi care ar putea suscita interpretări echivoce sau contradictorii în procesul aplicării legii: În temeiul art. 4 alin. (2) din Legea nr. 48/2023, Guvernul urmează să adopte lista sectoarelor, subsectoarelor, tipurilor și categoriilor de furnizori de servicii care vor cădea sub incidența prevederilor acestei legi și metodologia de identificare a persoanelor juridice ca fiind furnizori de servicii. Ca punct de pornire pentru determinarea conținutului listei menționate îl constituie anexele nr.1 și nr.2 la Directiva NIS2. Acestea cuprind sectoarele cu o importanță critică ridicată și, respectiv, alte sectoare de importanță critică. Urmare a unei analize și cercetării preliminare comparative a cadrului legislativ european sectorial de referință, menționat în aceste anexe, și cel național, au fost determinate legile sectoriale în care sunt necesare și, în consecință, se propun în proiectul de lege, intervenții normative pentru a exclude eventuale ambiguități în interpretarea ulterioară a aplicabilității normelor juridice specifice anumitor sectoare în coroborare cu cele relevante din Legea securității cibernetice. Aceste intervenții vizează responsabilitatea viitorilor furnizori de servicii în ce privește îndeplinirea obligațiilor de asigurare a securității cibernetice și, corespunzător, competența de supraveghere și control a autorității naționale competente în materie de securitate cibernetică în ce privește modul în care aceste obligații sunt îndeplinite.

b) finalizarea instituirii cadrului normativ primar necesar stabilirii modelului de guvernanță în domeniul securității cibernetice la nivel național: Proiectul de lege include prevederi de completare a cadrului legal existent cu norme juridice care au ca scop punerea în aplicare a unor reglementări ale Legii securității cibernetice în mod special în ce privește asigurarea legalității organizării și funcționării viitoarei autorități competente în domeniul securității cibernetice, inclusiv în ce privește exercitarea competenței de organ de control și agent constatator conform prevederilor legislației contravenționale.

3. Descrierea gradului de compatibilitate pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

După cum s-a menționat și mai sus, proiectul de lege propus spre consultare publică și avizare are ca obiectiv general aducerea legislației în concordanță cu prevederile Legii nr. 48/2023 privind securitatea cibernetică. Ultima constituie actul normativ principal prin care prevederile legislației naționale sunt armonizate la elementele esențiale în domeniul securității cibernetice cuprinse de Directivele NIS1 și NIS2.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

În proiectul de lege sunt propuse modificări la 23 de legi, care pot fi divizate, în funcție de factorii ce le determină, finalitățile pe care le urmăresc și efectele pe care le vor produce, în următoarele categorii:

1. **Prima categorie de modificări propuse în proiect (art. IV, VI, VII, XV, XVI și XXII)** constau în necesitatea finalizării constituirii cadrului juridico-normativ, care va fi baza stabilirii și asigurării funcționalității depline a modelului de guvernanță în domeniul securității cibernetice la nivel național. Aceste modificări vizează în principal clarificarea unor prevederi legale ce delimitează competența în domeniul securității cibernetice, ajustându-le la cadrul normativ ce reglementează competența și modul de organizare a administrației publice centrale de specialitate. De asemenea, această categorie de reglementări propuse în proiect sunt determinate de necesitatea constituirii autorității administrative care va exercita atribuțiile autorității competente în temeiul Legii nr. 48/2023 privind securitatea cibernetică.

Modificările propuse în **articolul IV** din proiectul de lege vizează ***Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat*** și au ca obiectiv să clarifice definiția noțiunii de securitate cibernetică și să aducă prevederile legii în cauză în concordanță cu prevederile Legii privind securitatea cibernetică.

Astfel, **la pct. 1** definiția actuală a noțiunii de securitate cibernetică este substituită cu o normă de trimitere la prevederea corespunzătoare din Legea nr. 48/2023. Reiterăm că redacția definiției acestei noțiuni, dată în Legea nr. 48/2023, este expresia procesului de armonizare a legislației naționale la Directiva NIS2. Având această premisă, uniformizarea terminologică în acest domeniu ar trebui să aibă ca punct de reper anume Legea privind securitatea cibernetică. Mai mult, definiția noțiunii de *securitate cibernetică*, dată actualmente în Legea nr. 467/2003 este în esență o compilare generică a două noțiuni cu care operează Directiva NIS2 și, implicit, Legea nr. 48/2023: *securitate cibernetică* și *securitate a rețelelor și sistemelor informatice*. În primul caz, urmează a fi înțelese *„activități necesare pentru protejarea rețelelor și sistemelor informatice, a utilizatorilor unor astfel de sisteme și a altor persoane expuse amenințărilor cibernetice”,* iar în cel de-al doilea *– „capacitatea rețelelor și sistemelor informatice de a rezista, la un anumit nivel de încredere, oricărei acțiuni care ar putea compromite disponibilitatea, autenticitatea, integritatea sau*

confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor oferite de rețelele și/sau de sistemele informatice respective sau accesibile prin intermediul acestora".

La pct. 2 redacția nouă a alineatului (1) din art. 10 al Legii nr 467/2003 se propune a fi revizuită corelând-o cu prevederile Legii privind securitatea cibernetică atât din perspectiva responsabilității persoanelor juridice de drept public de a asigura securitatea rețelelor și sistemelor pe care le dețin, cât și din punct de vedere terminologic.

La pct. 3 menționăm că în rezultatul ședinței comune din data de 23.01.2024 cu participarea SIS, AGE, STISC MDED și Consilierul Președintelui Republicii Moldova în domeniul apărării și securității naționale Stanislav Secrieru, s-a coordonat următoarea redacție a articolului 22, litera e) a Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat:

„e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene;".

La **Articolul VI** din proiectul de lege se propune completarea punctului 1 al anexei la ***Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător*** care cuprinde *Lista organelor de control și domeniile aferente acestora* cu o poziție nouă dedicată Agenției pentru Securitate Cibernetică. În conformitate cu art. 7 alin. (3) lit. e) autoritatea competentă în domeniul securității cibernetice urmează să exercite funcțiile de supraveghere și control de stat al modului în care furnizorii de servicii respectă obligațiile ce le revin conform Legii privind securitatea cibernetică. În conformitate cu art. 4 alin. $(2)^1$ din Legea privind controlul de stat asupra activității de întreprinzător au dreptul să inițieze și să desfășoare controlul doar autoritățile/instituțiile publice stabilite în anexa la respectiva lege, în limitele corespunzătoare. Prin urmare, această listă este una exhaustivă și pentru a evita interpretări ulterioare în detrimentul aplicării prevederilor Legii privind securitatea cibernetică este necesară completarea pct. 1 din anexa respectivă.

Articolul XVI conține propuneri de modificare a articolului 8 din ***Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate***. Art. 8 alin. (3) din legea respectivă prevede că participanții la schimbul de date sunt obligați să informeze autoritatea competentă despre vulnerabilitățile și incidentele de securitate în utilizarea platformei de interoperabilitate imediat sau în termen de cel mult 2 zile lucrătoare din momentul depistării acestora. Cel mai probabil un număr important dintre participanții la platforma de interoperabilitate vor avea calitatea de furnizor de servicii în sensul Legii privind securitatea cibernetică. Norma de concretizare propusă în redacția alin. $(3)^1$ are scopul de a exclude orice echivoc în interpretările ulterioare a prevederilor actualului alineat (3) din art. 8 în raport cu prevederile care stabilesc obligații de notificare în baza Legii nr. 48/2023. În același timp, considerăm oportună păstrarea alineatului (3) din art. 8 în textul Legii nr. 142/2018, în primul rând, pentru că Instituția publică „Agenția de Guvernare Electronică", urmând să aibă calitatea de furnizor de servicii potrivit Legii nr. 48/2023, trebuie să păstreze instrumentele existente în gestionarea vulnerabilităților sau incidentelor de securitate a platformei pe care o deține.

La articolul XVII din proiectul de lege sunt propuse completări ale art. 17 din ***Legea nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar.*** Potrivit art. 7 alin. (1) și art. 23 alin. (2) lit. b) din Legea nr. 48/2023 privind securitatea cibernetică, Guvernul urmează să desemneze sau să instituie autoritatea competentă în domeniul securității cibernetice și să o facă funcțională către data de 27 ianuarie 2024 (9 luni din data publicării legii). După cum am menționat mai sus, pentru realizarea acestei sarcini a Guvernului, Ministerul Dezvoltării Economice și Digitalizării a elaborat proiectul de hotărâre a Guvernului „Cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică". În ședința sa de la data de 21 decembrie,

Guvernul a aprobat acest proiect. Potrivit analizei de impact[4] , opțiunea recomandată (de bază) propune constituirea acestei entități ca autoritate administrativă subordonată ministerului, angajații urmând a avea statut de funcționar public. O provocare serioasă în asigurarea eficienței în funcționarea unei astfel de entități este salarizarea personalului. Nivelul acestei salarizări trebuie să constituie un compromis dintre obiectivele pe care și le propune statul în asigurarea unei protecții adecvate a infrastructurii informaționale critice, a rezilienței acesteia și asigurarea competitivității pe piața muncii a salariaților acestei entități, în mod special cu mediul privat. Pentru realizarea acestui compromis este necesar să fie instituite mecanisme eficiente de motivare a personalului viitoarei entități, astfel încât să se diminueze la maxim riscurile legate de potențialul unui înalt flux de cadre. Nu mai puțin important în atingerea acestui compromis este și necesitatea de a extinde potențiala bază de recrutare a viitorilor angajați cu calificarea suficientă și necesară realizării obiectivelor acestei organizații. Elementul realist care ar putea da rezultate palpabile în acest sens este o salarizare motivantă care ar descuraja scurgerea specialiștilor calificați și, implicit, creșterea costurilor ce țin de instruirea celor noi. Or, conform estimărilor[5] Agenției Europene pentru Securitate Cibernetică (ENISA) *„este obișnuit să se cheltuiască între 3 000 și 10 000 EUR pe formarea personalului, pe persoană și pe an”*.

Algoritmul aplicat la stabilirea salariilor angajaților viitoarei entități va avea trei parametri: valoarea de referință stabilită prin legea bugetară anuală, coeficientul corespunzător clasei de salarizare pentru funcțiile publice respective și sporul cu caracter specific. Astfel, urmare a discuțiilor cu reprezentanții Ministerului Finanțelor s-a ajuns la un compromis de aplicare a acestui algoritm după cum urmează: salariile personalului Direcției răspuns la incidente și crize cibernetice a ASC vor fi constituite după cum urmează: pentru funcțiile publice de conducere (șef și șef adjunct) – valoarea de referință (VR) 3600 MDL*coeficientul prevăzut pentru +15 clase de salarizare față de cele prevăzute în tabelul respectiv din Legea nr. 270/2017 pentru categoria respectivă de funcții + 120% sporul cu caracter specific, iar pentru funcțiile de execuție din cadrul aceleiași subdiviziuni datele algoritmului de calcul sunt aceleași, cu excepția majorării claselor de salarizare nu cu 15 clase succesive, ci cu 25. Pentru restul personalului din viitoarea entitate salariile vor fi constituite după cum urmează: VR 2500 MDL*coeficientul prevăzut în tabelul respectiv din Legea nr. 270/2017 pentru categoria respectivă de funcții + 120% sporul cu caracter specific. Reieșind din acest algoritm de calcul în proiect sunt propuse modificări ale art. 17 din legea nr. 270/2018 și în notele la tabelul respectiv al anexei nr. 3 la această lege. În valori absolute aceasta ar în semna că salariile personalului de execuție CSIRT va constitui în jur de 51 mii lei, iar al șefului și șefului adjunct – în jur de 82 mii lei și, respectiv, 76 mii lei. În ce privește ceilalți angajați ai autorității, directorul și directorul adjunct vor avea în jur de 57 mii lei și, respectiv, 53 mii lei, ceilalți funcționari cu funcții de conducere (șef direcție, șef secție, șef serviciu) – între 30 mii lei – 40 mii lei, iar personalul de execuție – între 21 mii lei și 28 mii lei.

Articolul XXIII include norme de intrare în vigoare și tranzitorii. Conform acestui articol modificările propuse în proiectul de lege ar urma să intre în vigoare la data de 1 ianuarie 2025, adică odată cu intrarea în vigoare a prevederilor Legii nr. 48/2023 privind securitatea cibernetică. Excepție fac prevederile art. XVII, care ar urma să intre în vigoare la data publicării legii. Intrarea în vigoare a modificărilor la Legea nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar este determinată de necesitatea asigurării condițiilor legale pentru instituirea și asigurarea funcționalității de către Guvern a autorității competente în domeniul securității cibernetice.

[4] https://particip.gov.md/ro/document/stages/anunt-de-initiere-a-procesului-de-elaborare-a-proiectului-hotararii-de-guvern-cu-privire-la-constituirea-organizarea-si-functionarea-agentiei-nationale-pentru-securitate-cibernetica/10814;

[5] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc, pag.18;

2. A doua categorie de norme, cuprinse la articolele I – III, V, VII – XIV și XVIII – XXII, rezidă în completarea legilor sectoriale, care au ca obiect de reglementare activități din domenii și subdomenii, corespondente sectoarelor sau subsectoarelor enumerate în anexele I și II ale Directivei NIS2, inclusiv statutul persoanelor juridice ce urmează a fi identificate de către autoritatea competentă în domeniul securității cibernetice ca furnizori de servicii. Reiterăm că în conformitate cu art. 4 alin. (2) din Legea nr. 48/2023, lista sectoarelor și subsectoarelor, dar și tipurile și categoriile de persoane juridice care urmează să cadă sub incidența prevederilor Legii privind securitatea cibernetică, precum și cadrul metodologic de identificare a acestora, urmează a fi adoptate de către Guvern. Astfel, pentru a exclude eventuale interpretări ambigui sau contradictorii, ar fi judicios ca aceste legi sectoriale să fie completate cu prevederi generale privind limitele competenței de supraveghere și control, ce urmează a fi exercitată de autoritatea competentă, și obligațiile exprese de asigurare a securității cibernetice de către diferitele categorii de furnizori de servicii. În același timp, această categorie de modificări constituie rezultatele analizei comparative dintre tipologia furnizorilor de servicii esențiale, oferită de anexele I și II ale Directivei NIS2 și tipologia persoanelor juridice din sectoarele sau subsectoarele respective, reglementată în legislația națională.

Astfel, în **articolele I, II și XII** sunt propuse un set de completări la legile care reglementează **sectorul sănătății**. Acesta este unul dintre sectoarele cu o importanță critică ridicată, menționat în anexa I la Directiva NIS2 și cuprinde 5 tipuri de entități esențiale, dintre acestea 4 sunt relevante pentru Republica Moldova: *furnizorii de servicii medicale, entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor, entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice și entitățile care fabrică dispozitive medicale considerate a fi esențiale în contextul unei urgențe de sănătate publică (lista dispozitivelor esențiale pentru urgența de sănătate publică)*.

Cu referire la **articolul I** din proiectul de lege menționăm că potrivit anexei nr. I pct. 5 din Directiva NIS2, *entitățile care desfășoară activități de cercetare și dezvoltare a medicamentelor* și *entitățile care fabrică produse farmaceutice de bază și preparate farmaceutice* sunt alte două tipuri de entități care au o importanță critică ridicată. În Republica Moldova activitățile de cercetare și dezvoltare a medicamentelor și cele de fabricare sunt reglementate de ***Legea nr. 1456/1993 cu privire la activitatea farmaceutică***. Legea respectivă nu conține noțiuni și definițiile acestora similare celor utilizate în textul relevant al anexei I la Directiva NIS2. Totuși, în ce privește tipul de entități care desfășoară activități de cercetare și dezvoltare a medicamentelor, Legea respectivă în art. 9, care cuprinde prevederi generale privind cercetările farmacologice și farmaceutice, stabilește la alin. (2) spectrul de entități care pot efectua investigații (adică cercetări) în vederea creării medicamentelor noi, acestea fiind *„instituții de cercetări științifice, științifice de producție, științifico-practice, de învățământ, precum și de către persoane fizice”*. Având în vedere că Legea privind securitatea cibernetică cuprinde în domeniul său de aplicare doar entități cu personalitate juridică, în proiectul de lege se propune completarea acestui articol cu un alineat nou care va stabili în responsabilitatea persoanelor juridice care efectuează investigații în vederea creării medicamentelor noi implementarea obligațiilor de asigurare a securității cibernetice. Această responsabilitate se va răsfrânge însă doar asupra acelor persoane juridice care vor fi identificate ca fiind furnizori de servicii în sensul Legii nr. 48/2023 de către autoritatea competentă respectivă. În ce privește cealaltă categorie menționăm că Legea nr. 1456/1993 operează cu termenul general de *întreprinderi și instituții farmaceutice* (art. 3 alin. (1)), care include *întreprinderile farmaceutice industriale, întreprinderile (laboratoarele) de microproducție farmaceutică, laboratoarele de control al calității medicamentelor, depozitele farmaceutice, farmaciile, instituțiile de cercetări farmaceutice, instituțiile farmaceutice științifico-practice*. Astfel, în proiect se propune ca acest articol să fie completat cu prevederi similare categoriei examinate anterior. Totodată, art. 16 urmează a fi completat cu prevederi care stabilesc expres competența în materie de supraveghere și control

al modului în care aceste categorii de persoane juridice își realizează obligațiile de asigurare a securității cibernetice.

Categoria corespondentă în legislația națională pentru furnizorii de servicii medicale sunt prestatorii de servicii medicale, categorie reglementată în principal de art. 4 din ***Legea ocrotirii sănătății, nr. 411/1995***. În **articolul II** din proiectul de lege se propune completarea acestui articol cu prevederi care ar stabili expres responsabilitatea prestatorilor de servicii medicale de a realiza obligațiile de asigurare a securității cibernetice stabilite de actele normative din domeniul securității cibernetice. Totuși, aceste obligații urmează să se răsfrângă doar asupra prestatorilor de servicii medicale care vor fi identificați ca furnizori de servicii de către autoritatea competentă în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică și cu cadrul metodologic subsidiar acesteia.

În ce privește **articolul XII** din proiectul de lege, relevăm că al patrulea tip de entități din sectorul sănătății, menționate în anexa I pct. 5 din Directiva NIS2, sunt *entitățile care fabrică dispozitive medicale considerate a fi esențiale în contextul unei urgențe de sănătate publică (lista dispozitivelor esențiale pentru urgența de sănătate publică).* Corespondentul acestui tip de entități în legislația Republicii Moldova este oferit de ***Legea nr. 102/2017 cu privire la dispozitivele medicale***. Termenul general utilizat în lege, deși nedefinit, este cel de producător de dispozitive medicale. Completările propuse la această lege vizează articolul 16 care reglementează „Vigilența dispozitivelor medicale", adică responsabilitățile subiecților legii în ce privește anumite complicații sau incidente care vizează dispozitivele medicale. Reieșind din prevederile anexei I, pct.5 liniuța a cincea din Directiva NIS2, criteriile definitorii specifice, de rând cu cele generale (personalitate juridică, dimensiunea persoanei juridice – cel puțin mijlocie de exemplu), care vor trebui să stea la baza procesului de identificare a acestui tip de furnizori de servicii sunt a) să desfășoare activitatea de fabricare/producere și b) dispozitivele medicale pe care le fabrică trebuie să fie esențiale în contextul unei urgențe de sănătate publică, adică să fie incluse în lista dispozitivelor esențiale pentru urgența de sănătate publică (în sensul articolului 22 din Regulamentul (UE) 2022/123[6]). Având în vedere faptul că Legea nr. 10/2009 privind supravegherea de stat a sănătății publice nu prevede adoptarea unei astfel de liste, pentru finalizarea procesului de identificare a furnizorilor de servicii de acest tip vor fi necesare intervenții normative și/sau organizatorice din partea autorității administrației publice centrale de specialitate responsabile de realizarea politicii statului în acest domeniu.

Alte două tipuri de entități care cad sub incidența completărilor propuse în art. XII, din categoria celor importante, adică cu activități în alte sectoare critice (anexa II la Directiva NIS2), sunt a) entitățile care fabrică dispozitive medicale și b) cele care fabrică dispozitive medicale in vitro. Aceste două categorii de entități, după cum de altfel am menționat-o mai sus intră în categoria legală de producători de dispozitive medicale, în sensul Legii nr. ***nr. 102/2017.***

Articolele III, VIII, XX și XXI conțin modificări la acte normative care reglementează relații sociale din subdomenii ale domeniului transporturilor. ***Sectorul transporturilor*** este un alt sector calificat de Directiva NIS2 ca fiind unul de o importanță critică ridicată. Acest sector este divizat în anexa I a directivei în patru subsectoare: aerian, feroviar, pe apă (maritim) și rutier. Dintre acestea, completările propuse în **art. III și VIII** vizează actele normative primare care reglementează în Republica Moldova subsectorul de transport pe ape, menționat la pct. 2 lit. c) din anexa I la Directiva NIS2. Algoritmul acestor completări este același ca și în cazul prevederilor proiectului examinate mai sus: instituirea obligațiilor de asigurare a securității cibernetice pentru anumite

[6] Regulamentul (UE) 2022/123 al Parlamentului European și al Consiliului din 25 ianuarie 2022 privind consolidarea rolului Agenției Europene pentru Medicamente în ceea ce privește pregătirea pentru situații de criză în domeniul medicamentelor și al dispozitivelor medicale și gestionarea acestora (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02022R0123-20220131)

categorii de subiecți ai legii în corelare cu atribuirea expresă a exercitării către autoritatea competentă în domeniul securității cibernetice a funcțiilor de supraveghere și control de stat al modului în care aceste obligații sunt realizate, algoritm care va asigura o interconexiune cu Legea privind securitatea cibernetică. Anexa I pct. 2 lit. c) din Directiva NIS2 evidențiază în acest subsector patru tipuri de entități:

- companiile de transport de mărfuri și pasageri pe ape interioare, maritime și de coastă (fără a include navele individuale operate de companiile respective);
- organele de gestionare a porturilor, inclusiv instalațiile portuare ale acestora;
- entitățile care realizează lucrări și operează echipamente în cadrul porturilor;
- operatorii de servicii de trafic maritim.

Astfel pentru determinarea primului tip de entități, în redacția alin. (1) al art. 9^1 propus în **articolul III** din proiect, având în vedere că actul normativ în speță nu definește termenii utilizați în actul legislativ european, se propune utilizarea unei formule generale pentru această categorie - *„persoane juridice care desfășoară activitatea de navigație maritimă comercială pentru transportul de mărfuri și/sau de pasageri*", bazată în principiu pe conținutul noțiunii de navigație maritimă comercială, a cărei definiție este dată în art. 1 din ***Codul navigației maritime comerciale***. Bineînțeles, această categorie de persoane juridice urmează să fie identificată de autoritatea competentă în domeniul securității cibernetice în baza cadrului metodologic aprobat de Guvern. Același modus operandi este propus și în ce privește completările de la **articolul VIII**, redacția fiind expresia terminologiei utilizate de ***Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova*** și anume – *persoanele juridice care prestează servicii de transport de încărcături și/sau de pasageri și bagaje.*

Al doilea și al treilea tip de entități își are corespondentul în legislația națională în persoana administrației portului maritim, reglementată în principal la art. 80 din Codul navigației maritime comerciale, a întreprinderilor menționate la alin. (2) din același articol, cărora administrațiile porturilor le dau în arendă anumite construcții portuare pentru realizarea anumitor activități/operațiuni portuare, precum și administrațiile portuare de stat ale transportului naval intern, reglementate la art. 51 din ***Legea nr. 176/2013*** (completările propuse la articolul IX din proiect).

În ce privește ultimul tip de entități – *operatorii de servicii de trafic maritim* – în legislația Republicii Moldova noțiunea de servicii de trafic maritim nu este definită de cadrul legal primar, ci doar de cel secundar – Regulamentul privind stabilirea Sistemului de informare și monitorizare a traficului navelor maritime, aprobat prin Hotărârea Guvernului nr. 413/2021. Reieșind din prevederile acestui Regulament, operator al serviciului de trafic maritim în jurisdicția teritorială și de competență a Republicii Moldova este Agenția Navală care este o persoană juridică de drept public și va cădea sub incidența Legii securității cibernetice reieșind din această calitate. Totuși având în vedere probabilitatea evoluției relațiilor sociale în acest domeniu în proiect se propune la art. III includerea și categoriei de entități – persoane juridice care operează serviciul de trafic maritim.

Prevederile **art. XX** din proiectul de lege au ca obiectiv completarea art. 22 din ***Legea nr.192/2019 privind securitatea aeronautică***. Acest articol actualmente are ca obiect de reglementare nemijlocit chestiunea asigurării securității cibernetice în domeniul aviației civile. Redacția actuală a alineatului (1) atribuie responsabilitatea exclusivă de asigurare a securității cibernetice pe seama autorității administrative de implementare și realizare a politicilor în domeniul aviației civile, adică Autoritatea Aeronautică Civilă și a instituției publice responsabile de implementarea politicii statului în domeniul securității cibernetice la nivel național *(presupunem că este vorba de Serviciul de Tehnologie a Informației și Securitate Cibernetică, deși acesta nu are nicio competență legală la nivel național, ci doar la nivel guvernamental),* ceea ce vine în

contradicție cu prevederile Legii privind securitatea cibernetică. Conform ultimei, responsabilitatea de asigurare a securității cibernetice este una partajată în primul rând între furnizorii de servicii și autoritatea competentă, fiecărei categorii revenindu-i obligații determinate de rolul și competența legală care le este atribuită, precum și, în cel de-al doilea rând, autorităților publice care realizează politica statului în domeniile relevante de activitate și autoritățile cu funcții regulatorii ale pieței, din perspectiva potențialului de exercitare de către acestea a competenței de reglementare ale unor cerințe specifice de securitate pentru anumite domenii/subdomenii sau categorii de persoane juridice cu activități în aceste domenii/subdomenii. În redacția propusă în proiect al alineatului (1) este reflectat anume acest principiu al responsabilității partajate. De asemenea în proiect se propune completarea art. 22 al Legii privind securitatea aeronautică cu două alineate noi. Redacția acestora este fundamentată pe prevederile anexei I pct. 2 lit. a) din Directiva NIS2, corelate cu terminologia utilizată de Legea ce se propune a fi modificată și reflectă același algoritm de reglementare a conexiunii cu Legea privind securitatea cibernetică: identificarea juridico-normativă a cercului generic de subiecți, instituirea obligațiilor de asigurare a securității cibernetice și competența ulterioară a autorității competente în domeniul securității cibernetice de identificare a subiecților relevanți și de supraveghere a modului în care aceștia își realizează obligațiile.

În **articolul XXI** din proiectul de lege se propun completări ale ***Codului transportului feroviar***. Transportul feroviar este un alt subsector al sectorului de transporturi, prevăzut de anexa I, pct. 2 lit. b) a Directivei NIS2. Tipurile de entități esențiale date de directivă în acest subsector sunt *administratorii infrastructurii* și *întreprinderile feroviare, inclusiv operatorii unei infrastructuri de servicii*, definiți în art. 3, pct. 1, pct. 2 și, respectiv, pct. 12 din Directiva 2012/34/UE[7]. Potrivit preambulului Codului transportului feroviar directiva respectivă este unul din actele legislative europene la care este armonizată legislația națională prin adoptarea acestui Cod. Într-adevăr noțiunile corespondente utilizate în lege și definițiile acestora au un conținut similar semnificației date de prevederile Directivei menționate. În consecință, completările propuse la Cod în proiectul de lege presupune același model de acțiune, adică identificarea categoriilor legale generice de potențiali subiecți ai Legii privind securitatea cibernetică, instituirea obligaților acestora de a asigura securitatea cibernetică în conformitate cu legislația respectiv și competența autorității competente în domeniul securității cibernetice de a exercita funcția de supraveghere și control al modului de îndeplinire a acelor obligații.

În ce privește subsectorul transportului rutier relevăm că potrivit anexei nr. I la Directiva NIS2 tipurile de entități din subsectorul transportului rutier sunt *autoritățile rutiere* și *operatorii de sisteme de transport inteligente*. În Republica Moldova autoritățile rutiere, astfel cum urmează a fi înțelese din definiția dată în articolul 2 punctul 12 din Regulamentul delegat (UE) 2015/962[8], este Agenția Națională Transport Auto. Aceasta va cădea sub incidența Legii nr. 48/2023, deoarece intră în categoria persoanelor juridice de drept public, menționată în art. 3 alin. (2) lit. i) din Legea nr. 48/2023. Cealaltă categorie – operatorii de sisteme de transport inteligente – nu este reglementată de legislația națională. Prin urmare, modificarea Codului transportului rutier la momentul actual este inoportună.

Articolul V din proiectul de lege cuprinde modificări ale ***Legii comunicațiilor electronice nr. 241/2007*** care constau în revizuirea prevederilor articolelor 21 și 22 din această lege, obiectul de reglementare al cărora se suprapune cu obiectul de reglementare al Legii privind securitatea

[7] Directiva 2012/34/UE a Parlamentului European și a Consiliului din 21 noiembrie 2012 privind instituirea spațiului feroviar unic european (reformare) (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02012L0034-20190101);

[8] Regulamentul delegat (UE) 2015/962 al Comisiei din 18 decembrie 2014 de completare a Directivei 2010/40/UE a Parlamentului European și a Consiliului în ceea ce privește prestarea la nivelul UE a unor servicii de informare în timp real cu privire la trafic (https://eur-lex.europa.eu/legal-content/RO/ALL/?uri=CELEX%3A32015R0962);

cibernetică. Aceste două articole reglementează în prezent obligativitatea implementării măsurilor de securitate de către furnizorii de rețele și servicii de comunicații electronice, obligațiile acestora de notificare a ANRCETI și competența ANRCETI de supraveghere și control al modului în care aceste obligații sunt realizate. Unul dintre actele UE la care s-a armonizat parțial legislația națională prin adoptarea Legii comunicațiilor electronice, menționat de altfel în preambulul acesteia din urmă, este Directiva 2002/21/CE[9]. Art. 13a alin. (1) – (3) și art.13b alin. (1) – (3) din această directivă sunt transpuse prin articolele 21 și 22 din Legea nr. 241/2007. Conținutul normativ al articolelor 13a și 13b din Directiva 2002/21/CE este în principiu corespondent celui al articolelor 40 și 41 din Directiva (UE) 2018/1972[10] (vezi tabelul de corespondență de la anexa XIII la această directivă). Potrivit prevederilor articolului 43 din Directiva NIS2 articolele 40 și 41 din Directiva (UE) 2018/1972 se abrogă. Abrogarea respectivă este determinată de necesitatea de a „*raționaliza obligațiile impuse furnizorilor de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului... în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, precum și pentru a permite acestor entități și autorităților competente în temeiul Directivei (UE) 2018/1972... să beneficieze de cadrul juridic instituit prin*" Directiva NIS2[11]. Această revizuire a Directivei (UE) 2018/1972 urmează să fie extrapolată la sistemul legislativ național în vederea asigurării aducerii în concordanță a cadrului legal la prevederile Legii privind securitatea cibernetică și, implicit, executarea prevederilor art. 23 alin. (2) lit. a) al acesteia. În consecință, în proiect se propune expunerea într-o nouă redacție a art. 21, redacție care va asigura conexiunea cu Legea privind securitatea cibernetică și va exclude eventuale interpretări echivoce din perspectiva aplicării principiului normă generală-normă specială, stabilit de art. 5 alin. (3) din Legea nr. 100/2017 privind actele normative. De asemenea, ținem să relevăm că, potrivit art. 2 alin. (2) și anexei I pct. 8 din Directiva NIS2, *furnizorii de rețele publice de comunicații electronice* și *furnizorii de servicii de comunicații electronice accesibile publicului* sunt tipuri de entități esențiale care, indiferent de dimensiunea pe care o au, urmează să cadă sub incidența obligațiilor de asigurare a securității cibernetice. Reglementările naționale din Legea privind securitatea cibernetică transpun de o manieră fidelă acest algoritm (art. 3 alin. (2) lit. a) din această lege). În concluzie în proiect este propusă expunerea art. 21 într-o redacție nouă care *a)* instituie responsabilitatea tipurilor respective de furnizori să realizeze obligațiile de asigurare a securității cibernetice conform Legii privind securitatea cibernetică, b) stabilește competența de supraveghere și control de stat în ce privește modul de îndeplinire a obligațiilor stabilite de Legea nr. 48/2023 a autorității competente în temeiul acestei legi și c) obligația acestei autorități competente să informeze ANRCETI despre rezultatele procesului de supraveghere și control. Această din urmă obligație este necesară în contextul prerogativei ANRCETI de exercitare a supravegherii respectării legislației în domeniul comunicațiilor electronice. Articolul 22 urmează a fi abrogat deoarece acesta cuprinde reglementări ce interferează cu aria de competență a autorității competente în temeiul Legii nr 48/2023.

La **articolul VII** din proiectul de lege sunt propuse un set de modificări la ***Legea nr.171/2012 privind piața de capital***. Acestea sunt determinate de faptul că un alt sector de importanță critică ridicată este ***sectorul infrastructurilor pieței financiare***, sector prevăzut la anexa I pct. 4 din Directiva NIS2. Acest sector include două tipuri de entități esențiale – *operatorii de locuri de tranzacționare* și *contrapărțile centrale.* În cazul primului tip, pentru identificarea categoriilor de persoane juridice corespondente în legislația națională este necesar să se țină cont de

[9] Directiva 2002/21/CE a Parlamentului European și a Consiliului din 7 martie 2002 privind un cadru de reglementare comun pentru rețelele și serviciile de comunicații electronice (Directivă-cadru) (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02002L0021-20091219)

[10] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice (reformare) (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02018L1972-20181217&qid=1693828518911)

[11] Recitalul 92 din Directiva NIS2 (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555);

terminologia utilizată de Directiva 2014/65/UE[12], în mod special noțiunea de loc de tranzacționare care înseamnă o piață reglementată, un sistem multilateral de tranzacționare (MTF) sau un sistem organizat de tranzacționare (OTF). Corelând terminologia utilizată de directiva respectivă cu cea utilizată de Legea privind piața de capital, putem identifica persoanele juridice care sunt potențiali furnizori de servicii în sensul Legii privind securitatea cibernetică: societățile de investiții și operatorii de piață, definiți în art. 6 din Legea nr.171/2012. În consecință în articolele 41, respectiv, 62 din această lege se propun completări care constau în corelarea prevederilor Legii privind piața de capital cu cele ale Legii privind securitatea cibernetică în ce privește responsabilitatea persoanelor juridice respective de a realiza obligațiile de asigurare a securității cibernetice, în mod special, implementarea măsurilor de securitate adecvate și notificarea incidentelor semnificative, competența autorității competente în temeiul Legii nr. 48/2023 de a identifica persoanele juridice respective în calitate de furnizori de servicii și de a exercita competența de supraveghere și control al modului în care aceste obligații sunt realizare de către viitorii furnizori de servicii din acest sector.

Completările propuse în **articolul IX** din proiect sunt determinate de faptul că potrivit punctelor 6 și 7 din anexa I la Directiva NIS2, ***apa potabilă*** și, respectiv, ***apele uzate*** sunt alte două sectoare de importanță critică ridicată, care includ tipurile de entități esențiale – *furnizorii și distribuitorii de apă destinată consumului uman*, și respectiv, *întreprinderile care colectează, evacuează sau tratează ape urbane reziduale, ape menajere uzate sau ape industriale uzate*, reglementate în principal de Directiva (UE) 2020/2184[13] și, respectiv, Directiva 91/271/CEE[14]. La nivelul normelor primare în plan național, actul de bază care reglementează aceste sectoare este ***Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare.*** Completările de bază vizează art. 9^1 și art. 15. În contextul determinării cercului de subiecți în aceste sectoare, potențiali furnizori de servicii în completările propuse este utilizat termenul general de operatori, care este definit la art. 4 din legea vizată. Conținutul de fond al completărilor este în esență similar celui cu care s-a operat și în cazul articolelor descrise mai sus. Suplimentar în această lege se propune completarea art. 9 cu o literă nouă care constă în referința expresă la autoritatea competentă la nivel național în domeniul securității cibernetice să exercite supravegherea și controlul de stat în acest domeniu. Acest articol cuprinde o listă, care având un caracter exhaustiv, ar putea implica, din perspectiva principiului priorității de aplicare a normei juridice speciale, interpretări ulterioare ce ar putea dăuna implementării adecvate a prevederilor Legii privind securitatea cibernetică.

Sectorul serviciilor poștale și de curierat este un sector de importanță critică, prevăzut în anexa II la Directiva NIS2. În acest sector directiva identifică furnizorii de servicii poștale, inclusiv furnizorii de servicii de curierat, ca tip de persoane juridice ce ar trebui identificate ca furnizori de servicii critice la nivel național. În Republica Moldova, sectorul respectiv este reglementat de ***Legea comunicațiilor poștale nr. 36/2016***. În acest context, în **articolul X** din proiect este propusă completarea art. 14 din Legea respectivă cu un alineat nou care are ca obiectiv corelarea și interconexiunea acestei legi cu Legea privind securitatea cibernetică, prin introducerea, după modelul descris anterior, a obligațiilor exprese de asigurare a securității cibernetice de către furnizorii de servicii poștale, identificați de autoritatea competentă și stabilirea competenței de

[12] Directiva 2014/65/UE a Parlamentului European și a Consiliului din 15 mai 2014 privind piețele instrumentelor financiare și de modificare a Directivei 2002/92/CE și a Directivei 2011/61/UE (reformare) (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02014L0065-20230323);

[13] Directiva (UE) 2020/2184 a Parlamentului European și a Consiliului din 16 decembrie 2020 privind calitatea apei destinate consumului uman (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32020L2184)

[14] Directiva Consiliului din 21 mai 1991 privind tratarea apelor urbane reziduale (91/271/CEE) (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A01991L0271-20140101)

exercitarea de către ultima a funcției de supraveghere și control de stat a modului în care aceste obligații sunt realizate.

În **articolul XI** se propune completarea ***Legii nr. 209/2016 privind deșeurile***. Această completare este determinată de faptul că potrivit pct. 2 din anexa nr. II la Directiva NIS2 gestionarea deșeurilor este un alt sector de importanță critică, *întreprinderile care efectuează gestionarea deșeurilor* definite în Directiva 2008/98/CE[15] fiind determinate ca tip de entități importante în acest sector. Reieșind din obiectivul general de a continua armonizarea legislației naționale la Directiva NIS2 și cel specific de asigurare a interconexiunii cu Legea securității cibernetice și eliminării potențialelor interpretări echivoce completările propuse în proiect la Legea privind deșeurile păstrează în principiu același tipar de reglementare care constă în determinarea generică a spectrului de subiecți și a obligațiilor de realizarea cărora aceștia sunt responsabili în domeniul securității cibernetice, precum și stabilirea competenței de supraveghere și control de stat al modului în care aceste obligații sunt realizare de către subiecții identificați.

În ce privește modificările la ***Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului,*** propuse în **articolul XIII** din proiectul de lege, acestea sunt determinate de necesitatea asigurării conexiunii reglementărilor din legea respectivă cu prevederile art. 3 alin. (2) lit. h) din Legea privind securitatea cibernetică. În conformitate cu această prevedere operatorul unui obiectiv de infrastructură critică intră în domeniul de aplicare a Legii privind securitatea cibernetică, dacă furnizarea serviciilor sale depinde de o rețea sau un sistem informatic. Astfel, completările la art. 20 sunt propuse din perspectiva delimitării competențelor și evitării unor conflicte de competență dintre organul de supraveghere și control în temeiul Legii nr. 120/2017 și autoritatea competentă în temeiul Legii nr. 48/2023 și pentru asigurarea unei cooperări eficiente dintre aceste două entități. Completările propuse la art. 3 al Legii nr. 120/2017 sunt conexe celor propuse la art. 20 și sunt necesare a fi efectuate, dat fiind faptul că în redacția noilor alineate propuse la pct. 2 sunt utilizate noțiuni care nu sunt definite de cadrul legal primar oferit de Legea nr. 120/2018. Noțiunile de *obiectiv al infrastructurii critice* și *operator* sunt preluate din cadrul normativ secundar, actualmente în vigoare, și anume din Regulamentul privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701/2018.

Sectorul energie este unul dintre sectoarele calificate de Directiva NIS2 ca fiind de o importanță critică ridicată. Acest sector este divizat potrivit pct. 1 din anexa I la directiva respectivă în cinci subsectoare: electricitate, încălzire centralizată și răcire centralizată, petrol, gaze și hidrogen. În Republica Moldova actul normativ cadru care reglementează la nivel primar acest sector este ***Legea 174/2017 cu privire la energetică*** (**articolul XIV** din proiectul de lege). Totuși fiecare din subsectoarele menționate au o lege națională dedicată. Aceste subsectoare sunt reglementate de legi specifice precum: Legea nr. 107/2016 cu privire la energia electrică, Legea nr. 461/2001 privind piața produselor petroliere, Legea nr. 108/2016 cu privire la gazele naturale, Legea nr. 92/2014 cu privire la energia termică și promovarea cogenerării, Legea nr.10/2016 privind promovarea utilizării energiei din surse regenerabile**.** Una din categoriile de subiecți ai raporturilor juridice reglementate de Legea cu privire la energetică sunt *întreprinderile energetice*, definite de această lege ca fiind „*persoană fizică sau persoană juridică, înregistrată în modul stabilit în Republica Moldova în calitate de întreprindere, care desfășoară cel puțin una dintre activitățile reglementate prin"* legile sectoriale specifice menționate mai sus. Această noțiune include toate tipurile de entități esențiale enumerate la pct. 1 din anexa I la Directiva NIS2. În consecință, ținând cont de principiul minimei intervenții, considerăm oportună completarea doar a Legii cu privire la energetică cu prevederi care reflectă același algoritm propus în cazul modificărilor operate la alte legi prin prezentul proiect și

[15] Directiva 2008/98/CE a Parlamentului European și a Consiliului din 19 noiembrie 2008 privind deșeurile și de abrogare a anumitor directive (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02008L0098-20180705)

anume: specificarea expresă a responsabilității întreprinderilor energetice, identificate ca furnizori de servicii de autoritatea competentă în domeniul securității cibernetice, de a implementa obligațiile de asigurare a securității cibernetice și stabilirea competenței autorității respective de exercitare a funcției de supraveghere și control a modului în care întreprinderile identificate ca furnizori de servicii își realizează obligațiile legale în domeniul securității cibernetice. Suplimentar în punctul 1 al articolului XV din proiectul de lege este o propusă o modificare care are ca obiectiv să excludă eventualele interpretări restrictive care ar putea fi generate de actuala normă de la art. 21 alin. (4) aplicată în coroborare cu alin. (2). Astfel, conform sensului normei actuale orice ingerință legală a oricărui organ de stat în activitatea întreprinderilor energetice, dacă nu este realizată în baza Legii cu privire la energetică sau a celorlalte 5 „legi sectoriale" este considerată *„a fi un amestec în activitatea întreprinderilor energetice în sensul alin.(2)"*, ceea ce formal juridic exclude posibilitatea de intervenție în baza legii, spre ex. a autorității competente în domeniul securității cibernetice.

Articolul XV din proiectul de lege include modificări la ***Legea nr. 202/2017 privind activitatea băncilor***. În conformitate cu pct. 3 din anexa 1 la Directiva NIS2 *sectorul bancar* este unul dintre sectoarele de importanță critică ridicată, iar ca tip de entități esențiale directiva respectivă determină *instituțiile de credit*, astfel cum sunt definite la articolul 4 punctul 1 din Regulamentul (UE) nr. 575/2013[16]. Completarea propusă în proiectul de lege este reflecția discuțiilor avute cu Banca Națională a Moldovei în procesul de avizare și consultare a proiectului de lege. Astfel, pe de o parte redacția articolului 38^2, în particular alin. (1) – alin. (6), este orientată spre realizare obiectivelor asumate de Banca Națională în consolidarea cadrului legal privind activitatea băncilor exprimată prin necesitatea înlăturării lacunelor legislative privind aspectele ce vizează administrarea riscurilor de tehnologie a informației și a comunicațiilor, de securitate a informațiilor și de continuitate a activității, sesizate în procesul de supraveghere bancară. Este de menționat că la elaborarea textului normelor propuse la art.381 au fost luate în considerare recomandările adresate de Autoritatea Bancară Europeană în cadrul Ghidului EBA/GL/2019/04, unde se precizează măsurile pe care trebuie să le ia instituțiile financiare pentru a-și administra riscurile TIC și de securitate a informației. Pe de altă parte, redacția acestui articol nou, în mod special alin. (7)-(8) are ca obiectiv asigurarea interconexiunii cu prevederile Legii nr. 48/2023 și stabilirea competenței autorității competente în domeniul securității cibernetice de exercitare a funcției de supraveghere și control a modului în care subiecții obligațiilor respective își realizează obligațiile legale, doar că în cazul acestor entități, ținnd cont de specificul activității lor, exercitarea acestei funcțții urmează a fi efectuată în comun cu Banca Națională a Moldovei.

În context ținem să relevăm că noțiunea de *instituție de credit* dată de Regulamentul UE nr. 575/2013 a fost transpusă în legislația națională prin noțiunea de *bancă* conținută de art. 3 din Legea nr. 202/2017. Între timp conținutul noțiunii de instituție de credit a fost extins prin modificările operate la Regulamentul respectiv al UE. În concluzie, este probabil ca odată cu armonizarea legislației naționale la Regulamentul UE revizuit să fie necesare ajustări și la alte acte normative primare din legislația națională în legătură cu aducerea acesteia în concordanță cu prevederile Legii nr. 48/2023.

La **articolul XVIII** sunt propuse completări la articolele 11 și 12 din ***Legea nr. 277/2018 privind substanțele chimice***. *Fabricarea, producția și distribuția de substanțe chimice* este un alt sector de importanță critică prevăzut la pct. 3 din anexa II la Directiva NIS2. În cazul acestui sector directiva respectivă evidențiază două tipuri de entități importante: *întreprinderile care produc*

[16] Regulamentul nr. 575/2013 al Parlamentului European și al Consiliului din 26 iunie 2013 privind cerințele prudențiale pentru instituțiile de credit și de modificare a Regulamentului (UE) nr. 648/2012 (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02013R0575-20230628)

substanțe și distribuie substanțe sau amestecuri și *întreprinderile care produc articole din substanțe sau amestecuri*. Ambele tipuri urmează a fi determinate ținând cont de prevederile articolului 3 punctele 3, 9 și 14 din Regulamentul (CE) nr. 1907/2006[17]. Legea privind substanțele chimice în art. 4 definește noțiunea de *furnizor al unei substanțe sau al unui amestec* ca fiind *orice producător, importator, utilizator din aval sau distribuitor care plasează pe piață o substanță ca atare sau în amestec ori un amestec*. Această definiție cuprinde ambele tipuri menționate la pct. 3 din anexa nr. 2 la Directiva NIS2. În consecință, în legea în speță, utilizând același tipar de reglementare se propune completarea art. 12, care are ca obiect de reglementare obligațiile generale ale operatorilor din lanțul de aprovizionare, cu o normă care să stabilească expres responsabilitatea furnizorilor unei substanțe sau al unui amestec, identificați de autoritatea competentă, de a realiza obligațiile de asigurare a securității cibernetice, stabilite de Legea privind securitatea cibernetică. Corespunzător la art. 11, care reglementează competențele altor autorități ale administrației publice centrale în domeniul respectiv, este propusă completarea cu prevederi care să stabilească expres competența autorității competente în exercitarea funcției de supraveghere și control al modului în care furnizorii de substanțe chimice sau de amestecuri realizează obligațiile respective.

În **articolul XIX** din proiectul de lege se propune completarea articolelor 7 și 8 din ***Legea nr. 306/2018 privind siguranța alimentelor***. *Producția, prelucrarea și distribuția de alimente* este prevăzut la pct. 4 anexa II al Directivei NIS2 ca fiind un sector de importanță critică. În acest sector directiva determină *întreprinderile din sectorul alimentar care sunt implicate în distribuția angro și în producția și prelucrarea industrială*. Identificarea acestor întreprinderi urmează a fi efectuată ținând cont, în mod special, de art.3 pct. (2) din Regulamentul (CE) nr. 178/2002[18]. În legislația națională, la art. 2 din Legea privind siguranța alimentelor este definită noțiunea de întreprindere din domeniul alimentar care în principiu este corespondentul noțiunii utilizate în actul legislativ european. În consecință, art. 7 din Legea nr. 306/2018 se propune să fie completat cu un alineat nou, care să instituie responsabilitatea întreprinderilor din domeniul alimentar, care sunt identificate ca fiind furnizor de servicii în sensul Legii privind securitatea cibernetică, să realizeze obligațiile stabilite de această din urmă lege și, corespunzător, art.8 cu un alineat nou care să stabilească competența de supraveghere și control al autorității competente al modului în care sunt îndeplinite aceste obligații.

În ce privește **articolul XXII**, raționamentele care au stat la baza propunerilor de modificare a Legii comunicațiilor electronice sunt valabile și în cazul celor de revizuire a ***Legii nr. 124/2022 privind identificarea electronică și serviciile de încredere***. Astfel, actualmente art. 39 din această lege conține prevederi care dublează prevederile Legii privind securitatea cibernetică, în mod special art. 11 alin. (2) pct. 2) art. 12 alineatele (1), (6) și (7). În context relevăm că articolul 39 este reflecția procesului de armonizare a legislației naționale la Regulamentul (UE) nr. 910/2014[19], inițiat prin adoptarea Legii nr. 124/2022 și, în mod specific, transpune art. 19 din acest act al UE. În temeiul art. 42 din Directiva NIS2, art. 19 din Regulamentul (UE) nr. 910/2014 urmează a fi eliminat

[17] Regulamentul (CE) nr. 1907/2006 al Parlamentului European și al Consiliului din 18 decembrie 2006 privind înregistrarea, evaluarea, autorizarea și restricționarea substanțelor chimice (REACH), de înființare a Agenției Europene pentru Produse Chimice, de modificare a Directivei 1999/45/CE și de abrogare a Regulamentului (CEE) nr. 793/93 al Consiliului și a Regulamentului (CE) nr. 1488/94 al Comisiei, precum și a Directivei 76/769/CEE a Consiliului și a Directivelor 91/155/CEE, 93/67/CEE, 93/105/CE și 2000/21/CE ale Comisiei (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02006R1907-20230806).

[18] Regulamentul (CE) nr. 178/2002 al Parlamentului European și al Consiliului din 28 ianuarie 2002 de stabilire a principiilor și a cerințelor generale ale legislației alimentare, de instituire a Autorității Europene pentru Siguranța Alimentară și de stabilire a procedurilor în domeniul siguranței produselor alimentare (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02002R0178-20220701)

[19] Regulamentul (UE) nr . 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A02014R0910-20140917)

începând cu data de 18 octombrie 2024. Această eliminare este determinată de necesitatea de a „raționaliza obligațiile impuse ... prestatorilor de servicii de încredere în ceea ce privește securitatea rețelelor și a sistemelor lor informatice, precum și pentru a permite acestor entități și autorității competente în temeiul... Regulamentul (UE) nr. 910/2014 să beneficieze de cadrul juridic instituit prin" Directiva NIS2. În vederea reflectării acestui aspect în legislația națională și eliminării dublărilor de norme juridice primare, precum și evitării unor interpretări echivoce în proiect se propune o nouă redacție a art. 39 din Legea nr. 124/2022. Această nouă redacție asigură o conexiune cu reglementările Legii privind securitatea cibernetică instituind responsabilitatea prestatorilor de servicii de încredere de a realiza obligațiile de asigurare a securității cibernetice, stabilind competența de supraveghere și control de stat a autorității competente în temeiul Legii nr. 48/2023 și obligativitatea de cooperare cu organul de supraveghere și control în temeiul Legii nr. 124/2022.

5. Fundamentarea economico-financiară

Proiectul de lege propus spre examinare este unul care vine să completeze inițiativa de legiferare realizată prin Legea privind securitatea cibernetică, având ca obiectiv primordial alinierea legislației actuale la prevederile Legii menționate. În principiu, prevederile proiectului nu implică cheltuieli financiare adiționale celor care în mod normal sunt prevăzute pentru activitatea curentă a entităților care vor fi afectate. Analiza de impact[20] la proiectul de Lege privind securitatea cibernetică cuprinde informații suficiente care acoperă și impactul financiar al prevederilor proiectului în speță. Totuși, referindu-ne la articolul care prevede modificarea *Legii privind sistemul unitar de salarizare în sectorul bugetar*, trebuie de relevat că acestea constau în costurile salariale pentru personalul Agenției pentru Securitate Cibernetică. Conform estimărilor, suma totală pentru salarizarea angajaților acestei entități va constitui circa 24,6 milioane lei anual. Din această sumă, aproximativ 11 milioane lei vor fi alocate subdiviziunii interne a Agenției responsabile de realizarea funcției de echipă de răspuns la incidentele cibernetice. Această alocare financiară semnificativă este esențială pentru funcționarea optimă a autorității competente în domeniul securității cibernetice și pentru asigurarea unui răspuns adecvat la amenințările cibernetice. Este important să se acorde o atenție specială costurilor salariale pentru echipa de răspuns la incidentele cibernetice, având în vedere rolul lor crucial în protejarea infrastructurii informaționale critice pentru funcționarea economiei naționale, a societății și a statului.

6. Modul de încorporare a actului în cadrul normativ în vigoare

Având în vedere întinderea efectelor pe care le va produce proiectul de lege, este important ca autoritățile administrației publice centrale de specialitate, responsabile de realizarea politicii statului în domeniile reglementate de legile a căror modificare se propune, să efectueze o evaluare a legislației subsidiare acestor legi în vederea identificării necesității de revizuire a acestora. Totodată, unei examinări aprofundate urmează a fi supuse legile cadru care reglementează sectoarele, subsectoarele și tipurile de entități ce prestează servicii în acestea, enumerate în anexele I și II la Directiva NIS2 din perspectiva armonizării acestora cu actele sectoriale relevante ale Uniunii Europene, menționate de altfel în anexele respective ale Directivei NIS2.

În context, Ministerului Justiției i-au fost propuse completări la Codul Contravențional nr. 218/2008, în special completarea capitolului XIV al cărții întâi „*Contravenții în domeniul comunicațiilor electronice și al comunicațiilor poștale*" cu două componențe noi: *încălcarea legislației în domeniul securității cibernetice* și *împiedicarea activității Agenției pentru Securitate Cibernetică,* precum și completarea capitolului III al cărții a doua *„Autoritățile competente să soluționeze cauzele contravenționale"* cu un articol dedicat Agenției pentru Securitate Cibernetică

[20] https://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/6386/language/ro-RO/Default.aspx

în stabilirea competenței acesteia de constatare și examinare a cauzelor contravenționale în privința contravențiilor respective.

În paralel, în vederea executării prevederilor art. 23 alin. (2) lit. c) din Legea privind securitatea cibernetică, Guvernul urmează să aducă actele sale normative în concordanță cu această lege. În contextul acestui exercițiu, Ministerul Dezvoltării Economice și Digitalizării urmează să elaboreze un proiect de act normativ în acest sens care vizează domeniile sale de competență, inclusiv domeniul securității cibernetice. Pentru a asigura realizarea acestei sarcini urmează a fi supuse dacă nu unei revizuiri, cel puțin unei examinări aprofundate în scopul confirmării conformității cu prevederile noii legislații a următoarelor acte normative guvernamentale:

- Hotărârea Guvernului nr. 201/2017 privind aprobarea cerințelor minime obligatorii de securitate cibernetică;
- Hotărârea Guvernului nr. 482/2020 privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental;
- Hotărârea Guvernului nr. 388/2022 cu privire la aprobarea Concepției Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică".

Totodată, în contextul modificărilor propuse la articolul XVIII din proiect va fi necesară modificarea Regulamentului cu privire la tipurile și modul de stabilire a sporurilor cu caracter specific, aprobat prin Hotărârea Guvernului nr. 1231/2018.

În ceea ce privește articolul XII, va trebui examinată de către autoritățile responsabile necesitatea revizuirii actului departamental aprobat în temeiul art. 16 alin. (3) din Legea privind dispozitivele medicale din perspectiva completărilor operate în acest articol în legătură cu punerea în aplicare a prevederilor Legii privind securitatea cibernetică. Cu referire, de asemenea, la art. XIII, în ceea ce privește tipul de furnizori de servicii – *producători de dispozitive medicale, care sunt esențiale în contextul unei urgențe de sănătate publică*, adică sunt incluse în lista dispozitivelor esențiale pentru urgența de sănătate publică, este posibil să fie necesară revizuirea Legii nr.10/2009 privind supravegherea de stat a sănătății publice în vederea clarificării chestiunii armonizării legislației naționale în acest domeniu inclusiv la Regulamentul (UE) 2022/123. Această revizuire va permite realizarea procesului de identificare a acestei categorii de furnizori de servicii de către autoritatea competentă în domeniul securității cibernetice.

7. Avizarea și consultarea publică a proiectului

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional, pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării ***mded.gov.md*** și pe platforma de consultare ***particip.gov.md,*** a fost publicat anunțul referitor la consultarea publică a proiectului de lege la care au fost anexate proiectul de lege, nota informativă, sinteza obiecțiilor și propunerilor și tabelul comparativ la proiectul de lege (https://particip.gov.md/ro/document/stages/anunt-privind-consultarea-publica-a-proiectului-de-lege-pentru-modificarea-unor-acte-normative-aducerea-cadrului-legal-in-concordanta-cu-legea-nr-482023-privind-securitatea-cibernetica/11456).

Proiectul a fost supus procedurii de avizare și reavizare conform cerințelor legislației în vigoare, care într-un final a soldat cu obiecții reiterate din partea MF, MJ, BNM, CNFP și CNA.

În continuare, la data de 30.01.2024, în vederea atingerii unui consens pe marginea obiecțiilor înaintate de către MF, MJ, BNM, CNFP și CNA, potrivit pct.205 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr.610/2018, a fost convocată ședința interinstituțională (procedura electronică), în rezultatul căreia sa ajuns la un consens asupra versiunii definitivate a proiectului.

8. Constatările expertizei anticorupție
Proiectul a fost supus expertizei anticorupție și a fost definitivat conform obiecțiilor prezentate. Referitor la obiecțiile care nu au fost acceptate de autor, menționăm că pe data de 30.01.2024 a fost convocată ședința interinstituțională în vederea atingerii unui consens pe marginea obiecțiilor înaintate, în rezultatul căreia reprezentantul CNA a acceptat argumentele expuse de reprezentanții MDED și a susținut proiectul.
9. Constatările expertizei de compatibilitate
Proiectul nu are ca scop transpunerea directă a unor prevederi din Directiva (UE) 2022/2555, precum și nu instituie careva prevederi noi care contravin actului UE, inserând obligații generale aferente securității cibernetice pentru furnizorii de servicii în actele normative sectoriale (scrisoarea Centrului de armonizare a legislației Nr. 31/02-69-12155 din 20.11.2023).
10. Constatările expertizei juridice
Proiectul a fost supus expertizei juridice și a fost modificat conform obiecțiilor și propunerilor prezentate. Referitor la obiecția de ordin tehnic prezentată de Ministerul Justiției și neacceptată de autor la etapa avizării repetate, menționăm că pe data de 30.01.2024 a fost convocată ședința interinstituțională în vederea atingerii unui consens pe marginea obiecțiilor înaintate, în rezultatul căreia reprezentanții MDED au acceptat argumentele expuse de reprezentanții MJ și respectiv proiectul a fost modificat.
11. Constatările altor expertize
Analiza impactului și proiectul de lege au fost examinate în cadrul ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, ambele fiind susținute condiționat - la data de 10.01.2024 și, respectiv – 30.01.2024.

Secretar general **Ina VOICU**

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul de lege pentru modificarea unor acte normative (aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică) (num. unic: 957/MDED/2023)

AVIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Finanțelor** *(Nr. 07/3-03-268/1800 din 04.12.2023)*	1)	În sinteza obiecțiilor și propunerilor (recomandărilor) la proiectul de lege, se indică neacceptarea propunerii de a revedea/ajusta mărimea procentului stabilit pentru sporul cu caracter specific pentru personalul Agenției pentru Securitate Cibernetică. Propunerea autorului privind includerea acestei norme în Art.XVII ce ține de stabilirea sporului cu carater specific în mărime de 200%-600% din salariul de bază a angajaților Agenției nu poate fi susținută, dat fiind faptul că această normă va crea inechitate între personalul altor instituții bugetare care activează în condiții similare, ceea ce presupune o deviere de la unul din principiile sistemului unitar de salarizare – „nediscriminare, echitate și coerență, în sensul asigurării tratamentului egal și a remunerării egale pentru munca de valoare egală”. Reieșind din cele relatate, considerăm necesar de a examina costurile aferente proiectului în corelare cu alocațiile bugetare acceptate în cadrul elaborării proiectului bugetului de stat pentru anul 2024 și estimărilor pe anii 2025-2026. Astfel, în conformitate cu proiectul legii bugetului de stat pentru anul 2024, aprobat în ședința Guvernului din 1 decembrie 2023, la subprogramul 1504	**Se acceptă.** Urmare a celor convenite în cadrul ședințelor dintre reprezentanții Ministerului Dezvoltării Economice și Digitalizării și Ministerul Finanțelor, art. XVIII din proiectul de lege a fost revizuit. Revizuirile sunt determinate de algoritmul propus de Ministerul Finanțelor la calcularea salariilor personalului viitoarei agenții, și anume: a) sporul specific de 120%, creșterea cu 15 clase de salarizare pentru funcțiile de șef și șef adjunct de direcție ce va exercita funcția de CSIRT național și cu 25 de clase de salarizare pentru funcțiile de execuție din subdiviziunea respectivă. În proiectul de lege în speță, acest algoritm este reflectat nu doar prin completările propuse la Legea nr. 270/2018, ci și prin completările propuse la Legea bugetului de stat pentru anul 2024 (art. XXIII din proiectul de lege). În ceea ce privește cel de-al treilea parametru – valoarea de referință, aceasta va fi de 3600 lei pentru toate funcțiile publice din cadrul Direcției răspuns la incidente și crize cibernetice a ASC și 2500 lei – pentru restul personalului.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			„Tehnologii informaționale” au fost aprobate cheltuieli în sumă de 15 000,0 mii lei (inclusiv cheltuieli de personal 12 449,2 mii lei pentru 49 unități de personal/calculat pentru 9 luni). Conform prevederilor art.17 alin. (2) din Legea finanțelor publice și responsabilității bugetar-fiscale nr.181/2014, pe parcursul anului bugetar nu pot fi puse în aplicare decizii care conduc la majorarea cheltuielilor bugetare, dacă impactul financiar al acestora nu este prevăzut în buget, iar conform art.131 alin. (6) din Constituția RM, nici o cheltuială bugetară nu poate fi aprobată fără stabilirea sursei de finanțare.	
		2)	Totodată, este de menționat că prevederile art.3 alin.(1) din Legea nr.48/2023 privind securitatea cibernetică stabilește că legea în cauză se aplică persoanelor juridice care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele critice, stabilite de către Guvern. Ținând cont de faptul că Guvernul nu a stabilit, deocamdată, lista sectoarelor sau subsectoarelor critice, care să ofere claritate asupra căror domenii specifice se va aplica legea prenotată, actualmente nu pot fi evaluate și identificate legile sectoriale care necesită intervenții pentru a le aduce în concordanță cu legea respectivă.	**Nu se acceptă.** Propunerile de modificare a legilor sectoriale, de rând cu obiectivul de aducere în concordanță a cadrului legal cu Legea privind securitatea cibernetică, se înscriu în contextul mai larg de continuare a procesului de armonizare a legislației naționale la prevederile Directivei NIS2. Deși Legea nr. 48/2023 deleagă Guvernului competența de a stabili sectoarele subsectoarele, tipurile și categoriile de furnizori de servicii, aceasta nu implică un rol determinant a acestei decizii a Guvernului în finalizarea constituirii cadrului normativ primar în acest domeniu, inclusiv după cum a fost menționat, pentru a armoniza legislația națională la prevederile Directivei NIS2.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
				În context, notăm că anexele I și II la Directiva NIS2 stabilesc sectoarele și subsectoarele critice și tipologia entităților esențiale și importante, care intră în domeniul de aplicare al acesteia. Tipologia acestor entități este determinată de prevederile relevante, menționate de altfel în aceste anexe, din actele normative ale UE care reglementează sectoarele/subsectoarele respective. În consecință, în cazurile materializate în modificările propuse în proiectul de lege, a fost posibilă determinarea, în baza unei analize comparative formal-juridice, a tipologiei corespondente în legislația națională prin identificarea termenilor care înglobează tipurile de entități enumerate în anexele Directivei NIS2.
		3)	Concomitent, remarcăm că Directiva (UE) 2022/2555, care este transpusă prin Legea nr.48/2023, stabilește în Anexa 1 "Sectoarele cu o importanță critică ridicată" și în Anexa II „Alte sectoare de importanță critică", precum și tipul entităților aferente acestor sectoare. Respectiv, în Anexa nr. 1 se identifică sectorul bancar și infrastructurile pieței financiare, precum și entitățile aferente acestora, cum sunt instituțiile de credit (băncile), operatorii de locuri de tranzacționare și contrapărțile centrale. Conform alin. (28) din preambulul Directivei 2022/2555, dispozițiile acestei Directive privind gestionarea riscurilor în materie de securitate	**Se acceptă.** Într-adevăr, Regulamentului UE 2022/2554 privind reziliența operațională digitală a sectorului financiar, așa-numitul DORA are caracter de lege specială în raport cu prevederile Directivei NIS2 în ceea ce privește aplicabilitatea prevederilor acesteia asupra entităților financiare. Modificările propuse în proiect însă reies din contextul actual, context în care legislația națională încă nu a fost armonizată la acest Regulament UE. Prin urmare, până la producerea acestui fapt, prevederile Legii privind securitatea

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			cibernetică și obligațiile de raportare, supraveghere și aplicarea legii, nu ar trebui să se aplice entităților financiare care fac obiectul Regulamentului UE 2022/2554 privind reziliența operațională digitală a sectorului financiar, acesta fiind considerat un act juridic sectorial specific entităților financiare. În acest context, atragem atenția că potrivit art.2 alin. (1) din Regulamentul 2022/2554, acesta se aplică instituțiilor de credit (băncile), operatorilor de locuri de tranzacționare și contrapărților centrale. Astfel, considerăm că asupra eventualelor intervenții pe legile specifice din domeniul financiar (Legea nr.202/2017, Legea nr.171/2012, și alte legi după caz) urmează a se reveni după transpunerea în legislația națională a Regulamentului 2022/2554, precum și după o analiză și evaluare a modului de aplicare corelată a celor 2 acte UE în legislația națională. În concluzie, ținând cont de finanțarea prudentă a cheltuielilor bugetare, proiectul de lege și documentele aferente urmează a fi revizuite prin prisma celor expuse mai sus.	cibernetică urmează a fi aplicate și asupra entităților financiare. Totuși, în procesul de identificare a furnizorilor de servicii, viitoarea autoritate competentă urmează să aplice principiile de aplicare a Legii nr. 48/2023 prevăzute de alineatele (5) și (6) ale art. 3 din legea respectivă.
2.	**Ministerul Afacerilor Interne** *(Nr. 44/22 – 5377 din 27.11.2023)*	4)	La Art. XIII din proiectul de lege, unde sunt propuse modificări la Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului, noțiunea „obiectiv al infrastructurii critice” se propune a fi expusă cu următorul cuprins: „obiectiv al infrastructurii critice - obiectiv de importanță vitală din domeniul administrației publice, tehnologiei informației și comunicațiilor	**Nu se acceptă.** Noțiunea respectivă, după cum de altfel se precizează și în nota informativă la proiect, este preluată din cadrul normativ secundar de punere în aplicare a Legii nr. 120/2018 în forma sa intactă. Preluarea acestei noțiuni are raționamente exclusiv formal juridice și nu

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			electronice și poștale, de infrastructură, energetică, din sfera social-economică, sănătății, cultural-educativă, industrială, ecologică și din sistemul informațional al țării în ansamblu, inclusiv infrastructura complexului militar și de apărare al organelor de forță, ce include sisteme interconectate și interdependente, esențiale pentru siguranța, securitatea, bunăstarea socială și economică a statului, perturbarea sau distrugerea căruia poate provoca pierderi de servicii esențiale, pericol pentru viața și sănătatea oamenilor, efecte negative asupra mediului." În acest sens, indicăm că, definiția propusă de autor, deși este cuprinzătoare, nu subliniază suficient aspectele legate de interconectivitatea și interdependența sistemelor în cadrul infrastructurii critice. Într-un peisaj global, tot mai interconectat, această omisiune poate genera lacune în înțelegerea și gestionarea riscurilor. Prin includerea explicită a interconectivității și interdependenței, definiția devine mai relevantă și reflectă mai bine complexitatea și realitățile actuale ale infrastructurilor critice. Acest lucru este important pentru înțelegerea modului în care diferite sisteme influențează și depind unul de altul, oferind o perspectivă mai amplă asupra potențialelor riscuri și impactului lor.	urmează să influențeze în vreun fel fondul acesteia. Astfel, completările propuse la art. 3 al Legii nr. 120/2017 sunt conexe celor propuse la art. 20 și sunt necesare a fi efectuate, dat fiind faptul că în redacția noilor alineate propuse la pct. 2 sunt utilizate noțiuni care nu sunt definite de cadrul legal primar oferit de Legea nr. 120/2018. Orice intervenție în definiția acestei noțiuni, fără o analiză prealabilă profundă, efectuată de către responsabilii de punerea în aplicare a Legii nr. 120/2018, ar putea genera disfuncționalități în întregul proces reglementat de această lege.
		5)	Cuprinsul proiectului notei informative se va ajusta conform prevederilor anexei nr. 1 din Legea nr. 100/2017 cu privire la actele normative, având în vedere că lipsesc compartimentele „Constatările	**Se acceptă.**

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			expertizei anticorupție", „Constatările expertizei de compatibilitate", „Constatările expertizei juridice" și „Constatările altor expertize".	
		6)	Subsidiar, învederăm că autorul proiectului urmează a se conforma prevederilor art. 54 din Legea nr. 100/2017 și a expune conținutul proiectului într-un limbaj simplu, clar și concis, pentru a se exclude orice echivoc, cu respectarea strictă a regulilor gramaticale, de ortografie și de punctuație.	**Se acceptă.**
3.	**Ministerul Apărării** *(Nr. 11/1659 din 23.11.2023)*		Lipsa obiecțiilor și propunerilor.	
4.	**Ministerul Afacerilor Externe și Integrării Europene** *(Nr. DI/3/041-13293 din 17.11.2023)*		Lipsa obiecțiilor și propunerilor.	
5.	**Ministerul Energiei** *(Nr. 10-2010 din 28.11.2023)*		Lipsa obiecțiilor și propunerilor.	
6.	**Ministerul Sănătății** *(Nr. 27/4514 din 29.11.2023)*		Lipsa obiecțiilor și propunerilor.	
7.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(Nr. 21-6041 din 28.11.2023)*		Lipsa obiecțiilor și propunerilor.	

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
8.	**Ministerul Muncii și Protecției Sociale** *(Nr. 22/5066 din 07.12.2023)*		Lipsa obiecțiilor și propunerilor.	
9.	**Ministerul Mediului** *(Nr.13-05/2856 din 01.12.2023)*		Lipsa obiecțiilor și propunerilor.	
10.	**Ministerul Justiției** *(Nr. 04/2-10472 din 29.11.2023)*	***La proiectul legii:***		
		7)	**La Art. I**, la sursa publicării *Legii nr. 1456/1993 cu privire la activitatea farmaceutică*, textul „Republicat:" se va substitui cu cuvintele „republicată în" (observația este valabilă și pentru Art. V). Totodată, ținând cont de rigorile tehnicii legislative, noilor elemente structurale ale articolelor (în cazul dat, alineatelor), li se vor atribui numere în ordine consecutivă. Spre exemplu, la pct. 1, prin care se modifică art. 3, se va menționa că acesta se completează cu alineatul (5), dar nu (4^1). Observația dată este valabilă pentru toate cazurile similare din proiect.	**Se acceptă parțial.** Nu se acceptă doar propunerea de a atribui noilor elemente structurale, completate în finalul prevederilor de bază, a numerelor în ordine consecutivă ce urmează celor deja existente în actul modificat. Această propunere nu este argumentată nici din punct de vedere tehnico-legislatov, nici juridic, dar nici logic. Regula numerotării noilor elemente structurale cu numărul de ordine și indicii corespunzător trebuie să fie una aplicabilă tuturor situațiilor juridice. Legea nr. 100/2017, la art. 63 alin. (2), deși nu este destul de explicită, stabilește faptul că succesiunea elementelor structurale trebuie să fie una firească. Caracterul firesc presupune, în primul rând, lipsa excepțiilor. Autorul obiecției însă propune aplicarea, nejustificată de vreo utilitate, a unei excepții de la „firească" regulă de utilizare a numerotării cu cifra de bază și indicele corespunzător în cazul completărilor.
		8)	**La Art. III** textul „Codul navigației maritime comerciale nr. 599/1999" se va substitui cu textul	**Se acceptă.**

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			„Codul navigaţiei maritime comerciale al Republicii Moldova, aprobat prin Legea nr. 599/1999”.	
			La Art. IV:	
		9)	la pct. 1, dispoziția se va expune după cum urmează: „La articolul 3 noțiunea *„securitate cibernetică”* va avea următorul cuprins:”, urmată de redarea integrală a acesteia, expusă din alineat;	**Se acceptă.**
		10)	la pct. 4, cuvintele „titlul articolului” se vor substitui cu cuvintele „denumirea articolului” (a se vedea: art. 51 alin. (2) din *Legea nr. 100/2017 cu privire la actele normative)*;	**Se acceptă.**
		11)	la pct. 5, prin care se propune noua redacție a lit. b) de la art. 22, urmează a fi concretizat domeniul de competență, deoarece în cazul dat sunt stabilite competențele Guvernului în sfera formării și utilizării resurselor informaționale de stat și a informatizării.	**Se acceptă.**
		12)	Cu referire la **Art. XII**, remarcăm că cele propuse spre completare la art. 16 din *Legea nr. 102/2017 cu privire la dispozitivele medicale*, nu se integrează armonios în conținutul acestui articol, care stabilește reglementări normative privind vigilența dispozitivelor medicale. Astfel, se recomandă completarea legii enunțate cu un articol distinct privind asigurarea securității cibernetice de către producătorii de dispozitive medicale (observație valabilă și pentru **Art. XVIII**, prin care se propun unele completări la art. 11 și 12 din *Legea nr. 277/2018 privind substanțele chimice*).	**Nu se acceptă.** În primul rând, poziția autorului obiecției nu este motivată corespunzător cerințelor stabilite de lege. Simpla afirmație că modificările propuse nu se integrează armonios nu este suficientă, cu atât mai mult în situația în care ministerul de resort nu a înaintat vreo obiecție pe marginea acestui aspect.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
		13)	**La Art. XVI**, în dispoziție, după denumirea *Legii nr. 142/2018 cu privire la schimbul de date și interoperabilitate* se va indica corect izvorul publicării acesteia – „(Monitorul Oficial al Republicii Moldova, 2018, nr. 295–308, art. 452)”.	**Se acceptă.**
		14)	**La Art. XXI**, ce vizează modificarea *Codului transportului feroviar nr. 19/2022*, în vederea asigurării respectării principiilor de legiferare, se recomandă modificarea propusă la art. 26 să fie plasată la art. 89.	
		15)	**La Art. XXIII** alin. (1), semnalăm că textul „cu excepția prevederilor art. IV punctele 2, 4-6 și XVIII care intră în vigoare la data publicării legii” este în dezacord cu faptul intrării în vigoare la data de 1 ianuarie 2025 a *Legii nr. 48/2023*, în concordanță cu care urmau să fie aduse actele normative respective. Astfel, modificările propuse prin proiect nu pot intra în vigoare înainte de data intrării în vigoare a *Legii nr. 48/2023*.	**Nu se acceptă.** Tocmai prevederile evidențiate sunt cele care pot intra în vigoare la data publicării legii și nu odată cu intrarea în vigoare a Legii nr. 48/2023. În cazul prevederilor art. IV intrarea imediată în vigoare este determinată de natura de clarificare a acestor prevederi în ceea ce privește competența unor autorități publice în domeniul informatizării și resurselor informaționale de stat și ajustarea acesteia la prevederile cadrului normativ general de organizare și funcționare a administrației publice centrale de specialitate. În ceea ce privește art. XVIII, intrarea în vigoare a modificărilor la Legea nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar este determinată de necesitatea asigurării condițiilor legale pentru instituirea și asigurarea funcționalității de către Guvern a autorității competente în domeniul securității cibernetice.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
		16)	Totodată, alin. (2) se va exclude, întrucât competența Guvernului de a aduce actele sale normative în concordanță cu *Legea nr. 48/2023*, precum și de a asigura elaborarea și adoptarea actelor normative necesare punerii în aplicare a prevederilor acestei legi, este prevăzută la art. 23 alin. (2) lit. c) din *Legea nr. 48/2023*.	**Se acceptă.** Alineatul (2) a fost exclus.
11.	**Serviciul de Informații și Securitate** *(Nr. E/13108 din 30.11.2023)*	17)	Potrivit art. 4 alin. (2) din Legea nr. 48/2023, *Guvernul aprobă lista sectoarelor și subsectoarelor critice și, corespunzător, a tipurilor și categoriilor de persoane juridice care prestează servicii în sectoarele și subsectoarele respective, stabilește cadrul metodologic privind identificarea persoanelor juridice de drept public și a celor de drept privat ca fiind furnizori de servicii, precum și modul de întocmire, ținere și actualizare a listei furnizorilor de servicii.* Prin urmare, în conformitate cu dispoziția legală citată *supra*, preponderent, trebuie ca Guvernul să aprobe lista sectoarelor și subsectoarelor, dar și tipurile și categoriile de persoane juridice care urmează să cadă sub incidența prevederilor Legii privind securitatea cibernetică, precum și cadrul metodologic de identificare a acestora. Astfel, completarea legilor sectoriale (Art. I – III, V, VII – XV, și XVIII - XXII) cu prevederile propuse prin care se stabilesc acele sectoare critice, contravine normei de la art. 4 alin. (2) din Legea nr. 48/2023.	**Nu se acceptă.** Propunerile de modificare a legilor sectoriale, de rând cu obiectivul de aducere în concordanță a cadrului legal cu Legea privind securitatea cibernetică, se înscriu în contextul mai larg de continuare a procesului de armonizare a legislației naționale la prevederile Directivei NIS2. Deși Legea nr. 48/2023 deleagă Guvernului competența de a stabili sectoarele subsectoarele, tipurile și categoriile de furnizori de servicii, aceasta nu implică un rol determinant a acestei decizii a Guvernului în finalizarea constituirii cadrului normativ primar în acest domeniu, inclusiv după cum a fost menționat, pentru a armoniza legislația națională la prevederile Directivei NIS2. În context, notăm că anexele I și II la Directiva NIS2 stabilesc sectoarele și subsectoarele critice și tipologia entităților esențiale și importante, care intră în domeniul de aplicare al acesteia. Tipologia acestor entități este determinată de prevederile relevante, menționate de altfel în aceste anexe, din actele

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
				normative ale UE care reglementează sectoarele/subsectoarele respective. În consecință, în cazurile materializate în modificările propuse în proiectul de lege, a fost posibilă determinarea, în baza unei analize comparative formal-juridice, a tipologiei corespondente în legislația națională prin identificarea termenilor care înglobează tipurile de entități enumerate în anexele Directivei NIS2. Suplimentar menționăm că, având caracter de norme juridice primare, modificările propuse la legile sectoriale vor constitui în comun cu prevederile Legii privind securitatea cibernetică un corp juridico-legal comun în acest domeniu și, în această calitate, pe cale de consecință, și unul din temeiurile juridice pentru actul normativ guvernamental menționat la art. 4 alin. (2) din legea nr. 48/2023.
		18)	La articolul IV din proiect (ce vizează modificarea **Legii nr.467/2003 cu privire la informatizare și la resursele informaționale de stat**): În scopul asigurării continuității funcționării și rezilienței sistemelor și resurselor informaționale de stat, se propune completarea Legii nr. 467/2003 cu articolul 7^7, cu următorul conținut: „**Articolul 7^7.** Păstrarea informațiilor din cadrul sistemelor și resurselor informaționale de stat în afara teritoriului Republicii Moldova	**Nu se acceptă.** Deși considerăm că o astfel de prevedere legală este necesară într-o formă sau alta în cadrul normativ primar al țării, totuși această propunere depășește obiectul de reglementare al proiectului de lege propuse spre avizare.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			(1) Păstrarea informației din sistemele și resursele informaționale de stat în afara teritoriului Republicii Moldova, poate fi realizată doar pe teritoriul unui stat membru al Uniunii Europene, în baza unui acord interguvernamental. (2) Condițiile și modul de păstrare a informației din sistemele și resursele informaționale de stat în afara teritoriului Republicii Moldova este stabilit de Guvern.”	
		19)	Cu referire la articolul XIII din proiect (ce vizează modificarea **Legii nr. 120/2017 cu privire la prevenirea și combaterea terorismului**): Potrivit pct. 9 din Capitolul 31 din Planul național de acțiuni pentru aderarea Republicii Moldova la Uniunea Europeană pe anii 2024-2027, aprobat prin Hotărârea Guvernului nr. 829/2023, către finele anului 2025 urmează a fi adoptată Legea de transpunere a Directivei 2022/2257 privind reziliența entităților critice și de abrogare a Directivei 2008/114/CE a Consiliului. Astfel, menționăm că potrivit art. 1, alin. (2) din Directiva 2022/2557, se impune o abordare coordonată a Directivei nominalizate cu Directiva 2022/2555, având în vedere relația dintre securitatea fizică și securitatea cibernetică a entităților critice. În acest sens, urmează a se ține cont că, odată cu intrarea în vigoarea a Legii menționate supra, autoritatea competentă în domeniul securității cibernetice, va informa despre încălcările legislației constatate în cadrul controlului exercitat	Autoritățile publice în exercitarea prerogativelor de putere publică, indiferent de domeniile de activitate, nu sunt doar în drept, ci obligate să coopereze, atunci când interesele statului sau ale societății în general o cer. Schimbul de informații ca o formă de materializare a acestei cooperări este o condiție indispensabilă inclusiv și mai ales pentru domeniul securității cibernetice. În ceea ce privește exercitarea supravegherii și controlului modului de asigurare a securității cibernetice, fiind o prerogativă exclusivă a autorității competente în baza Legii nr. 48/2023, furnizarea anumitor informații de către aceasta trebuie justificată nu doar formal-juridic, ci și reieșind din fondul chestiunii abordate: dacă o entitate publică nu are competență într-un anumit domeniu, care este utilitatea furnizării unor informații din acest domeniu autorității respective? Bineînțeles că informația care i-a devenit cunoscută în procesul de exercitare a competenței sale va

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			asupra operatorilor obiectivelor de infrastructură critică privind modul în care aceștia respectă obligațiile de asigurare a securității cibernetice, atât Centrul Antiterorist, cât și autoritatea competentă în domeniul rezilienței entităților critice.	trebui distribuită de către autoritatea competentă autorităților relevante, dacă această informație intră în domeniul de competență a ultimilor. Prevederea invocată de către autorul obiecției din Directiva CER urmează a fi interpretată în contextul nu doar a întregului alineat, și anume că Directiva CER nu se aplică aspectelor reglementate de Directiva NIS2, iar punerea în aplicare coordonată urmează a fi înțeleasă nu ca informarea unilaterală de către autoritatea competentă în domeniul securității cibernetice a anumitor autorități competente în temeiul Directivei CER. În acest context, este relevant recitalul (13) din preambulul la Directiva CER *„...Pentru a realiza o abordare cuprinzătoare, statele membre ar trebui să se asigure că strategiile lor oferă un cadru de politică pentru o coordonare consolidată între autoritățile competente în temeiul prezentei directive și autoritățile competente în temeiul Directivei (UE) 2022/2555 în contextul schimbului de informații privind riscurile de securitate cibernetică, amenințările cibernetice și incidentele cibernetice și riscurile, amenințările și incidentele non-cibernetice, precum și în contextul exercitării sarcinilor de supraveghere.”*. Cu alte cuvinte, cooperarea și schimbul de informații presupune reciprocitate și încredere în primul rând.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
12.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/1612/23 din 27.11.2023)*		Lipsa obiecțiilor și propunerilor.	
13.	**Agenția de Guvernare Electronică** *(Nr. 3007 – 258 din 28.11.2023)*		Lipsa obiecțiilor și propunerilor.	
14.	**Comisia Națională a Pieței Financiare** *(Nr. 03-4/3451 din 29.11.2023)*	20)	Potrivit obiectului de reglementare al Legii nr. 48/2023 privind securitatea cibernetică (Legea nr. 48/2023), acesta stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică și instituie cerințe, măsuri și mecanisme în scopul asigurării securității rețelelor și sistemelor informatice, care sunt esențiale pentru funcționarea societății și al gestionării incidentelor cibernetice. În acest sens, autoritatea competentă, care va fi desemnată de către Guvern, va întocmi și ține lista furnizorilor de servicii, conform normei stipulate în art. 4 din proiectul de Lege prenotat, care va cuprinde cel puțin tipul, categoria furnizorului de servicii și sectorul/subsectorul critic în care se prestează serviciul respectiv. Dat fiind faptul că, la momentul actual, nu au fost adoptate acte normative privind desemnarea autorității competente, în corespundere cu prevederile art. 23	**Nu se acceptă.** Propunerile de modificare a legilor sectoriale, de rând cu obiectivul de aducere în concordanță a cadrului legal cu Legea privind securitatea cibernetică, se înscriu în contextul mai larg de continuare a procesului de armonizare a legislației naționale la prevederile Directivei NIS2. Deși Legea nr. 48/2023 deleagă Guvernului competența de a stabili sectoarele subsectoarele, tipurile și categoriile de furnizori de servicii, aceasta nu implică un rol determinant a acestei decizii a Guvernului în finalizarea constituirii cadrului normativ primar în acest domeniu, inclusiv după cum a fost menționat, pentru a armoniza legislația națională la prevederile Directivei NIS2. În context, notăm că anexele I și II la Directiva NIS2 stabilesc sectoarele și subsectoarele

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			alin. (2) lit. c) din Legea nr. 48/2023, precum și nu a fost elaborată Lista furnizorilor de servicii, relevăm asupra necesității **excluderii propunerilor de modificare la Legea nr. 171/2012 privind piața de capital (art. VII din proiectul de Lege).**	critice și tipologia entităților esențiale și importante, care intră în domeniul de aplicare al acesteia. Tipologia acestor entități este determinată de prevederile relevante, menționate de altfel în aceste anexe, din actele normative ale UE care reglementează sectoarele/subsectoarele respective. În consecință, în cazurile materializate în modificările propuse în proiectul de lege, a fost posibilă determinarea, în baza unei analize comparative formal-juridice, a tipologiei corespondente în legislația națională prin identificarea termenilor care înglobează tipurile de entități enumerate în anexele Directivei NIS2. Suplimentar menționăm că, având caracter de norme juridice primare, modificările propuse la legile sectoriale vor constitui în comun cu prevederile Legii privind securitatea cibernetică un corp juridico-legal comun în acest domeniu și, în această calitate, pe cale de consecință, și unul din temeiurile juridice pentru actul normativ guvernamental menționat la art. 4 alin. (2) din Legea nr. 48/2023.
		21)	Mai mult ca atât, în contextul în care autorii proiectului s-au condus de Directiva NIS2 și s-a constatat faptul că sectorul infrastructurii pieței financiare este de importanță critică, informăm că nu toate societățile de investiții sunt considerate	**Precizare.** Nici proiectul de lege nu cuprinde propuneri de modificare care ar cuprinde formulări ce ar induce ideea exhaustivității conținutului normelor juridice respective. Potrivit

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			furnizori de servicii, or potrivit Anexei nr. 1 din Directivă, furnizori de servicii pe piețele de capital se referă la operatorii de piețe reglementate și sistemele multilaterale de tranzacționare (MTF), cât și Contrapărțile centrale (CPC). Menționăm că operatorii de piețe reglementate pot fi Bursele de Valori și societățile de investiții - doar în cazul obținerii autorizației și indeplinirii cerințelor și rigorilor prevăzute de legislație pentru o astfel de activitate. Concretizăm că, în Republica Moldova, la momentul actual nici o societate de investiții nu are autorizație de exploatarea MTF. Deasemenea, la nivel local, nu există nici o Contraparte centrală, în sensul definiției enunțate în art. 1 pct. 1 din Regulamentul (UE) nr. 648/2012 al Parlamentului European și al Consiliului privind instrumentele financiare derivate extrabursiere, contrapărțile centrale și registrele centrale de tranzacții.	formulării redacționale se au în vedere doar operatorii de piață sau societățile de investiții, care vor fi identificați de autoritatea competentă în conformitate cu cadrul metodologic ce urmează a fi aprobat de Guvern în temeiul art. 4 alin. (2) din Legea nr. 48/2023.
15.	**Agenția Medicamentului și Dispozitivelor Medicale** *(Nr. Rg02 – 005180 din 24.11.2023)*		Lipsa obiecțiilor și propunerilor.	
16.	**Banca Națională a Moldovei** *(Nr. 31-002/166/6716 din 21.12.2023)*	22)	BNM urmează a fi exceptată din rândul subiecților cărora le este aplicabilă legea privind securitatea cibernetică, având în vedere, pe de o parte, imperativul de menținere și consolidare a autonomiei băncii centrale (inclusiv în virtutea angajamentelor asumate de Republica Moldova prin Acordul de Asociere RM-UE) și mecanismele	**Precizare.** În principiu opinia BNM pe marginea proiectului de lege prezentat spre avizare și, implicit, asupra unor prevederi ale Legii nr. 48/2023 privind securitatea cibernetică sunt pertinente problematicii finalizării constituirii în Republica Moldova a unui model de

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			intruzive de supraveghere și control, prevăzute în proiectul de lege, care impactează această autonomie, pe de altă parte. Mai mult, Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (în continuare - Directiva (UE) 2022/2555), prevederile căreia sunt transpuse de Legea nr. 48/2023 privind securitatea cibernetică, prin art. 6 pct.35) exclude expres băncile centrale din domeniul de aplicare al acestei Directive. Important, potrivit opiniei Băncii Centrale Europene pe marginea proiectului Directivei (UE) 2022/2555, exceptarea s-ar aplica la toate misiunile *și competențele fundamentale ale* Băncii Centrale, inclusiv sisteme de plăți.[1] Având în vedere cele menționate *supra,* considerăm că prin proiectul supus avizării urmează a fi remediate deficiențele admise la elaborarea Legii nr. 48/2023 privind securitatea cibernetică, în vederea asigurării obiectivului statuat al proiectului – corelarea cadrului legal existent cu prevederile Legii nr. 48/2023 privind securitatea cibernetică. Corespunzător, propunem completarea proiectului de lege cu un articol nou, care prevede exceptarea	guvernanță în domeniul securității cibernetice care să corespundă principiilor eficienței și eficacității, principii care în ultimă instanță trebuie să asigure o astfel de funcționalitate a entităților responsabile care să aibă ca efect, pe termen mediu și lung, creșterea continuă a rezilienței cibernetice în țara noastră. Totuși, pertinența argumentelor invocate nu implică suficientă concludență acestora pentru obiectivele urmărite de legea respectivă și contextul în care aceasta a fost adoptată și publicată și urmează pe cale de consecință, să fie pusă în aplicare, reieșind din următoarele. Legea nr. 48/2023 privind securitatea cibernetică asigură o armonizare doar parțială a Directivei NIS2. Această parțialitate este însă determinată nu doar de faptul că Republica Moldova nu este un stat membru al UE, ci mai degrabă de faptul că țara noastră nu a implementat în legislația sa națională Directiva NIS. Or, trebuie să ținem cont de faptul că raportul dintre aceste două acte legislative ale UE este unul de succesivitate ascendentă în uniformizarea instrumentelor juridico-normative la nivelul statelor membre ale UE pentru realizarea obiectivelor de creștere a rezilienței la nivelul Uniunii. Prin urmare,

[1] pct. 1.2 din Avizul Băncii Centrale Europene din 11 aprilie 2022: *„BCE constată că, în abordarea sa generală cu privire la directiva propusă, Consiliul propune o modificare pentru a exclude „entitățile care desfășoară activități în domeniul judiciar, al parlamentelor sau al băncilor centrale" din sfera de aplicare al directivei propuse. BCE înțelege că modificarea propusă s-ar extinde la toate misiunile și competențele fundamentale ale Sistemului European al Băncilor Centrale (SEBC), astfel cum sunt prevăzute la articolul 127 alineatul (2) din tratat și la articolul 3.1 din Statutul Sistemului European al Băncilor Centrale și al Băncii Centrale Europene, cum ar fi promovarea bunei funcționări a sistemelor de plăți […]".* Link Aviz BCE:https://op.europa.eu/ro/publication-detail/-/publication/227d3a03-ed0e-11ec-a534-01aa75ed71a1/language-ro

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			BNM de la dispozițiile Legii nr. 48/2023 privind securitatea cibernetică.	transpunerea de către Statele Membre ale UE a Directivei NIS2 nu poate fi înțeleasă și nici realizată practic fără efectiva transpunere într-o primă etapă a Directivei NIS. Această caracteristică este una fundamentală pentru crearea în Republica Moldova a unui model de guvernanță în domeniul securității cibernetice atât sub aspect formal (procesul de armonizare a legislației naționale la cea europeană), cât și din punct de vedere practic (instituirea cadrului instituțional, punerea în aplicare a unor mecanisme viabile de cooperare, cooptarea sectorului privat în creșterea rezilienței cibernetice a țării, etc). Din această perspectivă, deși unul dintre obiectivele formal juridice declarate ale Legii nr. 48/2023 este cel de armonizare a legislației naționale la prevederile Directivei NIS2, totuși la nivel practic, elemente reglementate de legea moldovenească sunt comune pentru ambele Directive. Cu toate că Legea nr. 48/2023 cuprinde reglementări de armonizare la Directiva NIS2, totuși aceasta are în cuprinsul său și elemente care ar putea fi mai degrabă asignate exclusiv conceptului reglementativ al Directivei NIS, în mod special ne referim aici la cadrul de supraveghere care, în legea moldovenească, este unul ex-post pentru toți furnizorii de servicii, neavând caracteristicile reglementărilor din Directiva NIS2: supraveghere ex-ante pentru entitățile esențiale

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
				și ex-post pentru cele importante; precum și la cadrul de asigurare a respectării legii , nici Legea nr. 48/2023, nici propunerile de completare a legislației naționale cu componențe contravenționale (acestea nu sunt parte a proiectului în speță, fiind înaintate Ministerului Justiției pentru promovare centralizată a modificărilor la Codul contravențional) nu au ca obiectiv armonizarea legislației naționale în ceea ce privește aplicarea legii. Or, sancțiunile propuse în inițiativa respectivă înaintată Ministerului Justiției nici pe departe nu corespund sancțiunilor prevăzute în Directiva NIS2. Această soluție este una optimă pentru țara noastră având în vedere că Republica Moldova este într-o fază incipientă de creare a unor mecanisme inclusiv instituționale în domeniul securității cibernetice la nivel național. Din acest punct de vedere într-o primă etapă evitarea punerii accentului pe caracterul represiv al normei juridice ar putea constitui un fundament serios pentru asigurarea încrederii și cooperării reciproce mutuale dintre autoritățile publice responsabile în domeniu și sectorul privat în mod special. Referitor la opinia BCE, ținem să relevăm faptul că în spatele caracterului pozitiv al acesteia față de propunerea de atunci a Directivei NIS2 stă în principal existența deja a unui cadru normativ european și, implicit

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
				național al statelor membre ale UE, mai mult sau mai puțin coerent și definit de asigurare a securității cibernetice în sectorul financiar-bancar, inclusiv și în mod special din perspectiva supravegherii băncilor naționale. Referindu-se la competențele Sistemului European al Băncilor Centrale și ale Eurosistemului în materie de monitorizare, BCE opinează că „...În exercitarea rolului său de supraveghere, BCE a adoptat Regulamentul Băncii Centrale Europene (UE) nr. 795/2014 (BCE/2014/28) (11) (denumit în continuare „Regulamentul SIPS"), care transpune principiile CPSS-IOSCO pentru infrastructurile piețelor financiare în legislație direct aplicabilă.". Aceste realități nu sunt caracteristice contextului din Republica Moldova dat, după cum deja am menționat, și de lipsa statutului de membru al UE al țării noastre și de armonizarea parțială sau lipsa de armonizare a legislației naționale la actele legislative ale UE relevante din perspectiva obligațiilor de asigurare a securității cibernetice de către persoanele juridice de drept public, inclusiv BNM. Astfel trebuie să avem în vedere faptul că totuși norma juridică este emanația unei voințe politice de reglementare a unor relații sociale ce se constituie într-un cadru circumstanțial definit factologic. Contextul respectiv pentru Republica Moldova este dat în primul rând de

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
				statutul de stat non membru al UE. Pe cale de consecință armonizarea absolută a legislației naționale la directivele UE este în mod obiectiv imposibilă, cu atât mai mult a regulamentelor UE care în statele membre au o aplicabilitate directă. Astfel, odată cu obținerea de către Republica Moldova a statutului de stat membru al UE, contextul respectiv se va schimba fundamental, aceasta urmând a constitui temei suficient pentru revizuirea nu doar a Legii nr. 48/2023, ci a întregului cadru normativ național.
		23)	În continuare, cu referire la Art. XV din proiectul de lege prin care se propun modificări la Legea nr. 202/2017 privind activitatea băncilor (în continuare - Legea nr. 202/2017), atenționăm că astfel de modificări sunt improprii obiectului de reglementare al Legii nr. 202/2017. Susținem includerea unor prevederi care fortifică exigențele înaintate față de securitatea cibernetică în bănci, însă atenționăm asupra faptului că monitorizarea și supravegherea respectării prevederilor Legii nr. 202/2017 este apanajul exclusiv al BNM. În aceeași ordine de idei, atenționăm că prin proiectul de lege pentru modificarea unor acte normative (consolidarea cadrului de activitate al Băncii Naționale a Moldovei), nr. unic 988/MF/BNM/2023, au fost propuse modificări la Legea nr. 202/2017 cu referire la cerințele înaintate față de sistemele și serviciile eficiente aferente tehnologiilor informaționale și de	**Se acceptă.** Articolul respectiv a fost exclus. În consecință prevederile Legii 48/2023 vor trebui aplicate în măsura în care anumite situații juridice nu sunt reglementate, inclusiv prin prisma principiilor enunțate la art. 3 alin. (5) din Legea nr. 48/2023, de legislația sectorială cu caracter special. De asemenea, trebuie să remarcăm că, din perspectiva exercițiului de către Agenția de Securitate Cibernetică a funcției de supraveghere și control, pentru punerea în aplicare a prevederilor Legii nr. 48/2023 prin reglementarea modului de supraveghere și control al respectării acestei legi, urmează, în comun cu Banca Națională a Moldovei să fie identificate mecanisme fiabile de coordonare a eforturilor în procesul de asigurare a respectării prevederilor acestei legi.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			comunicare (TIC) în bănci și securitatea cibernetică (în mare parte preluate din Ghidul Autorității Bancare Europene privind administrarea riscurilor privind tehnologia informațiilor și comunicațiilor (TIC) și de securitate (EBA/GL/2019/04)). În același context, menționăm că, prin Regulamentul nr. 47/2018 privind cerințele minime pentru sistemele informaționale și de comunicare ale băncilor, BNM a prescris băncilor implementarea unui șir de măsuri în vederea gestiunii eficiente a riscurilor TIC. BNM evaluează cadrul intern aferent TIC în fiecare bancă, în raport cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă și cu profilul/apetitul de risc în cadrul controalelor desfășurate la bancă și poate aplica măsuri de supraveghere și sancțiuni în cazul identificării riscurilor sau încălcărilor în acest domeniu. În această ordine de idei, semnalăm că unele competențe de reglementare, supraveghere și control ale autorității competente în domeniul securității cibernetice (prevăzute în Legea nr. 48/2023 privind securitatea cibernetică), în raport cu băncile, s-ar putea suprapune cu competențele menționate supra ale BNM. Mai mult, opinăm că o astfel de suprapunere de competențe ar putea crea impedimente procesului de supraveghere efectuat atât de BNM, cât și de către autoritatea competentă în domeniul securității cibernetice.	Mecanismele respective bineînțeles urmează să asigure evitarea suprapunerii de competențe dintre BNM și ASC și, cu atât mai mult intrusiunile reciproce nejustificate. În ce privește caracterul de lege specială al Regulamentului DORA în raport cu prevederile Directivei NIS2, considerăm important să remarcăm faptul că această relație decurge din caracterul orizontal al cadrului de reglementare oferit de Directiva NIS2. Această caracteristică este extrapolată și la nivel național prin articolul 3 alineatele (5) și (6) din Legea nr. 48/2023. În situația în care legile sectoriale în domeniul financiar bancar vor stabili cerințe de securitate și obligații de notificare cel puțin echivalente cu cele prevăzute de Legea nr. 48/2023 și actele de punere a acesteia în aplicare, atunci legile sectoriale bineînțeles vor cele care vor reglementa raporturile juridice respective. Din considerentele expuse mai sus este eronat să considerăm că Directiva NIS2 exceptează expres entitățile financiare din domeniul său de aplicare. Din contra aceste entități urmează a fi identificate ca atare nu doar în baza Directivei NIS2, ci și a Directivei privind reziliența entităților critice (așa-numita Directiva CER). Astfel, nici art. 4 alin. 1 din Directiva NIS, nici recitalul (28) din preambulul la această Directivă nu exclud entitățile financiare din sfera de aplicare a Directivei NIS2. Aceste

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			În acest context, remarcăm că la nivelul Uniunii Europene reziliența operațională și securitatea cibernetică în sectorul financiar este reglementată de Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar (în continuare - Regulamentul (UE) 2022/2554). Acest regulament este aplicabil inclusiv băncilor și prevede cerințe uniforme privind securitatea rețelelor și a sistemelor informatice care sprijină procesele operaționale ale entităților financiare. Observăm în acest sens că, Directiva (UE) 2022/2555 exceptează expres de la prevederile acesteia, entitățile financiare care fac obiectul Regulamentului (UE) 2022/2554, astfel, atât la art. 4 alin. (1) din Directiva (UE) 2022/2555, cât și în preambulul acestea (pct. 28) este stipulat că: „Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului ar trebui considerat a fi un act juridic sectorial al Uniunii în legătură cu prezenta directivă în ce privește entitățile financiare. Dispozițiile Regulamentului (UE) 2022/2554 referitoare la gestionarea riscurilor legate de tehnologia informației și comunicațiilor (TIC), la gestionarea incidentelor legate de TIC și, în special, la raportarea incidentelor majore legate de TIC, precum și la testarea rezilienței operaționale digitale, la acordurile privind schimbul de informații și la riscurile TIC generate de părți terțe ar trebui să se aplice în locul celor	prevederi doar stabilesc principiile de aplicare a legislației, în mod special raportul dintre legea specială și cea generală. În același context este important de remarcat faptul că în procesul de identificare a furnizorilor de servicii și exercitare a supravegherii modului cum aceștia implementează legea, autoritatea competentă în temeiul Legii nr. 48/2023 urmează să determine echivalența și implicit aplicabilitatea reglementărilor sectoriale în raport cu cele ale Legii nr. 48/2023 și să acționeze în consecință.

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			prevăzute în prezenta directivă. Prin urmare, statele membre nu ar trebui să aplice dispozițiile prezentei directive privind gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare, supraveghere și aplicarea legii, entităților financiare care fac obiectul Regulamentului (UE) 2022/2554. În același timp, este important ca, în temeiul prezentei directive, să se mențină o relație puternică cu sectorul financiar și să se facă un schimb de informații cu acesta […]". În consecință, atenționăm că armonizarea parțială a legislației europene în domeniul securității cibernetice, prin transpunerea (viciată) a Directivei (UE) 2022/2555, fără transpunerea corelativă și simultană a Regulamentului (UE) 2022/2554, poate conduce la soluții eronate și riscante în cazul sectorului bancar, cu potențiale suprapuneri de competențe și incertitudini, care ar putea compromite obiectivul final de consolidare a rezilienței sectorului bancar față de riscurile cibernetice. Din considerentele expuse *supra*, Banca Națională a Moldovei, propune completarea proiectului de lege cu următoarele prevederi:	
			1. Exceptarea expresă a Băncii Naționale a Moldovei de la domeniul de aplicare al Legii nr. 48/2023 privind securitatea cibernetică (asigurând, astfel, transpunerea corespunzătoare a Directivei (UE) 2022/2555);	**Nu se acceptă.** (poziție argumentată mai sus).

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
			2. Excluderea din proiectul de lege a Art. XV prin care se propun modificări la Legea nr. 202/2017 privind activitatea băncilor (Monitorul Oficial al Republicii Moldova, 2017, nr. 434–439, art. 727);	**Se acceptă.**
			3. La articolul 1 alineatul (2) din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, după textul ”nestatale”, propunem completarea cu textul ”resurselor informaționale ale Băncii Naționale a Moldovei,”. Propunerea de completare a art. 1 alin. (2) din Legea nr. 467/2003 vine doar să precizeze statutul juridic actual al Băncii Naționale a Moldovei, care nu se circumscrie domeniului de aplicare al Legii nr. 467/2003 în virtutea garanțiilor de independență funcțională (care derivă atât din cadrul legal în vigoare, dar și din standardele internaționale în domeniul bancar), fapt comunicat prin corespondența dintre Banca Națională a Moldovei și Agenția de Guvernare Electronică.	**Nu se acceptă.** Această propunere depășește obiectul de reglementare a proiectului de lege propus spre avizare.
			Adițional, confirmăm că BNM va examina opțiunile de transpunere a Regulamentului (UE) 2022/2554 (lege, act normativ subordonat legii) și va demara procesul de transpunere a acestuia, cel puțin cu referire la categoriile de subiecți care sunt supravegheați de BNM.	**Se acceptă.**
17.	**Agenția Națională pentru Siguranța Alimentelor** *(Nr. 10-5665 din 28.11.2023)*		Lipsa obiecțiilor și propunerilor.	

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
18.	**Centrul pentru Comunicare Strategică și Combatere a Dezinformării**		Nu a prezentat avizul.	
19.	**Centrul de Armonizare a Legislației** *(Nr. 31/02-69-12155)*		Lipsa obiecțiilor și propunerilor.	
20.	**Centrul Național Anticorupție** *(Nr. 06/2/18443 din 20.11.2023)*		Se va remite spre avizare proiectul definitivat.	

REAVIZARE

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
21.	**Ministerul Finanțelor** *(Nr. 07/3-03-8/73 din 15.01.2024)*	1.	Potrivit modificărilor/completărilor la proiectul legii, supus reavizării se propune completarea Art.IV privind modificarea Legii nr.467/2003 cu privire la informatizare și la resursele informaționale de stat, cu articolul 7^7 referitor la prevederile de *păstrare a informațiilor din cadrul sistemelor și resurselor informaționale de stat în afara teritoriului Republicii Moldova*. Respectiv, urmează a fi completată nota informativă de către autor în vederea aducerii clarității în	**Precizare** În contextul obiecțiilor prezentate de AGE, prevederile pentru completarea cu articolul 7^7 a Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat au fost excluse din proiect. Totodată, în rezultatul ședinței comune din data de 23.01.2024 cu participarea SIS, AGE, STISC MDED și Consilierul Președintelui Republicii Moldova în domeniul apărării și securității naționale Stanislav Secrieru, s-a coordonat

			contextul eventualelor necesități de resurse financiare suplimentare în vederea implementării normei date și/sau alocațiile bugetare aprobate în acest scop în Legea bugetului de stat pentru anul 2024.	următoarea redacție a articolului 22, litera e) a Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat: „e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene;”.
		2.	Suplimentar, remarcăm că Directiva (UE) 2022/2555, care este transpusă prin Legea nr. 48/2023, stabilește în Anexa 1 “Sectoarele cu o importanță critică ridicată” și în Anexa II „Alte sectoare de importanță critică”, precum și tipul entităților aferente acestor sectoare. Respectiv, în Anexa nr. 1 se identifică sectorul bancar și infrastructurile pieței financiare, precum și entitățile aferente acestora, cum sunt instituțiile de credit (băncile), operatorii de locuri de tranzacționare și contrapărțile centrale. În această ordine de idei, conform alin. (28) din preambulul Directivei 2022/2555, dispozițiile acestei Directive privind gestionarea riscurilor în materie de securitate cibernetică și obligațiile de raportare, supraveghere și aplicarea legii, nu ar trebui să se aplice entităților financiare care fac obiectul Regulamentului UE 2022/2554 privind reziliența operațională digitală a sectorului financiar, acesta fiind considerat un act juridic	**Nu se acceptă.** La nivel de cadru legislativ european, într-adevăr relația dintre Directiva NIS2[2] și Regulamentul DORA[3] este una de lex generalli – lex specialis. Cu toate acestea, atât entitățile din sectorul bancar, cât și cele din sectorul infrastructurii pieței financiare intră în domeniul de aplicare al Directivei NIS2. Mai mult, acestea intră și în domeniul de aplicare al Directivei CER[4] Caracterul de lege specială al Regulamentului DORA în raport cu prevederile Directivei NIS2, decurge din caracterul orizontal al cadrului de reglementare oferit de Directiva NIS2. Cu alte cuvinte, prevederile Directivei NIS2 se aplică în măsura în care anumite raporturi juridice nu sunt reglementate de Regulamentul DORA. Acest algoritm urmează a fi extrapolat și la nivel normativ național și este reflectat în art. 3 alin. (5) din Legea nr. 48/ 2023 privind securitatea cibernetică. Toate cele trei acte legislative europene au fost publicate concomitent în aceeași ediție a

[2] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555
[3] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0001.01.RON&toc=OJ%3AL%3A2022%3A333%3ATOC
[4] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557

			sectorial specific entităților financiare. În context, atragem atenția ca potrivit art.2 alin. (1) din Regulamentul 2022/2554, acesta se aplică acelorași instituții de credit (băncile), operatori de locuri de tranzacționare și contrapărților centrale. În aceste condiții, precum și în contextul avizului prezentat asupra proiectului la avizarea primară de către Comisia Națională a Pieței Financiare, în calitate de autoritate de reglementare a pieței de capital, considerăm că propunerile de modificare a Legii nr. 171/2012 privind piața de capital urmează a fi excluse din proiect, asupra oportunității acestora urmând a se reveni după transpunerea în legislația națională a Regulamentului 2022/2554, precum și după o analiză și evaluare a modului de aplicare corelată a celor 2 acte UE în legislația națională.	Jurnalului Oficial al UE. Aceasta denotă intenția legiuitorului european de a asigura o sincronicitate în procesul de implementare a acestor acte la nivel național de către Statele Membre ale UE. Având în vedere că o astfel de sincronizare a acțiunilor de implementare pe cele trei direcții în Republica Moldova este deja imposibil de realizat, soluția logică juridică este de asigurare a aplicabilității legii generale, adică a Legii nr. 48/2023 privind securitatea cibernetică. Odată cu armonizarea legislației naționale la prevederile Regulamentului DORA, bineînțeles că va trebui supusă unei examinări aprofundate și revizuirea prevederilor relevante ale Legii nr. 48/2023.
22.	**Ministerul Afacerilor Interne** *(Nr. 44/22 – 101 din 11.01.2024)*		Lipsa de obiecții sau propuneri.	
23.	**Ministerul Apărării** *(Nr. 11/38 din 15.01.2023)*		Lipsa de obiecții sau propuneri.	
24.	**Ministerul Afacerilor Externe și Integrării Europene** *(Nr. DI/3/041-217 din 10.01.2024)*		Lipsa de obiecții sau propuneri.	

25.	**Ministerul Energiei** *(Nr. 10-81 din 12.01.2024)*		Lipsa de obiecții sau propuneri.	
26.	**Ministerul Sănătății** *(Nr. 18/223 din 18.01.2024)*	3.	**La Art. I.** din proiect, pentru modificarea Legii nr. 1456/1993 cu privire la activitatea farmaceutică: 1) pct. 2, în alineatul $(2)^1$ propus, după cuvintele „persoanele juridice” se completează cu cuvintele „și fizice”;	**Se acceptă.** Din textul prevederii respective a fost exclus cuvântul „juridice”.
		4.	2) pct. 3, în alineatul $(4)^1$ propus: 2.1) după cuvintele „persoanele juridice” se completează cu cuvintele „și fizice”;	**Se acceptă.** Din textul prevederii respective a fost exclus cuvântul „juridice”.
		5.	2.2) cuvântul „creării” se substituie cu cuvântul „dezvoltării”.	**Nu se acceptă.** Propunerile respective păstrează terminologia utilizată de Legea nr. 1456/2023. Art. 9 al acesteia utilizează noțiunea de „creare”.
		6.	**La Art. XII.** din proiect, pentru modificarea Articolului 16 din Legea nr. 102/2017 cu privire la dispozitivele medicale, se propune completarea cu alineatele $(1)^1$ și $(1)^2$, relevantă fiind includerea conținutului alineatelor $(3)^1$ și $(3)^2$ după alineatul (1), și nu după alineatul (3).	**Se acceptă.**
27.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(Nr.21/1-96 din 09.01.2023)*		Lipsa de obiecții sau propuneri.	

28.	**Ministerul Muncii și Protecției Sociale** *(Nr. 22/178 din 12.01.2024)*		Lipsa de obiecții sau propuneri.	
29.	**Ministerul Mediului** *(Nr. 13-05/98 din 16.01.2024)*		Lipsa de obiecții sau propuneri.	
30.	**Ministerul Justiției** *(Nr. 04/2-525 din 18.01.2024)*	Obiecții de ordin conceptual nu avem de formulat. Aferent rigorilor de tehnică legislativă, se vor reține următoarele: ***La proiectul legii:***		
		7.	**La Art. I** *(Legea nr. 1456/1993 cu privire la activitatea farmaceutică)*, atenționăm că noilor elemente structurale ale articolelor (în cazul dat, alineatelor), li se vor atribui numere în ordine consecutivă, dar nu numere cu indice. Spre exemplu, la pct. 1, prin care se modifică art. 3, se va menționa că acesta se completează cu alineatul (5), dar nu (41). Observația dată este valabilă pentru toate cazurile similare din proiect (pct. 2 și 3 din Art. I; Art. II; pct. 1 și 2 din Art. VII; pct. 1 și 2 din Art. IX; pct. 1 și 2 din Art. XI; Art. XII; Art. XV; Art. XVII; pct. 2 din Art. XIX).	**Nu se acceptă.** Această propunere nu este argumentată nici din punct de vedere tehnico-legislativ, nici juridic, dar nici logic. Regula numerotării noilor elemente structurale cu numărul de ordine și indicii corespunzător trebuie să fie una aplicabilă tuturor situațiilor juridice. Legea nr. 100/2017, la art. 63 alin. (2), deși nu este destul de explicită, stabilește faptul că succesiunea elementelor structurale trebuie să fie una firească. Caracterul firesc presupune, în primul rând, lipsa excepțiilor. Autorul obiecției însă propune aplicarea, nejustificată de vreo utilitate, a unei excepții de la „fireasca” regulă de utilizare a numerotării cu cifra de bază și indicele corespunzător în cazul completărilor.
		8.	**La Art. III** textul „Codul navigației maritime comerciale nr. 599/1999” se va substitui cu textul „Codul navigaţiei maritime comerciale	**Se acceptă.**

			al Republicii Moldova, aprobat prin Legea nr. 599/1999”.	
		9.	**La Art. IV:** în partea dispozitivă, după cuvintele „cu modificările ulterioare”, se vor exclude cuvintele „și se completează”. Semnalăm că, modificarea actului normativ constă în schimbarea oficială a textului actului, inclusiv a dispozițiilor finale sau tranzitorii, realizată prin modificări, excluderi sau completări ale unor părţi din text. Prin urmare, nu este necesară referința la completare, deoarece modificările includ și completări;	**Se acceptă.**
		10.	la pct. 3, în dispoziție, textul „cu următorul conținut:” se va substitui cu textul „cu următorul cuprins:”	**Precizare** În redacția transmisă spre reavizare pct. 3 al art. IV a fost exclus
		11.	**La Art. VII,** la sursa publicării Legii nr. 176/2013, după cuvintele „Monitorul Oficial” se va completa cu cuvintele „al Republicii Moldova”.	**Se acceptă.**
		12.	Cu referire la **Art. XII**, remarcăm că cele propuse spre completare la art. 16 din Legea nr. 102/2017 cu privire la dispozitivele medicale, nu se integrează armonios în conținutul acestui articol, care stabilește reglementări normative privind vigilența dispozitivelor medicale. Astfel, se recomandă completarea legii enunțate cu un articol distinct privind asigurarea securității cibernetice de către producătorii de dispozitive medicale (observație valabilă și pentru Art. XVII, prin care se propun unele completări la	**Se acceptă parțial.** La propunerea Ministerului Sănătății articolul respectiv a fost revizuit în sensul efectuării completărilor propuse în proiect nu după alineatul (3) al art. 16 din Legea nr. 102/2017, ci după alineatul (3). Nu a fost acceptată propunerea de a insera aceste completări într-un articol separat, deoarece art. 16 din Legea nr. 102/2017 are ca obiect de reglementare unele aspecte ce vizează managementul riscurilor și gestionarea incidentelor legate de dispozitivele medicale.

			art. 11 și 12 din Legea nr. 277/2018 privind substanțele chimice).	Propunerile de completare vizează aceleași aspecte doar că din perspectiva asigurării securității cibernetice a acestor dispozitive.
		13.	La **Art. XXII**, la pct. 1, în dispoziție, se va exclude cuvântul „nouă”, iar la pct. 2 se vor exclude cuvintele „în final”. Menționăm că, completarea unui text sau alineat, fără a specifica ordinea în care se inserează cuvintele, semnifică, conform regulii generale de tehnică legislativă, completarea textului la sfârșitul acestuia.	**Se acceptă.**
31.	**Serviciul de Informații și Securitate** *(Nr. E/370 din 16.01.2024)*		Lipsa de obiecții sau propuneri.	
32.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(Nr. 1.4/118/24 din 15.01.2024)*		Lipsa de obiecții sau propuneri	
33.	**Comisia Națională a Pieței Financiare** *(Nr. 03-4/122 din 17.01.2024)*	14.	Exprimăm convingerea că este imperativ să se reevalueze abordările și argumentele expuse de către CNPF anterior prin scrisoarea nr. 03-4/3451 din 29.11.2023. În susținerea argumentelor prezentate anterior, observăm că, potrivit art. 1 alin. (2) din Regulamentul UE 2022/2554 privind reziliența	**Nu se acceptă.** Suplimentar la argumentele expuse în cadrul avizării inițiale a proiectului relevăm următoarele. La nivel de cadru legislativ european, într-adevăr relația dintre Directiva NIS2[5] și Regulamentul DORA[6] este una de lex generalli – lex specialis.

[5] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555
[6] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=uriserv%3AOJ.L_.2022.333.01.0001.01.RON&toc=OJ%3AL%3A2022%3A333%3ATOC

			operațională digitală a sectorului financiar, în ceea ce privește entitățile financiare identificate drept entități esențiale sau importante în temeiul normelor naționale care transpun articolul 3 din Directiva (UE) 2022/2555 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (transpusă în legislația națională prin Legea nr. 48/2023), regulamentul prenotat este considerat un act juridic sectorial al Uniunii în sensul articolului 4 din directiva respectivă. În aceeași ordine de idei, în corespundere cu considerentul (28) și art. 4 alin. (1) din Directiva 2022/2555, regulile referitoare la gestionarea riscurilor în ceea ce privește securitatea cibernetică, precum și obligațiile de raportare, supraveghere și aplicare a legii, nu ar trebui să se aplice entităților financiare care fac obiectul Regulamentului UE 2022/2554 privind reziliența operațională digitală a sectorului financiar. În această conjunctură, Regulamentul UE 2022/2554 se aplică, inclusiv, operatorilor de locuri de tranzacționare, dar și contrapărților centrale (art. 2 alin. (1)). Prin urmare, în rezumat, având în vedere clauzele conform cărora prevederile semnalate ale Directivei în cauză sunt destinate entităților neincluse în actele juridice sectoriale ale Uniunii, proiectul urmează a fi supus unei revizuiri în lumina acestor considerații.	Cu toate acestea, atât entitățile din sectorul bancar, cât și cele din sectorul infrastructurii pieței financiare intră în domeniul de aplicare al Directivei NIS2. Mai mult, acestea intră și în domeniul de aplicare al Directivei CER[7] Caracterul de lege specială al Regulamentului DORA în raport cu prevederile Directivei NIS2, decurge din caracterul orizontal al cadrului de reglementare oferit de Directiva NIS2. Cu alte cuvinte, prevederile Directivei NIS2 se aplică în măsura în care anumite raporturi juridice nu sunt reglementate de Regulamentul DORA. Acest algoritm urmează a fi extrapolat și la nivel normativ național și este reflectat în art. 3 alin. (5) din Legea nr. 48/ 2023 privind securitatea cibernetică. Toate cele trei acte legislative europene au fost publicate concomitent în aceeași ediție a Jurnalului Oficial al UE. Aceasta denotă intenția legiuitorului european de a asigura o sincronicitate în procesul de implementare a acestor acte la nivel național de către Statele Membre ale UE. Având în vedere că o astfel de sincronizare a acțiunilor de implementare pe cele trei direcții în Republica Moldova este deja imposibil de realizat, soluția logică juridică este de asigurare a aplicabilității legii generale, adică a Legii nr. 48/2023 privind securitatea cibernetică. Odată cu armonizarea legislației naționale la prevederile Regulamentului DORA, bineînțeles că va trebui supusă unei examinări

[7] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557

				aprofundate și revizuirea prevederilor relevante ale Legii nr. 48/2023.
34.	**Agenția Medicamentului și Dispozitivelor Medicale** *(Nr. Rg02- 000056 din 10.01.2024)*		Lipsa obiecțiilor.	
35.	**Banca Națională a Moldovei**		Nu a prezentat avizul	
36.	**Agenția Națională pentru Siguranța Alimentelor** *(Nr. 15-195 din 15.01.2024)*		Lipsa de obiecții sau propuneri.	
37.	**Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei** *(Nr. 01-DRA/58 din 15.01.2024)*		Lipsa de obiecții sau propuneri.	
38.	**Agenția Națională pentru Reglementare în Energetică (ANRE)** *(Nr. 12/234 din 15.01.2024)*		Nota informativă și Analiza Impactului de Reglementare la proiectul de lege pentru modificarea unor acte normative, nu conțin informații privind impactul economico-financiar asupra autorităților de drept privat (operatorilor de servicii), în special asupra tarifelor.	**Precizare.** În analiza de impact se menționează explicit că estimarea acestui impact este destul de dificilă dată fiind lipsa datelor statistice primare în domeniul securității cibernetice, precum și lipsei unor evaluări și analize financiare bazate pe astfel de date.

				Totuși, unele estimări generale sunt furnizate de Comisia Europeană în procesul de evaluare[8] a costurilor de conformare pentru mediul privat în procesul de pregătire a propunerii de Directivă NIS1: *costul de conformare pentru fiecare întreprindere mică și mijlocie s-ar situa între 2 500 și 5 000 de euro.*
			Cu referire la art. IX din proiectul de lege pentru modificarea unor acte normative, ținem să menționăm că majoritatea operatorilor din domeniul serviciului public de alimentare cu apă și de canalizare nu dispun de personal calificat în domeniul cibernetic, or, luând în considerare că veniturile acestora sunt reglementate, ultimii nu vor putea implementa prevederile legii în cazul în care nu vor fi prevăzute expres mijloacele financiare și sursele în aceste scopuri. Astfel, urmează a fi implementate sisteme informaționale, organizate seminare de instruire a operatorilor în domeniul securității cibernetice. În acest sens, considerăm necesar și oportun de estimat cheltuielile necesare pentru îndeplinirea obligațiilor de asigurare cibernetică, de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice, de către operatorii serviciului public de alimentare cu apă și de canalizare, sursele de finanțare. Dacă se prevede finanțarea acestor activități din tarife, este	**Precizare.** În domeniu de aplicare al Legii nr. 48/2023 privind securitatea cibernetică urmează să intre persoanele juridice care prestează servicii esențiale în sectoarele și subsectoarele, lista cărora urmează, în temeiul art. 4 alin. (2) din aceeași lege, să fie aprobată de către Guvern. De asemenea, Guvernul în această listă urmează să stabilească și tipurile și categoriile de persoane juridice care vor fi identificate de către Agenția pentru securitate cibernetică ca fiind furnizori de servicii. Potrivit legii respective, furnizorii de servicii care vor intra în domeniul de aplicare al acesteia sunt obligați să implementeze măsuri de securitate pentru a preveni și a soluționa incidentele de securitate cibernetică. *Măsurile de securitate* sunt definite de lege ca operațiuni și/sau resurse organizaționale, fizice și de tehnologie a informației, ***aplicate în scopul obținerii și menținerii securității rețelelor și sistemelor informatice și a securității datelor procesate prin acestea***, iar *incidentele cibernetice* – ca evenimente care compromit

[8] https://www.consilium.europa.eu/ro/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentNumber=6342%2F13%7C6342%2F*%2F13&DocumentLanguage=FR

			iminentă determinarea impactului asupra tarifelor prin prisma riscurilor și eficienței economice.	disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate, transmise sau prelucrate ori a serviciilor ***oferite de rețelele și sistemele informatice sau accesibile prin intermediul acestora*** . Prin urmare, dependența de o rețea și/sau sistem informatic, astfel cum acestea sunt definite de Legea nr. 48/2023, este o condiție fundamentală pentru ca o persoană juridică să fie identificată ca fiind furnizor de servicii în sensul aceleiași legi. Astfel, referindu-ne nemijlocit la categoria de operatori relevată de autorul obiecției, menționăm că aceștia vor fi identificați de către autoritatea competentă ca furnizori de servicii și, implicit, vor fi responsabili de realizarea obligațiilor impuse de lege doar dacă în activitatea lor, de prestare a serviciilor esențiale/critice, utilizează rețele sau sisteme informatice. Cu alte cuvinte, nu este necesar ca operatorii să implementeze sisteme informaționale pentru a fi „eligibili” domeniului de aplicare al legii.
39.	**Cancelaria de Stat** *(Nr. 38-78-346 din 15.01.2024)*	*EXTRAS din PROCESUL-VERBAL nr. 1 al şedinţei Grupului de lucru al Comisiei de stat pentru reglementarea activităţii de întreprinzător (şedinţă prin corespondenţă) 10 ianuarie 2024*		

		15.	***La definirea problemei***, în acest compartiment, conform cerințelor Metodologiei, este necesar de identificat clar ce probleme (existente sau potențiale) sunt depistate, care probabil necesită intervenția statului. Se clarifică în detaliu situația existentă, se identifică cauzele problemelor depistate, care exact sunt părțile afectate și în ce mod. Cu toate că în definirea problemei se expune destul de multă informație despre impactul unui incident cibernetic, inclusiv sunt acordate și unele cifre potențiale care ar estima prejudiciul financiar în urma unui incident cibernetic, totuși această analiză nu este dusă până la capăt. În cazul în care se invocă riscuri de incidente și prejudicii potențiale datorate unui nivel de protecție insuficient, atunci este deosebit de important în definirea problemei ca, în baza datelor colectate, să se estimeze în mod argumentat care este nivelul de risc, care sunt prejudiciile reale și potențiale anume pentru Moldova (*în realitățile economice și tehnologice existente*) în cazul materializării riscurilor, luând în calcul tendința de creștere sau descreștere a riscurilor. Este recomandabil pentru a identifica riscul global și riscul materializat în practică la întreprinderi/instituții, să fie raportat numărul de incidente din ultimii ani la numărul de întreprinderi/instituții (*la modul ideal, luând în calcul varietatea și magnitudinea sistemelor informatice utilizate de aceste*	**<u>Nu se acceptă.</u>** Proiectul de lege însoțit de analiza de impact propune o abordare etapizată pentru determinarea subiecților obligațiilor de asigurare a securității cibernetice. O primă iterație a fost adoptarea Legii nr. 48/2023 privind securitatea cibernetică, care stabilește norme legale, care stabilesc într-un volum limitat, domeniul de aplicare/cercul de subiecți ai obligațiilor legale. Legea de asemenea deleagă Guvernului competența de adoptare a cadrului normativ subsidiar necesar pentru finalizarea constituirii domeniului de aplicare a Legii. Astfel, determinarea subiecților obligațiilor legale nu va fi și nici nu poate fi finalizată prin adoptarea prezentului proiect de lege. Ulterior, după aprobarea întregului cadru normativ, în mod special a metodologiei de identificare a furnizorilor de servicii de către autoritatea competentă, urmează fi continuat procesul de determinare a domeniului de aplicare a legii. Potrivit art. 4 alin. (2) din Legea privind securitatea cibernetică, Guvernul, în vederea implementării prevederilor legii, urmează să adopte: - lista sectoarelor și subsectoarelor critice și, corespunzător, a tipurilor și categoriilor de persoane juridice care prestează servicii în sectoarele și subsectoarele respective; - cadrul metodologic privind identificarea persoanelor juridice de drept public și a celor de drept privat ca fiind furnizori de servicii;

			întreprinderi/instituții). Sau cel puțin de clarificat câte incidente pot fi identificate în ultimii ani și care este tendința. Care este valoarea estimativă a prejudiciilor și, dacă există tempo de creștere a incidentelor, cum crește această valoarea anual. Astfel va fi posibil de identificat întreaga magnitudine a problemei și, ulterior la analiza impactului, în temeiul scăderii riscurilor și a prejudiciilor pot fi estimate beneficii potențiale în baza economiilor obținute. Corespunzător, la definirea problemei nu se descrie suficient mediul de afaceri, întreprinderile (categoriile acestora) care sunt vizate de inițiativa în cauză. Cel puțin este important de a clarifica tipologia lor, numărul lor, rolul lor și categoriile de riscuri cibernetice cele mai înalte, aferente domeniului economic de activitate. Cu toate că la analiza problemei se expune destul de multă informație cu privire la nivelul de securitatea cibernetică a Moldovei, inclusiv unele componente ale acesteia, totuși este extrem de important de a efectua analiza nivelului de securitate cibernetică a întreprinderilor (celor mai importante întreprinderi sau unele exemple relevante individuale) care vor fi vizate direct de proiectul de lege preconizat. În urma acestei analize se va identifica ce elemente și practici lipsesc sau nu sunt dezvoltate suficient, comparativ cu exigențele/standardele UE în acest sens. Corespunzător, se va putea identifica nivelul real de riscuri existent dar și,	- modul de întocmire, ținere și actualizare a listei furnizorilor de servicii. Chiar și adoptarea acestui cadru normativ specific va constitui în esență doar o continuare a constituirii domeniul de aplicare a legii, adică a subiecților obligațiilor instituite prin aceasta. Acest proces se va finaliza doar după ce Agenția pentru Securitate Cibernetică va notifica în mod oficial, prin act administrativ, fiecare persoană juridică că aceasta are calitate de furnizor de servicii cu toate consecințele legale care le implică această calitate și după ce va expira termenul legal de contestare a acestei calități (acest termen urmează a fi reglementat de acest cadru normativ subsidiar legii). Legea în sine stabilește un nivel standardizat de securitate a rețelelor și sistemelor informatice și calea cum acest nivel urmează a fi atins. Astfel, subiecții legii urmează, în contextul implementării prevederilor legii să efectueze ei înșiși o analiză a riscurilor și, aplicând principiul proporționalității, să implementeze măsuri de securitate corespunzătoare riscurilor identificate. În context, notăm că Directiva NIS2 este un act, care, în baza principiului minimei armonizări, instituie mecanisme, proceduri și cerințe care au menirea să asigure un nivel comun ridicat de securitate cibernetică la nivelul UE. Promovarea și adoptarea acestui act au fost precedate de o analiză temeinică nu doar a impactului pe care aceasta îl va produce asupra mediului de afaceri, ci și a modului de implementare de către statele membre ale UE a Directivei NIS. Urmare a

			mai jos la analiza impacturilor, se va putea estima impactul real pentru conformarea mediului de afaceri la noul proiect de lege sau cel puțin va fi posibil de identificat cele mai importante costuri de conformare care nu pot fi evitate. În lipsa unei analize de riscuri pe domenii economice de activitate, rămâne neclar din ce cauză au fost selectate anume domeniile propuse în proiect (farmaceutica, transport naval, etc.) și din ce cauză nu sunt alte domenii sau nu au fost selectate domenii mai puține, cel puțin pentru prima perioadă.	acestei analize au fost identificate sectoarele cu nivelul de criticalitate cel mai înalt pentru funcționarea în regim normal a economiei naționale, a societății și a statului. Sectoarele respective au fost stabilite ca un „standard minim" pentru toate statele membre, indiferent de dimensiunea teritorială și specificul geografic, de numărul populației sau de dezvoltarea economică. Din această perspectivă, dar și având în vedere faptul că evaluarea riscurilor la nivel național, ulterior la nivel de domeniul economic, ulterior la nivel de subdomeniu și în ultimă instanță la nivel de întreprindere este una destul de costisitoare din perspectiva resurselor de timp, financiare și umane și, pe cale de consecință, lipsită, mai ales în contextul descris, de o utilitate practică. În aceeași ordine de idei, trebuie remarcat faptul că, din perspectiva practicii de elaborare și adoptare a legislației în acest domeniu de către statele membre ale UE pentru a transpune Directiva NIS, în mod special al procesului de identificare a persoanelor juridice care intră în domeniul de aplicare al unei astfel de legislații, în raportul său de evaluare a coerenței abordărilor adoptate de statele membre pentru identificarea operatorilor de servicii esențiale, Comisia Europeană a subliniat că „Statele membre au conceput diferite metodologii de identificare a operatorilor, utilizând pe deplin flexibilitatea oferită de Directiva NIS. Unul dintre elementele care influențează metodologiile naționale a fost preexistența unui cadru, precum

				Directiva 2008/114/CE a Consiliului privind infrastructurile critice sau alte dispoziții naționale privind „operatorii vitali”. În astfel de cazuri, statele membre și-au utilizat experiența anterioară ca punct de referință și au inclus, în metodologiile existente, particularități legate de Directiva NIS.” Urmare a acestei evaluări, Comisia a tras concluzia preliminară că, deși Directiva NIS a demarat un proces esențial de sporire și de îmbunătățire a practicilor de gestionare a riscurilor în sectoare critice, în Uniune există un grad considerabil de fragmentare în ceea ce privește identificarea operatorilor de servicii esențiale. Acest lucru este determinat parțial de modul în care este concepută directiva (n.n. – Directiva NIS1) și parțial de metodologiile diferite de punere în aplicare utilizate de statele membre. Pe cale de consecință, Directiva NIS2 urmărește să elimine astfel de divergențe marcante dintre statele membre, în special prin stabilirea unor norme minime privind funcționarea unui cadru de reglementare coordonat, prin stabilirea unor mecanisme pentru cooperarea eficace între autoritățile responsabile din fiecare stat membru, prin actualizarea listei sectoarelor și a activităților care fac obiectul obligațiilor în materie de securitate cibernetică și prin instituirea unor căi de atac și măsuri de asigurare a respectării legii eficace care sunt esențiale pentru asigurarea efectivă a respectării acestor obligații .

				Această uniformizare în mod evident, dată fiind calitatea Republica Moldova de stat candidat la aderare la UE, trebuie extrapolată și la nivel național în țara noastră. Este necesar de ținut cont în acest proces că sectoarele și subsectoarele stabilite în Directiva NIS2 sunt un minim determinat ca fiind caracteristic tuturor statelor membre. Și, în acest context, chiar dacă un anumit sector nu este caracteristic pentru un anumit stat membru acesta ar putea fi critic pentru alt stat membru din perspectiva interconexiunilor dintre acestea, în mod special din punctul de vedere a securizării lanțului de aprovizionare pentru entitățile care prestează servicii esențiale determinate ca atare de norma legală. Astfel, completările propuse în proiect la legile sectoriale sunt în esență de natură mai degrabă conexă, care au menirea de a exclude la nivelul reglementărilor primare interpretările ambigue sau contradictorii. Trebuie de relevat faptul intervențiile respective vizează în mod specific doar domeniile care sunt reglementate la nivel primar, asigurând o respectare cât mai fidelă a principiului minimei intervenții și evitării suprareglementării în legile sectoriale. În același timp, aceste modificări reprezintă rezultatele analizei comparative dintre tipologia furnizorilor de servicii esențiale, oferită de anexele I și II ale Directivei NIS2, și tipologia persoanelor juridice din sectoarele sau subsectoarele respective, reglementată în legislația națională.

		16.	În mod separat, luând în calcul propuneri de completare a Legii nr.131/2012 cu un nou organ cu funcții de control, este important să fie dezvoltată o analiză distinctă pe rolul Agenției. Din ce cauză aceasta necesită funcții de control de stat, din ce cauză alte instrumente (*de schimb de informații, înregistrări oficiale, interacțiune la distanță etc.)* nu sunt suficiente. Cum se preconizează activitatea de control și care se presupune a fi impactul „benefic" al controlului de stat. Care se preconizează să fie spectrul de măsuri restrictive din atribuția Agenției și cum acestea trebuie să schimbe situația existentă în raport cu nivelul de conformare al agenților economici. Evident, toate acestea necesită să pornească de la analiza și expunerea nivelului mediu de conformare al întreprinderilor la cerințele de securitate cibernetică care se preconizează a fi preluate din standardele UE.	Unul dintre obiectivele urmărite prin adoptarea Legii privind securitatea cibernetică și, implicit a actelor normative ce urmează să o pună în aplicare (inclusiv proiectul în speță) este armonizarea cadrului normativ național la legislația Uniunii Europene. Acest obiectiv decurge din statutul de candidat la aderarea la UE a țării noastre. Obiectivul general determinant al Legii respective însă este acela de a asigura un nivel înalt de protecție a infrastructurii informaționale critice naționale, astfel încât să fie asigurată o reziliență corespunzătoare a subiecților care cad sub incidența prevederilor legii și prin urmare și a întregii țări. Deși obiectivul armonizării nu este unul determinant, acesta urmează a fi înțeles și tratat din perspectiva nivelului de maturitate și a bunelor practici deja existente în spațiul comunității europene. Alinierea legislației naționale la cadrul normativ european în domeniul securității cibernetice, ca de altfel și în alte domenii, nu poate fi realizat în volum deplin. Totuși principalele elemente comune în principiu nu doar pentru spațiul jurisdicției UE, sunt reglementate și în legea moldovenească. Unul dintre aceste elemente este supravegherea și asigurarea respectării legii. Astfel, conform art. 32 din Directiva NIS2 stabilește expres că *statele membre se asigură că autoritățile lor competente supraveghează în mod eficace și iau măsurile necesare pentru a asigura respectarea prezentei directive.* Această prevedere a Directivei este reflectată și în

				conținutul Legii nr. 48/2023 privind securitatea cibernetică. Potrivit art. 7 alin. (1) Guvernul urmează să desemneze autoritatea competentă respectivă. Pentru executarea acestor prevederi Guvernul a adoptat Hotărârea nr. 1028/2023 „Cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică". Prin prisma celor expuse, relevăm că normele legale primare referitoare la exercitarea funcției de supraveghere și control de stat de către Agenția pentru Securitate Cibernetică (ASC) este o premisă fundamentală care stă la baza prevederilor proiectului de lege prin care se propune completarea Legii 131/2012 privind controlul de stat asupra activității de întreprinzător. Cu alte cuvinte relația dintre normele Legii 48/2023 și propunerile de modificare ale Legii nr. 131/2012 poate fi caracterizată ca o relație de cauză și efect. În același context, referindu-ne în mod specific la enunțurile interogative ale autorului opiniei din ce cauză ASC necesită funcții de control de stat, din ce cauză alte instrumente nu sunt suficiente, relevăm următoarele. Pentru a-și realiza misiunea ministerele și alte autorități administrative centrale, care de altfel sunt responsabile de realizarea politicii de stat în domenii determinate, sunt învestite cu competență de exercitare a anumitor funcții, inclusiv de implementare. Una dintre acestea este funcția de supraveghere și control de stat. În acest sens controlul de stat, fiind în principiu o formă în care supravegherea este exercitată, rezidă în evaluarea conformității

				comportamentului anumitor subiecți ai legii la cerințele stabilite de această lege/legislație. Legislația în domeniul securității cibernetice stabilește, și le va dezvolta în continuare, cerințe de securitate specifice, care includ o componentă tehnică pronunțată și care implică cunoștințe, competențe și capabilități înalte și specifice obiectivelor acestui domeniu. De rând cu evaluarea conformității și în directă legătură de consecvență, controlul de stat mai oferă oportunitatea unei analize continue a modului în care legislația este implementată și, în baza acesteia, a intervenției de diferită manieră pentru restabilirea ordinii publice, inclusiv în mediul virtual. Având în vedere sensibilitatea și criticalitatea anumitor domenii pentru funcționarea în condiții de normalitate a serviciilor esențiale pentru economie, societate și stat o astfel de funcție cum este supravegherea modului de respectarea a legislației și, implicit controlul acestuia este inerentă unui model de guvernanță în domeniul securității cibernetice. Formele alternative de interacțiune relevate în opinia la Analiza de impact nu se exclud aplicarea controlului de stat, ci din contra urmează a fi utilizate în tandem cu acesta. Aplicate singular acestea nu vor oferi eficiența și eficacitatea necesare realizării scopurilor pentru care o astfel de funcție este atribuită unei autorități publice – o viziune clară, asupra modului în care În context trebuie să ținem cont de faptul că un nou organ cu funcții de control de stat nu implică

				în mod neapărat exercitarea funcției represive a statului față de mediul de afaceri. Atâta timp cât legea este respectată intervenția unui astfel de organ urmează a fi redusă bineînțeles la maxim.
		17.	La ***stabilirea obiectivelor*** este necesar ca acestea să fie racordate la cauzele problemelor, să fie măsurabile, tangibile și expuse în timp (SMART). O mare parte din „obiectivele specifice" sunt de fapt mai mult acțiuni ce urmează a fi întreprinse.	**<u>Se acceptă.</u>** Obiectivele specifice au fost reformulate. Cu toate acestea, aspectul temporal nu este reflectat în aceste obiective, deoarece termenele și condițiile temporale sunt stabilite în Legea nr. 48/2023 privind securitatea cibernetică și cadrul normativ conex.
		18.	La ***identificarea opțiunilor***, conform cerințelor Metodologiei, trebuie să se clarifice clar și în detaliu ce soluții (drepturi, obligații, mecanisme) se propun prin intervenția preconizată și cum acestea abordează situația existentă. Așa cum s-a stabilit la compartimentul definirii problemei, intervențiile în legile sectoriale sunt mai mult decât discutabile. În lipsa unei analize de riscuri la nivel național, se fac doar referințe la cadrul normativ european, dar și din acel cadru prioritățile sunt preluate selectiv. De exemplu, nu e clar din cauză autorii consideră că anume transportul naval este atât de important (*deși este evident că acesta în Moldova este mai mult decât subdezvoltat cât în privința numărului de transportatori, atât și a infrastructurii navale și portuare*), la fel nu e tocmai clară și abordarea în raport cu întreprinderile farmaceutice, în care partea de producere este infimă, prevalând partea de importuri și	**<u>Nu se acceptă.</u>** Cât privește modul de selectare a anumitor domenii în detrimentul altora și intervențiilor legislative, a se vedea argumentele prezentate mai sus la compartimentul *definirea problemei*.

			distribuție. Din perspectiva alegerii domeniilor prioritare în care să fie instituite cerințe de securitate cibernetică și, corespunzător, care să fie supravegheate de noua Agenție, sunt necesare opțiuni alternative și argumentare corespunzătoare, mult mai fundamentală, decât simpla trimitere la cadrul normativ european. În cazul în care domeniile critice evidente (*autoritățile publice, segmentul bancar și financiar, utilitățile publice etc.*) reprezintă marea majoritate a punctelor critice de risc, atunci împovărarea cu noi cerințe dar și dispersarea neeficientă a resurselor Agenției pentru domenii care nu sunt critice în realitatea MD, nu are sens, sau cel puțin nu este rațională în prima perioadă.	

		19.	***Analiza opțiunilor***, în cadrul acestui compartiment, conform cerințelor Metodologiei, este necesar să se indice impactul noilor prevederi din proiect și costurile de conformare în comparație cu beneficiile și costurile situației actuale, la fel să clarifice cum vor influența soluțiile propuse asupra cauzelor problemelor. În rezultatul expunerii costurilor și beneficiilor, acestea se contrapun și se identifică beneficiile nete. În raport cu beneficiile potențiale nu se estimează impactul noului sistem propus, adică cu cât estimativ ar putea scădea riscul de incidente cibernetice și cum se traduce în valori monetare scăderea acestui risc (*sau schimbarea tendinței de creștere*). Ori prejudiciile care au fost evitate pot fi calificate ca și potențiale beneficii, chiar și prin scăderea doar a riscului în puncte procentuale, unde fiecare punct procentual poate avea o valoarea monetară destul de tangibilă. În partea ce se referă la ***costuri*** este insuficient dezvoltat impactul asupra întreprinderilor. Sunt prezentate unele cifre cât în raport cu conformarea la noi cerințe și standarde de securitate cibernetică care vin să fie instituite prin noua lege (costuri de conformare), dar și povara administrativă pentru notificări și alte proceduri de raportare. Însă cifrele prezentate sunt estimări la nivel de UE. Este necesar ca acestea să fie extrapolate la realitățile MD și la numărul concret de întreprinderi care vor fi vizate. Nu în ultimul rând, în raport cu funcțiile	**Precizare.** Așa cum menționează analiza de impact, la nivel național nu se poate face o estimare precisă din cauza lipsei de date cu privire la numărul incidentelor semnificative, conform definiției acestora în legislația europeană. Numărul incidentelor semnificative ar putea determina frecvența raportării și efortul temporar necesar din partea furnizorilor de servicii. În cadrul analizei de impact, s-a evidențiat că costul unei notificări pentru un incident semnificativ este aproximativ 125 de euro, conform evaluărilor Comisiei Europene. Fără a avea la dispoziție date concrete la nivel național, nu poate fi realizată o analiză corespunzătoare care să ne furnizeze date veridice și verosimile, în baza cărora să se poată emite decizii corecte și să se procedeze în consecință la executarea lor. În această situație putem opera doar cu informațiile disponibile la nivel european. Astfel, după cum s-a contraargumentat și în procesul de promovare a proiectului de lege cu privire la securitatea cibernetică (având în vedere că se invocă aceleași obiecții) media anuală a incidentelor semnificative raportate la nivelul unui stat membru este estimată la 1414 incidente / 27 state membre / 4 ani = 13 incidente semnificative raportate pe an. Extrapolând această medie la contextul Republicii Moldova, costurile administrative totale pe an pentru îndeplinirea obligațiilor de notificare ar ajunge la 125 de euro * 13 incidente semnificative = 1625 de euro la

			de control și supraveghere noi ale Agenției, este important să se clarifice impactul potențial al controlului în raport cu alte soluții mai puțin invazive.	nivel național, pentru toți furnizorii de servicii identificați. Este important de subliniat că aceste estimări sunt realizate în baza datelor europene disponibile și că, pentru o imagine mai precisă, este necesară colectarea și analiza datelor specifice Republicii Moldova în ceea ce privește incidentele semnificative. Toate aceste date vor fi disponibile odată cu operaționalizarea activității Agenției pentru Securitate Cibernetică, după o perioadă anumită de timp de implementare a prevederilor legale, inclusiv în contextul exercitării de către această entitate a funcției de cercetare și dezvoltare. Cât privește precizările normative efectuate în Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător, care cuprinde lista organelor de control și domeniile aferente acestora cu o poziție nouă dedicată Agenției pentru Securitate Cibernetică, urmează de subliniat că aceasta nu poate fi interpretată ca o opțiune, ci ca o obligație. Acest aspect devine evident având în vedere prevederile art. 7 alin. (3) lit. e) din Legea nr. 48/2023 privind securitatea cibernetică, care stabilește că autoritatea competentă în domeniul securității cibernetice este însărcinată să exercite funcțiile de supraveghere și control de stat asupra modului în care furnizorii de servicii respectă obligațiile impuse de legea menționată.

		20.	Totodată să se clarifice și care va fi spectrul de măsuri restrictive și sancțiuni pe care le va putea aplica Agenția.	**Se acceptă.** În varianta inițială a proiectului de lege au fost incluse propuneri de completare a Codului contravențional cu componențele de contravenții în domeniul de aplicare a Legii securității cibernetice. Aceste propuneri însă au fost excluse din proiect urmare a obiecției Ministerului Justiției conform căreia aceste propuneri urmează a fi promovate de acest minister în mod centralizat în comun cu alte modificări la Codul contravențional. Deși în viziunea noastră aceasta este o practică vicioasă deoarece știrbește din înțelegerea în ansamblu al corpului de reglementări cuprinse în proiect în contextul obiectivului general de aducere a cadrului legal în concordanță cu prevederile Legii nr. 48/2023 și trezește îngrijorări în ce privește integritatea procesului de promovare a unui act normativ cu un obiect de reglementare determinat.
		21.	În partea ce ține de ***consultările publice*** în situația intervenției propuse, este important de a indica expres care sunt acele persoane juridice care vor fi afectate de intervenție, cel puțin în ce domenii de activitate și ce mărime, cu o listă a acestora care au fost abordate pentru consultare cu scopul de a înțelege situația existentă și validare a soluțiilor propuse. Atenționează că, contrar cerințelor Metodologiei, lipsește orice proces de consultare, ori deja în procesul de elaborare a proiectului și analizei de impact, acest proces trebuia derulat. Corespunzător este important ca deja la această etapă să fie reflectată poziția	**Se acceptă parțial.** În conformitate cu prevederile art. 9 al Legii nr. 239/2008 privind transparența în procesul decizional, anunțul privind inițierea elaborării proiectului de lege a fost plasat pe pagina web a Ministerului Economiei și platforma oficială de consultări particip.gov.md. La anunț au fost anexate și versiunile inițiale ale analizei de impact și proiectului de lege. În același timp, urmează a fi atras atenția că prevederile prezentului proiect de lege urmăresc să aducă cadrul legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică și să asigure funcționalitatea deplină a Agenției pentru

			persoanelor afectate, în special a agenților economici. ***<u>Concluzii:</u>*** *Analiza prezentată corespunde în parte cu cerințele Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, odată ce nu reflectă suficient impactul soluțiilor propuse. În special lipsește analizei situației reale din Moldova în privința mediului de afaceri vizat de intervenție, inclusiv lipsește o argumentare clară în baza analizei de riscuri din ce cauză au fost selectate ca și prioritare anume domeniile economice propuse în proiect. Analiza necesită să fie completată substanțial.*	Securitate Cibernetică. Atât prevederile Legii nr. 48/2023 privind securitatea cibernetică, cât și rolul Agenției pentru Securitate Cibernetică au fost supuse mai multe discuții și dezbateri publice pe parcursul anului 2023 cu părțile interesate, inclusiv mediul privat. În același timp, în contextul în care entitățile care vor fi direct afectate trebuie să fie identificate după aprobarea metodologiei pentru identificarea persoanelor juridice din sectorul privat, care vor deveni furnizori de servicii esențiale, și după aprobarea listei sectoarelor, subsectoarelor, tipurilor și categoriilor de furnizori de servicii esențiale, identificare care va avea loc după ce Agenția pentru Securitate Cibernetică își va începe activitatea operațională. În aceste condiții, consultarea directă a acestor entități la această etapă devine imposibilă.
40.	**Aparatul Președintelui Republicii Moldova** *(Nr. 2/2-06-37 din 15.01.2024)*		Lipsa de obiecții sau propuneri.	
41.	**Centrul Național Anticorupție** *(Nr. 06/2/625 din 16.01.2024)*	22.	**Obiecție generală** *Art. I. - [...] „(4)1 Întreprinderile şi instituţiile farmaceutice [...] sunt responsabili pentru îndeplinirea obligaţiilor de asigurare a securităţii cibernetice stabilite de această lege, [...];* *Art. III. - Codul navigaţiei maritime comerciale al Republicii Moldova, aprobat*	**Se acceptă parțial.** În tot textul legii, la articolele la care se face referință în raportul de expertiză anticorupție, pentru a exclude ambiguitatea, cuvintele „legea respectivă” au fost înlocuite cu cuvintele „această lege”. Această din urmă formulare exprimă fără echivoc, inclusiv din punct de vedere a regulilor gramaticale, trimiterea la Legea nr. 48/2023

			prin Legea nr. 599/1999 [...] stabilite de legea respectivă, [...]; *Art. VII. - Legea nr. 171/2012 privind piaţa de capital [...] 1. Articolul 41 se completează cu alineatul (8)1 cu următorul cuprins: [...] obligaţiilor care le revin conform legii respective [...];* *Art. VIII. [...] „Articolul 371 . Asigurarea securităţii cibernetice [...] stabilite de legea respectivă [...];* *Art. X. [...] stabilite de legea respectivă [...];* *Art. XI. [...] stabilite de legea respectivă [...];* *Art. XIV. [...] stabilite de legea respectivă [...];* *Art. XVII. [...] stabilite de legea respectivă [...];* *Art. XVIII. [...] stabilite de legea respectivă [...];* *Art. XIX. [...] stabilite de legea respectivă [...];* *Art. XX. [...] stabilite de legea respectivă [...].* **Obiecții:** Modul de stabilire a sarcinii prestatorilor de servicii de îndeplinire a obligațiilor de asigurare a securității cibernetice corespunzător dispozițiilor Legii nr.48/2023 privind securitatea cibernetică, se consideră a fi descris ambiguu, fiind dificilă interpretarea și identificarea actului normativ la care se referă textului proiectului prin utilizarea expresiilor „de această lege” sau „stabilite de legea respectivă”, întrucât nu este clar dacă se referă la legea supusă modificării sau actul	privind securitatea cibernetică. Totodată, atragem atenția că norma invocată de la art. 55 alin. (5) din Legea nr. 100/2017 are ca obiectiv evitarea reproducerii unor norma complementare și stabilind datele de identificare a actului la care se face referință. Normele propuse în proiectul de lege respectă această regulă. Reproducerea încă o dată a denumirii Legii nr. 48/2023 privind securitatea cibernetică ar constitui o încălcare a prevederilor art. 54 alin. (1), în particular lit. a).

			normativ care reglementează domeniul securității cibernetice. Totodată, potrivit rigorilor de elaborare a actelor normative statuate în Legea nr.100/2017, se stabilește că conţinutul proiectului trebuie să se expună într-un limbaj simplu, clar şi concis, pentru a se exclude orice echivoc. Subsidiar, la art. 55 alin.5) din Legea nr.100/2017, se stabilește că *„În cazul în care se face trimitere la o normă juridică care este stabilită în alt act normativ, pentru evitarea reproducerii normelor complementare, se face trimitere la elementul structural sau constitutiv respectiv, indicîndu-se denumirea, numărul şi anul adoptării, aprobării sau emiterii actului citat.”* Prin urmare, se relevă necesitatea revizuirii conținutului proiectului, în vederea respectării reglementărilor Legii nr.100/2017 și evitarea interpretărilor eronate a normelor proiectului, în special în contextul stabilirii obligațiilor care necesită a fi îndeplinite de către furnizorii de servicii, or ambiguitatea creată în urma trimiterilor defectuoase, ar servi drept motiv pentru omisiunea realizării sarcinilor descrise în actul normativ privind securitatea cibernetică. **Recomandări:** Se recomandă modificarea textului proiectului prin excluderea expresiilor „de această lege”, „legea respectivă” și precizarea exactă a	

			actului normativ la care se face trimitere în contextul stabilirii necesității de îndeplinire a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii din sectoarele menționate în proiect.	
		23.	*Art. XVI. pct.1.* *XVI. - Legea nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar [...] se modifică după cum urmează:* *1. Articolul 17 alineatul (2) se completează cu litera b^2), cu următorul cuprins: „b2) pentru personalul Agenţiei pentru Securitate Cibernetică - 120% din suma anuală a salariilor de bază;”.* **Obiecții:** Norma prezentată supra stabilește suma anuală a sporului cu caracter specific inclusă în partea variabilă a salariului lunar, care pentru personalul Agenției pentru Securitate Cibernetică va constitui 120% din suma anuală a salariilor de bază. Reieșind din modul de formulare a normei nu este clar cum este stabilită această sumă anuală a salariilor de bază, care salarii de bază vor fi luate în calcul pentru determinarea sporului, or potrivit prevederilor art.17 din Legea nr.270/2018, pentru precizarea modului de calcul al sporului cu caracter specific se precizează salariile de bază din contul cărora se calculează sporul. În acest sens se subliniază necesitatea de respectare a regulilor de elaborare a actelor	**Se acceptă**.

			normative statuate în Legea nr.100/2017, unde se stabilește că conţinutul proiectului se expune într-un limbaj simplu, clar şi concis, pentru a se exclude orice echivoc. **Recomandări:** Se recomandă completarea art. XVI. pct.1 din proiect cu precizarea din contul căror salarii de bază se va realiza determinarea sporului de 120%	
		24.	**Concluzia expertizei** Cu referire la stabilirea sporului cu caracter specific de 120% din salariul de bază pentru tot personalul Agenției pentru Securitate Cibernetică, subliniem că nota informativă nu reflectă necesitatea stabilirii acestui spor pentru funcțiile de suport al instituției (secretariat/contabilitate. resurse umane etc.), fiind considerate a fi excesive și nejustificate în raport cu personalul din sectorul bugetar care realizează sarcini similare, dar și în raport cu personalul Agenției care realizează sarcini complexe orientate efectiv pentru îndeplinirea obiectivelor de asigurare a securității cibernetice naționale. În acest sens, se recomandă revizuirea normei de la art. XVI. pct.1 din proiect prin prisma celor expuse la compartimentul I.5.1. din raport, astfel încât de sporul cu carcater specific să poată beneficia decât personalul Agenției antrenat în asigurarea securității cibernetice.	**Nu se acceptă.** Deși sunt funcții de suport acestea direct vizează modul de îndeplinire a funcțiilor de bază ale acestei autorități. Admiterea unei discrepanțe mari între angajații Agenției ar putea periclita atingerea obiectivelor pentru care aceasta a fost instituită. Totodată, este necesar de relevat că problematica salarizării „excepționale” a întregului personal al Agenției pentru Securitate Cibernetică nu este o chestiune de legalitate, ci una mai degrabă de oportunitate și urmează a fi tratată ca atare.

		25.	Suplimentar, în textul proiectului au fost identificate formulări echivoce și trimiteri defectuoase susceptibile să afecteze modul de implementare a prevederilor proiectului. Prin urmare, în scopul evitării apariției incidentelor de integritate, se recomandă revizuirea conținutului proiectului, reieșind din obiecțiile și propunerile de modificare enunțate în prezentul raport de expertiză.	**Se acceptă.** Formulările echivoce și trimiterile defectuoase au fost excluse din proiect în corespundere cu recomandările raportului de expertiză.
	Instituția Publică „Agenția de Guvernare Electronică” *(Nr. 3007 – 3 din 09.01.2024)*	26.	În versiunea definitivată a proiectului sunt incluse prevederi pentru completarea cu articolul 7^7 a Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, care în accepțiunea AGE au un caracter ambiguu și impredictibil, generând riscuri de interpretare și aplicare arbitrară, implicit și dificultăți majore în procesul de aplicare a acestora. Reieșind din modul laconic de expunere a argumentelor în favoarea includerii normelor respective nu este clară rațiunea reglementării necesității semnării unui acord interguvernamental cu statul membru al Uniunii Europene (UE) pe teritoriul căruia urmează a fi păstrate informațiile, în condițiile în care cel mai probabil serviciile respective urmează a fi procurate urmare a unor concursuri competitive de la prestatori de servicii privați. În condițiile în care principalele prevederi contractuale ce vor include nivelul agreat al serviciilor (SLA), volumul și parametrii acestora, prețul, aspectele privind confidențialitatea și	**Se acceptă** Prevederile pentru completarea cu articolul 7^7 a Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat au fost excluse din proiect. Totodată, în rezultatul ședinței comune din data de 23.01.2024 cu participarea SIS, AGE, STISC MDED și Consilierul Președintelui Republicii Moldova în domeniul apărării și securității naționale Stanislav Secrieru, s-a coordonat următoarea redacție a articolului 22, litera e) a Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat: „e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene;”.

			securitatea datelor, legislația aplicabilă, soluționarea litigiilor și altele, vor fi stabilite prin contractele încheiate cu prestatorii de servicii, nu este clar ce ar trebui să conțină acordurile interguvernamentale. În acest context, este de menționat că reglementarea activității și modului de interacțiune cu marii prestatori de servicii de cloud (ex. Amazon, Microsoft, Google, Oracle, Alibaba, etc.) care provin preponderent din Statele Unite ale Americii și China, reprezintă o mare provocare pentru statele membre UE[9][10] și în aceste condiții este greu de anticipat și de estimat disponibilitatea acestora de a semna asemenea tratate internaționale. De asemenea, prevederile respective nu stabilesc niște linii directoare clare în privința faptului cum urmează a fi păstrate în afară țării informațiile din cadrul sistemelor și resurselor informaționale de stat, ex. izolate de sistemele informaționale în care sunt stocate asigurându-se doar copii de rezervă sau unele sisteme informaționale de stat în anumite condiții ar putea fi găzduite în centre de date amplasate pe teritoriul unor state membre UE ori vor fi păstrate doar date arhivate care sunt utilizate în activitățile curente etc. Avînd în vedere că multe servicii inovatoare, precum majoritatea soluțiilor prestate ca servicii (SaaS) și platforme (PaaS), AI, platforme de dezvoltare, magazine de aplicații	

[9] https://www.cer.eu/insights/can-eu-afford-drive-out-american-cloud-services
[10] https://www2.deloitte.com/uk/en/insights/technology-management/cloud-sovereignty-three-imperatives-for-the-european-public-sector.html

			și alte servicii asociate platformelor mobile, mesagerie scurtă sau instant, etc. nu sunt disponibile pe teritoriul Republicii Moldova și nici din centrele de date administrate de alte guverne, aplicarea arbitrară a prevederii poate rezulta în faptul că aceste servicii nu vor mai putea fi folosite de către autoritățile publice, fapt ce va duce la ineficiențe și stagnare în dezvoltările tehnice, chiar și la nivel de studii comparative sau analize cost-beneficiu. Totodată, în condițiile în care legiutorul, anterior a adoptat reglementări referitoare la transmiterea transfrontalieră și libera circulație a datelor cu caracter personal, din care rezultă că datele respective pot fi transmise către statele membre ale Spațiului Economic European și alte state care asigură un nivel adecvat de protecție a datelor cu caracter personal, nu este clară logica includerii la moment a unor norme mai restrictive pentru informațiile din sectorul public. La etapa incipientă de implementare a prevederilor respective în lipsa unor acorduri interguvernamentale cu marea majoritate a statelor membre UE, restricția respectivă va reprezenta impediment major atât pentru prestatorii de servicii a căror infrastructură este amplasată în state respective, cât și pentru autoritățile publice din Republica Moldova de a contracta servicii în mod eficient și competitiv. În altă ordine de idei, la definitivarea proiectului urmează să se țină cont de faptul că	

			modificările propuse sunt și în disonanță cu strategia Guvernului de extindere a capacității platformei tehnologice guvernamentale comune (MCloud) prin reutilizarea serviciilor de Cloud Public furnizate prestatori de servicii din cadrul centrelor de date amplasate pe teritoriul statelor membre ale Uniunii Europene sau altor state, care, conform prevederilor art. 32 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, asigură un nivel adecvat de protecție a datelor cu caracter personal. În acest context este de menționat că anul precedent Guvernul a aprobat Hotărârea Guvernului nr. 208/2023 pentru modificarea Hotărârii Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud) , scopul căreia este de crea condițiile de ordin normativ pentru implementarea opțiuni viabile de extindere a capacităților și resurselor guvernamentale utilizând servicii de cloud transfrontaliere furnizate de prestatori de servicii de cloud public ce dispun de centre de date amplasate în state care asigură un nivel adecvat de protecție a datelor cu caracter personal, inclusiv statele membre ale UE. Prevederile respective au fost elaborate în scopul executării acțiunii 2.1.13 din Planul de acțiuni al Guvernului pentru anii 2021-2022, aprobat prin Hotărârea Guvernului nr. 235/2021 , din care rezulta necesitatea reglementării modului de extindere a	

			capacităţii platformei tehnologice guvernamentale comune (MCloud) utilizând resurse informaţionale ale prestatorilor de servicii de cloud din domeniul public (cloud hibrid). Astfel, în deplină aliniere cu prevederile Legii nr. 131/2011 a fost reglementată posibilitatea de contractare de către posesorul platformei MCloud a serviciilor de Cloud Public furnizate de către prestatori de servicii ce dispun de centre de date amplasate pe teritoriul statelor membre ale UE sau altor state care oferă un nivel adecvat de protecție a datelor conform prevederilor articolului 32 din Legea menționată. Reutilizarea serviciilor de Cloud public pentru găzduirea sistemelor și resurselor informaționale de stat a fost reglementată ca fiind una opțională, la care se poate recurge prin decizia comună a posesorului MCloud și posesorului sistemului/resursei informaționale. Prin crearea condițiilor tehnice, financiare și juridice pentru reutilizarea serviciilor de Cloud public, Guvernul a identificat o opțiune viabilă pentru păstrarea securizată a datelor și după caz asigurarea funcționării continue a sistemelor informaționale de stat în caz de indisponibilitate a centrelor de date guvernamentale sau identificării unor riscuri de securitate în privința acestora. În contextul riscurilor de securitate regionale diversificarea posibilităților de găzduire a sistemelor informaționale de stat, inclusiv cu utilizarea	

			serviciilor de Cloud public furnizate din centre de date amplasate pe teritoriul statelor membre UE reprezintă o oportunitate și un element important pentru asigurarea securității și integrității sistemelor informaționale de stat. Reieșind din cele menționate și ținând cont de faptul că există reglementări în materie de transmitere/păstrare/găzduire a datelor din sectorul public transfrontalier considerăm oportună excluderea prevederilor din proiectul supus avizării. În situația în care se optează totuși pentru completarea Legii nr. 467/2003, propunem expunerea articolul 77 în următoarea redacție: „Articolul 77. Găzduirea sistemelor și resurselor informaționale de stat (1) Sistemele și resursele informaționale de stat sunt găzduite pe platforma tehnologică guvernamentală comună (MCloud) (în continuare – platforma MCloud), cu excepția cazurilor expres prevăzute de lege. (2) Platforma MCloud reprezintă o infrastructură informatică de tip cloud hibrid, constituită dintr-o componentă de cloud privat și din resurse și servicii furnizate de prestatori de servicii care oferă serviciile din cadrul centrelor de date amplasate pe teritoriile statelor membre ale Uniunii Europene sau altor state, care, conform prevederilor art. 32 din Legea nr. 133/2011 privind protecția datelor cu caracter personal, asigură un nivel adecvat de protecție a datelor cu caracter personal, cu	

			condiția că aceste date să fie localizate doar în țările strict menționate. (3) Prelucrarea datelor cu caracter personal prin intermediul sistemelor și resurselor informaționale de stat se realizează de către reprezentanţii autorităţilor şi instituţiilor publice, cu respectarea reglementărilor legale aplicabile în domeniul protecţiei datelor cu caracter personal. (4) Informaţiile atribuite la secret de stat pot fi prelucrate în cadrul platformei MCloud cu asigurarea respectării prevederilor Legii nr. 245/2008 cu privire la secretul de stat. (5) Informațiile atribuite la secret de stat și informațiile din domeniile apărării, situațiilor de urgență, ordinii publice și securității naționale nu pot fi prelucrate reutilizând serviciile din Cloud Public. (6) Modul de utilizare, administrare și dezvoltare a platformei MCloud și a serviciilor aferente acesteia sunt stabilite de Guvern.”.	

Ședința interinstituțională

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1	**Ministerul Justiției**	1	Cu referire la proiectul de lege pentru modificarea unor acte normative (aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică) (număr unic 957/MDED/2023), definitivat de către autor în urma avizării repetate, relevăm	**Se acceptă**

			că, obiecții de ordin conceptual nu avem de formulat. Totodată, aferent rigorilor de tehnică legislativă, este recomandabil, ca în cazul completării articolelor cu noi elemente structurale (în cazul dat, alineate), acestora să li se atribuie numere în ordine consecutivă, dar nu numere cu indice, or, numerotarea elementelor structurale cu indicii respectivi se efectuează doar în cazul completării în interior a unui șir numeric (pct. 1-3 din Art. I; Art. II; pct. 1 și 2 din Art. VII; pct. 1 și 2 din Art. IX; pct. 1 și 2 din Art. XI; Art. XII; Art. XV; Art. XVII; pct. 2 din Art. XIX).	
2	**Banca Națională a Moldovei**		Cu referire la proiectul de lege pentru modificarea unor acte normative (aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică), număr unic 957/MDED/2023, remis spre reexaminare prin scrisoarea Ministerului Dezvoltării Economice și Digitalizării al Republicii Moldova nr. 11/2-48 din 03.01.2024, Banca Națională a Moldovei (BNM), în limitele competenței sale, reiterează propunerea expusă în scrisoarea nr. 31-002/166/6716 din 21.12.2023 privind exceptarea BNM de la aplicarea prevederilor Legii nr. 48/2023 privind securitatea cibernetică (Legea nr. 48/2023). Potrivit argumentelor autorilor proiectului, enunțate în sinteza propunerilor, recomandărilor și obiecțiilor, prevederile art. 6 pct. 35 din Directiva (UE) 2022/25551, care	**Precizare.** Din start trebuie să precizăm că băncile centrale nu sunt excluse „expres” din domeniul de aplicare al Directivei NIS2. Punctul 35 al art. 6 din directiva respectivă exclude aceste entități, de rând cu parlamentele și autoritățile din sistemul judiciar din noțiunea de „entitate a administrației publice”. În ce privește argumentarea anterioară la opinia BNM de excludere a acesteia din domeniul de aplicare al Legii nr. 48/2023, relevăm că argumentarea precum că armonizarea parțială a legislației naționale a stat la baza netranspunerii prevederilor pct. 35 din art. 6 al Directivei NIS2 este una eronată. Este probabil ca această interpretare inexactă să fie datorată mai degrabă tendinței autorului proiectului de a argumenta de o manieră mai generală neacceptarea unei astfel de excepții. Caracterul parțial de armonizarea a

			exclud expres băncile centrale de la domeniul de aplicare al acestei Directive, nu au fost transpuse în Legea 48/2023 din motiv că prin această lege s-a urmărit obiectivul de transpunere parțială (și nu deplină) a prevederilor Directivei (UE) 2022/2555. Având în vedere impactul anticipat al Legii 48/2023, în redacția curentă, asupra autonomiei BNM (cel puțin în virtutea competențelor extensive de solicitare informații, supraveghere și control deținute de autoritatea competentă la nivel național în domeniul securității cibernetice), pe de o parte, precum și necesitatea de armonizare deplină a sistemului juridic național cu legislația Uniunii Europene, în lumina deciziei Consiliului European din 14 decembrie 2023, pe de altă parte, opinăm că este importantă, la această etapă, transpunerea prevederilor Directivei (UE) 2022/2555 care au fost omise la etapa de elaborare a proiectului de lege privind securitatea cibernetică (cel puțin a prevederilor care vizează exceptarea băncii centrale din obiectul de reglementare a acestei Directive).	legislației țării noastre la prevederile Directivei NIS2 este o premisă necesară emiterii raționamentului conform căruia excepția băncilor centrale de la prevederile Directivei NIS2 nu poate fi extrapolată la nivel național, deoarece Republica Moldova nu este un stat membru al UE și, prin urmare BNM nu este parte a sistemului european de supraveghere a băncilor centrale oferit de cadrul normativ existent la nivel supranațional al UE. În concluzie, această excepție va putea fi operată doar atunci când, dat fiind statul de stat membru al UE, R. Moldova va transpune integral nu doar Directiva NIS2, dar și Regulamentul DORA și, mai ales, alte acte legislative europene relevante atât domeniului financiar bancar, cât și celui de securitate cibernetică cu incidență în acest sector.
			Cu referire la conținutul proiectului de lege, având în vedere finalitatea urmărită de acest proiect și anume asigurarea interconexiunii dintre normele Legii nr.48/2023 și cele cuprinse în legile care reglementează activitatea viitorilor furnizori de servicii și eliminarea/revizuirea unor prevederi care ar putea suscita interpretări echivoce sau	**Precizare.** În conformitate cu prevederile art. 23 alin. (2) din Legea nr. 48/2023 privind securitatea cibernetică, Guvernul urmează să aprobe în anumite termene limită cadrul normativ de punere în aplicare a acestei legi. Printre actele ce urmează a fi aprobate de Guvern se numără și

			contradictorii în procesul aplicării legii, observăm că rămâne incert, în procesul de supraveghere a asigurării securității cibernetice, modul în care vor fi delimitate competențele de supraveghere și control ale autorității competente la nivel național în domeniul securității cibernetice, de cele ale autorităților care reglementează și supraveghează propriu-zis un anumit sector/subsector critic. Observăm că riscul potențialelor conflicte negative sau pozitive de competențe dintre BNM și autoritatea competentă la nivel național în domeniul securității cibernetice au fost semnalate și de autorii proiectului, care la pct. 16 subpct. 23) din sinteza propunerilor/recomandărilor și obiecțiilor au remarcat că: „[...] din perspectiva exercițiului de către Agenția de Securitate Cibernetică a funcției de supraveghere și control, pentru punerea în aplicare a prevederilor Legii nr. 48/2023 prin reglementarea modului de supraveghere și control al respectării acestei legi, urmează, în comun cu Banca Națională a Moldovei să fie identificate mecanisme fiabile de coordonare a eforturilor în procesul de asigurare a respectării prevederilor acestei legi. Mecanismele respective bineînțeles urmează să asigure evitarea suprapunerii de competențe dintre BNM și ASC și, cu atât mai mult intrusiunile reciproce nejustificate”. Înțelegem că un astfel de mecanism urmează a fi identificat nu doar pentru	cele două acte normative prevăzute la art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023. Aceste acte urmează să reglementeze procedurile privind modul de exercitare de către ASC a funcției de supraveghere și control al modului în care furnizorii de servii își realizează obligațiile impuse de această lege. Având în vedere că în opinia BNM la proiectul de lege în speță au fost invocate îngrijorări vizavi de problematică conflictului de competențe pe dimensiunea supravegherii, în sinteză s-a opinat că în procesul de constituire a cadrului normativ subsidiar legii, date fiind îngrijorările respective, urmează a fi găsite, dacă îngrijorările sunt întemeiate, mecanisme de cooperare dintre aceste autorități competente. În ce privește celelalte sectoare, astfel de îngrijorări nu au fost exprimate, prevederile legale urmând a fi interpretată aplicând principiile generale stabilite de legislația relevantă și principiile dreptului.

			sectorul bancar, dar și pentru toate sectoarele supravegheate de către autoritatea competentă la nivel național în domeniul securității cibernetice în vederea asigurării respectării prevederilor Legii nr. 48/2023. Propunem în acest sens, identificarea unui mecanism unic reglementat prin lege și manifestăm disponibilitate pentru conlucrare în vederea atingerii acestui obiectiv.	
			Suplimentar, cu privire la excluderea din proiectul de lege a modificărilor propuse la Legea nr. 202/2017 privind activitatea băncilor (Legea nr. 202/2017), observăm că autorul în sinteza propunerilor/recomandărilor și obiecțiilor la proiectul de lege, menționează că: „în consecință prevederile Legii 48/2023 vor trebui aplicate în măsura în care anumite situații juridice nu sunt reglementate, inclusiv prin prisma principiilor enunțate la art. 3 alin. (5) din Legea nr. 48/2023, de legislația sectorială cu caracter special". Menționăm în acest context că, actualmente Legea nr. 202/2017 conține unele prevederi generale cu privire la asigurarea securității cibernetice de către bănci (a se vedea, spre exemplu, art. 38, care stabilește cerințele față de cadrul de administrare al unei bănci din perspectiva desfășurării activității acesteia în condiții de asigurare a unei gestiuni efective și prudente a tuturor riscurilor inclusiv, dar fără a se limita la riscul tehnologiilor informaționale și de comunicare). Menționăm că, prevederi	**Se acceptă.** În principiu propunerea BNM a fost reflectată în proiect cu unele ajustări. Sub aspect de concept principalele ajustări rezidă în completarea propunerii BNM cu alineatele (7) și (8). Astfel, proiectul de lege a fost completat cu Art. propuneri de modificare a Legii nr. 202/2017 privind activitatea băncilor, în următoarea redacție: „Articolul 38^2. Gestionarea riscurilor de tehnologie a informației și a comunicațiilor (TIC), de securitate a informației și de continuitate a activității (1) Fiecare bancă trebuie să dispună de personal, sisteme și servicii eficiente aferente tehnologiei informației și a comunicațiilor (TIC) ce asigură, de o manieră proporțională cu natura, amploarea și complexitatea riscurilor inerente activităților și modelului de afaceri, desfășurarea activităților băncii. În acest scop, banca stabilește roluri și responsabilități, aprobă și pune în aplicare o strategie TIC și de securitate a informației și planuri de acțiuni în vederea atingerii obiectivelor acesteia.

			detaliate privind gestionarea riscului tehnologiilor informaționale și de comunicare se regăsesc în reglementările secundare ale BNM, spre exemplu, Regulamentul nr. 47/2018 privind cerințele minime pentru sistemele informaționale și de comunicare ale băncilor. Totodată, având în vedere că art. 3 alin. (5) din Legea nr.48/2023 condiționează aplicarea directă a prevederilor derogatorii ce țin de asigurarea securității cibernetice - de reglementarea acestora prin lege (și nu prin act subordonat legii), înțelegem că modul și măsura în care acest regulament va fi aplicabil băncilor, odată cu intrarea în vigoare a Legii nr. 48/2023, rămân a fi interpretabile. În această ordine de idei, supunem atenției Dvs. faptul, că BNM este în proces de promovare a proiectului de lege pentru modificarea unor acte normative (consolidarea cadrului de activitate al Băncii Naționale a Moldovei), numărul unic de înregistrare 988/MF/BNM/2023, prin care se completează Legea nr. 202/2017 cu un articol care instituie reglementări detaliate privind administrarea riscurilor aferente tehnologiilor informaționale și de comunicare, de securitate a informației și continuitatea activității (art. 38 cu indice 2), cu următorul cuprins: ”Articolul 382. Administrarea riscurilor aferente tehnologiilor informaționale și de comunicare, de securitate a informației și continuitatea activității	(2) Banca trebuie să stabilească un cadru de administrare a continuității activității capabil să asigure capacitatea de a funcționa în mod continuu cu asigurarea protejării tuturor informațiilor critice, inclusiv, în vederea limitării pierderilor în cazul unei întreruperi severe a activității. În acest scop, banca va identifica riscurile de continuitate la care este expusă și va aproba și pune în aplicare planuri de asigurare a continuității activității. (3) Banca trebuie să dispună de un cadru de administrare a riscurilor aferente TIC și de securitate a informației care să conțină procese și proceduri pentru a asigura identificarea, analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al băncii. (4) Banca trebuie să dispună de un cadru de administrare a securității informației care trebuie să definească principiile, normele și modalitățile de protejare a confidențialității, integrității și disponibilității datelor și informației băncii și ale clienților acesteia, instituind în baza acestuia măsuri pentru diminuarea nivelurilor riscurilor TIC și de securitate a informației la care este expusă. (5) Banca trebuie să stabilească procese de revizuire a riscurilor, de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității.

			(1) Fiecare bancă trebuie să dispună de personal, sisteme și servicii eficiente aferente tehnologiilor informaționale și de comunicare (TIC) ce asigură, de o manieră proporțională cu natura, amploarea și complexitatea riscurilor inerente activităților și modelului de afaceri, desfășurarea activităților băncii. În acest scop, banca va stabili roluri și responsabilități, va aproba și pune în aplicare o strategie TIC și de securitate a informației și planuri de acțiuni în vederea atingerii obiectivelor acesteia. (2) Banca trebuie să stabilească un cadru de administrare a continuității activității capabil să asigure capacitatea de a funcționa în mod continuu cu asigurarea protejării tuturor informațiilor critice, inclusiv, în vederea limitării pierderilor în cazul unei întreruperi severe a activității. În acest scop, banca va identifica riscurile de continuitate la care este expusă și va aproba și pune în aplicare planuri de asigurare a continuității activității. (3) Banca trebuie să dispună de un cadru de administrare a riscurilor aferente TIC și de securitate a informației care să conțină procese și proceduri pentru a asigura identificarea, analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al băncii. (4) Banca trebuie să dispună de un cadru de administrare a securității informației care trebuie să definească principiile, normele și modalitățile de protejare a confidențialității,	(6) Cerințe specifice privind punerea în aplicare a alin.(1)-(5) se stabilesc în actele normative ale Băncii Naționale. (7) În măsura în care gestionarea riscurilor TIC, de securitate a informației și de continuitate a activității nu este reglementată de dispozițiile prezentei legi și a actului normativ menționat la alineatul (6), acestea se completează cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și de actele normative de punere a acesteia în aplicare. (8) Supravegherea și controlul modului în care băncile realizează obligațiile stabilite de prezentul articol se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Banca Națională a Moldovei, în conformitate cu actul normativ prevăzut la alineatul (6) și actele normative de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică.”.

			integrității și disponibilității datelor și informației băncii și ale clienților acesteia, instituind în baza acestuia măsuri pentru diminuarea nivelurilor riscurilor TIC și de securitate a informației la care este expusă. (5) Banca trebuie să stabilească procese de revizuire a riscurilor, de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității. (6) Cerințe specifice privind punerea în aplicare a alin.(1)-(5) sunt stabilite în actele normative ale Băncii Naționale.”. Propunem includerea acestor prevederi în proiect, pentru a soluționa, parțial, problematica aplicabilității reglementărilor speciale în materie de securitate cibernetică în domeniul bancar și a competențelor corelative ale BNM de a urmări respectarea acestora.	
			Suplimentar, cu referire la completarea Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat cu art. 77 (păstrarea informațiilor din cadrul sistemelor și resurselor informaționale de stat în afara teritoriului Republicii Moldova), propunem a se preciza aplicabilitatea acestui articol în raport cu autoritățile publice autonome care gestionează în mod independent sistemele și resursele informaționale deținute. În acest sens, menționăm că BNM, în procesul de gestionare independentă a sistemelor sale informaționale, utilizează serviciile Cloud	**Se acceptă.** Articolul respectiv a fost exclus din proiectul de lege. În proiect au fost înserate propuneri de modificare a art. 22 lit. e) din Legea nr. 467/2003 potrivit cărora Guvernul va avea competența de reglementare a modului de găzduire a sistemelor informaționale de stat, inclusiv aspectele ce vizează găzduirea acestora pe teritoriul statelor membre ale UE.

			pentru realizarea copiilor de rezervă criptate ale sistemelor informaționale și pentru stocarea acestora în Cloud, asigurând astfel capacitatea de restabilire rapidă în caz de incident major. De asemenea, BNM utilizează aplicații bazate pe Cloud, precum M365, ZOOM Meetings, Microsoft Teams (ș.a.), precum și tehnologii emergente cloud-enabled, inclusiv soluții pilot AI/ML/LLM, care sunt esențiale pentru progresul și inovația în activitatea BNM. Ținem să evidențiem că utilizarea serviciilor Cloud de către BNM se bazează pe o înțelegere profundă și o evaluare riguroasă a tuturor riscurilor implicate (riscurile operaționale, riscurile legate de continuitatea afacerii, riscurile de securitate a informației, riscurile aferente protecției datelor cu caracter personal) și se desfășoară conform celor mai bune practici și standarde internaționale, pentru a asigura ca orice utilizare a tehnologiei Cloud să fie securizată și aliniată obiectivelor strategice de securitate cibernetică și de continuitate operațională. Adițional, observăm că potrivit art. 77 din Legea nr. 467/2003, păstrarea informațiilor din cadrul sistemelor și resurselor informaționale de stat în afara teritoriului Republicii Moldova se realizează în baza unui acord interguvernamental. În acest context, având în vedere, pe de o parte, durata procedurilor de încheiere a acordurilor interguvernamentale, dar și necesitatea asigurării disponibilității serviciilor Cloud în termeni proximi, solicităm	

			respectuos informații privind acordurile în vigoare, care corespund prevederilor art. 77 din Legea nr. 467/2003, precum și informații privind termenele estimative propuse pentru încheierea acestor categorii de acorduri. În concluzie, reiterăm susținerea pentru eforturile consolidate ale autorităților publice în fortificarea cadrului legal privind securitatea cibernetică și solicităm respectuos reevaluarea proiectului din perspectiva propunerilor enunțate în prezentul aviz. Suntem disponibili pentru a discuta în comun potențialele soluții de ordin legislativ și practic.	

Secretar de stat **Mihai LUPAȘCU**