Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr._____
din _____2023
mun. Chișinău

Pentru aprobarea proiectului de lege pentru modificarea unor acte normative (aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică)

Guvernul HOTĂRĂȘTE:

Se aprobă și se prezintă Parlamentului spre examinare proiectul de lege cu privire la modificarea unor acte normative (aducerea cadrului legal în concordanță 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

LEGE
pentru modificarea unor acte normative
(aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică)

Parlamentul adoptă prezenta lege organică.

Art. I. – Legea nr. 1456/1993 cu privire la activitatea farmaceutică (Republicat: 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 $(4)^1$, cu următorul cuprins:

„$(4)^1$ 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 $(2)^1$ cu următorul cuprins:

„$(2)^1$ Persoanele juridice 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 $(4)^1$ cu următorul cuprins:

„$(4)^1$ Supravegherea și controlul de stat al respectării de către întreprinderile și instituțiile farmaceutice a obligațiilor stabilite la art. 3 alin. $(4)^1$, precum și de către persoanele juridice care efectuează investigații în vederea creării medicamentelor noi a obligațiilor stabilite la art. 9 alin. $(2)^1$, 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 $(7)^1$ și $(7)^2$, cu următorul cuprins:

„(7)[1] 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.

(7)[2] Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor prevăzute la alin. (7)[1] 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 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 legea respectivă, 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 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. 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, definiția noțiunii „securitate cibernetică” va avea următorul cuprins „ – astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică”;

2. Articolul 7^6 alineatul (3) se completează în final cu textul: „la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul informatizării și a resurselor informaționale de stat”.

3. 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.”

4. La articolul 21:

titlul articolului va avea următorul cuprins: „Articolul 21. Politica statului în domeniul informatizării și resurselor informaționale de stat”;

la alineatul (1) cuvintele „Politica informațională de stat” se substituie cu cuvintele „Politica statului în domeniul informatizării și resurselor informaționale de stat”;

alineatul (1) devine alineat unic;

alineatul (2) se abrogă.

5. La articolul 22:

literele a) și b) vor avea următorul cuprins:

„a) asigură realizarea politicii statului în domeniul informatizării și resurselor informaționale de stat prin intermediul ministerelor și altor autorități administrative centrale;

b) determină competența ministerelor, a altor autorități administrative centrale, a structurilor organizaționale din sfera de competență ale acestora și a altor autorități și instituții publice;”;

6. Articolul 23 se abrogă.

Art. V. – Legea comunicațiilor electronice nr. 241/2007 (Republicat: 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:

„Articolul 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 alineatul (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 alineatul $(8)^1$ cu următorul cuprins:

„$(8)^1$ 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 legii respective

conform actelor normative de punere a acesteia în aplicare și conform altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. Supravegherea și controlul de stat al modului în care societățile de investiții îndeplinesc obligațiile respective se realizează de către autoritatea competentă conform Legii nr. 48/2023 privind securitatea cibernetică.”.

2. Articolul 62 se completează cu alineatul $(3)^1$ cu următorul cuprins:

„$(3)^1$ 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. Supravegherea și controlul de stat al modului în care operatorii de piață îndeplinesc obligațiile respective se realizează de către autoritatea competentă conform Legii nr. 48/2023 privind securitatea cibernetică.”

Art. VIII. – Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova (Monitorul Oficial, 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 legea respectivă, 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 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. 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 d)[1], cu următorul cuprins:

„d)[1] 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 (3)[1], cu următorul cuprins:

„(3)[1] 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 legea respectivă, 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 (5)[1] cu următorul cuprins:

„(5)[1] 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 legea respectivă, 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 (4)[1], cu următorul cuprins:

„(4)[1] 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. (5)[1] 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 (3)[1] și (3)[2], cu următorul cuprins:

„(3)[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.

(3)[2] Supravegherea și controlul de stat al respectării de către producătorii de dispozitive medicale a obligațiilor stabilite la alin. (3)[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, 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** (Monitorul Oficial al Republicii Moldova, 2017, nr. 364 – 370, art. 620), 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 responsabili pentru

îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de legea respectivă, 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 modifică după cum urmează:

1. Articolul 38 se completează cu alineatul (4)[1], cu următorul cuprins:

„(4)[1] În vederea protecției rețelelor și sistemelor informatice pe care le deține, banca, identificată ca furnizor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, este responsabilă pentru realizarea obligațiilor de asigurare a securității cibernetice stabilite de articolele 11 și 12 din legea respectivă, de actele normative de punere în aplicare a acestora și de actele normative care stabilesc cerințe specifice de asigurare a securității cibernetice în domeniul bancar.”.

2. Articolul 138 se completează cu alineatul (6)[1], cu următorul cuprins:

„(6)[1] Supravegherea și controlul de stat al respectării de către bancă a obligațiilor stabilite la art. 38 alin. (4)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și actele normative de punere a acesteia în aplicare. În exercitarea funcției de supraveghere și control de stat, autoritatea competentă la nivel național în domeniul securității cibernetice informează în termen de 5 zile Banca Națională a Moldovei despre orice încălcare depistată și sancțiune aplicată”.

Art. XVI. – Articolul 8 din **Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate** (Monitorul Oficial al Republicii Moldova nr. 34-38 art. 34 din 04.02.2022), cu modificările ulterioare, se completează cu alineatul (3)[1] cu următorul cuprins:

„(3)[1] 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 legea respectivă.”

Art. XVII. – Articolul 17 din **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 completează cu alineatul 2^1, cu următorul cuprins:

„$(2)^1$ Personalul autorității competente în domeniul securității cibernetice conform Legii nr. 48/2023 privind securitatea cibernetică beneficiază de sporuri cu caracter specific incluse în partea variabilă a salariului lunar, după cum urmează:

a) pentru personalul încadrat în funcțiile publice din cadrul subdiviziunii interne care exercită nemijlocit funcția de echipă națională de răspuns la incidente de securitate cibernetică – în mărime de 600% din suma anuală a salariilor de bază ale personalului acestei subdiviziuni;

b) pentru personalul încadrat în celelalte funcții publice – în mărime de 200% din suma anuală a salariilor de bază ale personalului încadrat în aceste funcții publice.”.

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 $(4)^1$, cu următorul cuprins:

„$(4)^1$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la articolul 12 alineatul $(5)^1$ 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.”

2. Articolul 12 se completează cu alineatul $(5)^1$, cu următorul cuprins:

„$(5)^1$ 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 legea respectivă, 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 legea respectivă, 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 articolul 7 alineatul $(13)^1$ 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 $(2)^1$ și $(2)^2$ cu următorul cuprins:

„$(2)^1$ 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 legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

$(2)^2$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul $(2)^1$ 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. XXI. – **Codul transportului feroviar 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 articolul 89 alineatul $(3)^1$ 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, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de legea respectivă, 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 prin 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 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.

(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. – (1) Prezenta lege intră în vigoare la data de 1 ianuarie 2025, cu excepția prevederilor art. IV punctele 2, 4-6 și XVIII care intră în vigoare la data publicării legii.

(2) Până la data de 1 ianuarie 2025, Guvernul va aduce actele sale normative în concordanță cu prezenta lege.

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 a anului curent 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,

---

[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

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 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, în termen de 6 luni din data publicării legii, adică până la data de 28 octombrie a anului curent, 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: Potrivit art. 7 alin. (1) din Legea privind securitatea cibernetică, *Guvernul desemnează autoritatea competentă la nivel național în domeniul securității cibernetice și stabilește modul de organizare și funcționare a acesteia*. Această competență a Guvernului urmează, conform art. 23 alin. (2) lit. b), a fi exercitată până la data de 28 ianuarie 2024. În scopul realizării acestei sarcini, Ministerul Dezvoltării Economice și Digitalizării, în calitate de autoritate responsabilă de realizarea politicii statului în domeniul securității cibernetice, a elaborat analiza de impact[4] și proiectul de hotărâre a Guvernului privind organizarea și funcționarea Agenției pentru Securitate Cibernetică. Astfel, 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 22 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, XVII și XVIII)** 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

[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

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 unele prevederi ale acestei legi din perspectiva necesității asigurării bazei juridico-normative pentru instituirea unui model funcțional și eficient de guvernanță în domeniul securității cibernetice și să le alinieze la reglementările legale existente privind modul și principiile de organizare și funcționare a administrației publice centrale de specialitate (punctele 4 și 5), să excludă unele dublări din textul legii (pct. 2, pct. 6) și să aducă în concordanță cu prevederile Legii privind securitatea cibernetică (punctele 1 și 3).

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”.*

Completarea propusă în **pct. 2** este necesară pentru concretizarea responsabilității în elaborarea și promovarea actului respectiv. Notăm că până în prezent acest act normativ nu a fost aprobat de către Guvern. De asemenea, această concretizare este necesară și pentru că la **pct. 6** se abrogă art. 23 din Legea nr. 467/2003. Abrogarea art. 23 este determinată de faptul că prevederile acestuia sunt în disonanță cu prevederile art. 22 din Legea nr. 467/2003 și ale Legii cu privire la Guvern. Or, art. 22 stabilește că Guvernul este cel care stabilește împuternicirile autorităților și instituțiilor publice în domeniul creării, administrării, mentenanței, dezvoltării și utilizării sistemelor și resurselor informaționale de stat.

La pct. 3 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.

Modificările propuse la **pct. 4** au scopul de a ajusta alineatul (1) la obiectul de reglementare al legii, inclusiv din perspectivă terminologică și de a exclude alinatul (2), deoarece acesta dublează prevederile art. 22 din aceeași lege.

În **pct. 5** se propune expunerea în redacție nouă a literelor a) și b), în principiu din aceleași considerente de unificare terminologică nu doar în conținutul normativ al legii modificate, dar și cu terminologia utilizată de legislația privind organizarea și funcționarea administrației publice, în particular Legea nr. 98/2012 privind administrația publică centrală de specialitate.

După cum s-a menționat și mai sus în **pct. 6** se propune abrogarea art. 23, deoarece în primul rând acestea sunt în disonanță cu prevederile art. 22 lit. b), conform căreia Guvernul este

cel competent să stabilească limitele competenței autorităților guvernamentale în acest domeniu și, în al doilea rând, prerogativele atribuite persoanelor juridice de drept public menționate în textul art. 23 sunt deja reglementate în actele normative care reglementează activitatea autorităților și instituțiilor publice menționate la art. 23, aprobate de Guvern.

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. Reiterăm că Ministerul Dezvoltării Economice și Digitalizării a elaborat o primă versiune a proiectului de act normativ care urmează să reglementeze activitatea viitoarei autorități competente. Potrivit opțiunii de bază propuse de minister în analiza de impact[5] la acest proiect această autoritate va avea denumirea de Agenția pentru Securitate 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 28 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 analiza de impact la proiectul de hotărâre a Guvernului „Cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică" și proiectul de act normativ respectiv. La data de 13 iulie anul curent, a fost publicat anunțul de inițiere a

[5] 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

elaborării acestei inițiative de reglementare, analiza de impact[6] fiind anexată. Potrivit acestei analize de impact, 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[7] 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”.*

Actualmente articolul 17, care se propune a fi completat, reglementează sporurile cu caracter specific, care este o componentă a părții variabile a salariului personalului din unitățile bugetare. În proiect este propusă completarea acestui articol cu un alineat nou, al cărui redacție prevede sporuri cu caracter specific în cuantum diferit pentru 2 categorii de personal al viitoarei autorități competente în domeniul securității cibernetice. Astfel, pentru angajații care vor fi implicați direct în exercitarea competenței subdiviziunii de răspuns la incidentele de securitate cibernetică (CSIRT[8]-ul național) acest spor urmează să constituie 600%, iar pentru ceilalți angajați – 200% din suma salariului de bază. În valori absolute aceasta ar însemna că salariile personalului de execuție CSIRT va constitui în jur de 53 mii lei, iar al șefului și șefului adjunct – în jur de 94 mii lei și, respectiv, 87 mii lei. În ce privește ceilalți angajați ai autorității, directorul și directorul adjunct vor avea în jur de 55,6 mii lei și, respectiv, 51 mii lei, ceilalți funcționari cu funcții de conducere (șef direcție, șef secție, șef serviciu) – între 28,5 mii lei – 40,7 mii lei, iar personalul de execuție – între 20 mii lei și 25 mii lei. Ținem să relevăm că în același raport[9] al ENISA, cu titlu orientativ, sunt aduse cifre privind salarizarea personalului unei echipe CSIRT în statele membre ale UE „*un membru al personalului CSIRT (inclusiv managerii) costă în medie 40 000 – 60 000 EUR pe an”. Operațiunile unui CSIRT de mici dimensiuni, cu un personal format din trei persoane (manager, două persoane care se ocupă de gestionarea incidentelor), ar trebui să aibă un buget anual de aproximativ 120 000-180 000 EUR. În cazul în care un CSIRT trebuie să asigure operațiuni 24/7 timp de 365 de zile pe an, acesta are nevoie de cel puțin 12 angajați suplimentari (șase echipe de câte doi membri ai personalului pentru a acoperi 24/7, fiecare tură acoperind 8 ore). Acest lucru va adăuga 480 000 EUR anual la buget”.*

În principiu completările propuse în proiectul de lege constituie un mijloc de atenuare a riscurilor de implementare a opțiunii recomandate în analiza de impact la proiectul de Hotărâre a Guvernului cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate

---

[6] 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;

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

[8] Computer security incident response team - trad. Echipă de răspuns la incidentele de securitate cibernetică

[9] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc, pag 17;

Cibernetică, și au rolul de a asigura baza legală pentru salarizarea personalului autorității competente proporțional riscurilor și obiectivelor pe care această autoritate urmează să le îndeplinească.

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 articolului IV punctele 2, 4-6 și articolului XVIII, care ar urma să intre în vigoare la data publicării legii. În cazul prevederilor art. IV intrarea imediată în vigoare este determinată de natura de clarificare a acestor prevederi în 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.

2. A doua categorie de norme, cuprinse la articolele I – III, V, VII – XV 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 ştiinţifice, ştiinţifice de producţie, ştiinţifico-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 ştiinţifico-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[10]). 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. XIII, 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. 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 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

[10] 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)

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[11]. 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 obligațiilor 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[12], 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 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[13]. 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[14] (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)*

[11] 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);

[12] 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);

[13] 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)

[14] 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)

2018/1972... să beneficieze de cadrul juridic instituit prin" Directiva NIS2[15]. 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 terminologia utilizată de Directiva 2014/65/UE[16], 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

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

[16] 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);

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[17] și, respectiv, Directiva 91/271/CEE[18]. 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 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[19] 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

[17] 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)

[18] 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)

[19] 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)

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 şi 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 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[20]. În consecință, în proiect sunt propuse completări la articolele 38 și 138 din Legea nr. 202/2017 cu prevederi care reflectă același algoritm propus în cazul modificărilor operate la alte legi prin prezentul proiect și anume: specificarea expresă a responsabilității băncilor, identificate ca furnizori de servicii de autoritatea competentă în domeniul securității cibernetice, de a implementa obligațiile de asigurare a securității cibernetice, stabilirea competenței autorității respective de exercitare a funcției de supraveghere și control a modului în care subiecții obligațiilor respective își realizează obligațiile legale și, implicit, asigurarea informării de către autoritatea competentă a Băncii Naționale a Moldovei dacă sunt depistate anumite încălcări legale.

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 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[21]. 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

[20] 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)

[21] 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).

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[22]. 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[23], 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 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.

[22] 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)

[23] 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)

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[24] la proiectul de Lege privind securitatea cibernetică cuprinde informații suficiente care acoperă într-o măsură generală și impactul financiar al prevederilor proiectului în speță. Totuși, referindu-ne la articolul XVIII, 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 25,5 milioane lei anual. Din această sumă, aproximativ 11,2 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 vor fi 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 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

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

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 XVII 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 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. XII, în 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,*** la data de 15 septembrie 2023 a fost publicat anunțul referitor la inițierea elaborării proiectului de lege la care au fost anexate versiunea inițială a proiectului și nota informativă la acesta (https://particip.gov.md/ro/document/stages/anunt-privind-initierea-elaborarii-proiectului-de-lege-pentru-modificarea-unor-acte-normative-executarea-art23-alin-2-lit-a-si-partial-a-lit-b-din-legea-nr-482023-privind-securitatea-cibernetica/11155).

Secretar de stat **Mihai LUPAȘCU**

Tabel comparativ
la proiectul de Lege cu privire la modificarea unor acte normative
(aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică)

Nr. d/o	Prevederea actuală	Modificarea propusă	Prevederea după modificare
Legea nr. 1456/1993 cu privire la activitatea farmaceutică			
1.	**Articolul 3.** Întreprinderi şi instituţii farmaceutice şi tipurile de proprietate asupra lor (1) La întreprinderile şi instituţiile farmaceutice se raportă întreprinderile farmaceutice industriale, întreprinderile (laboratoarele) de microproducţie farmaceutică, laboratoarele de control al calităţii medicamentelor, depozitele farmaceutice, farmaciile, instituţiile de cercetări farmaceutice, instituţiile farmaceutice ştiinţifico-practice. (2) Întreprinderile şi instituţiile farmaceutice pot fi de stat, private sau cu o formă mixtă de proprietate. Schimbarea formei de proprietate a întreprinderilor farmaceutice se efectuează în conformitate cu legislaţia în vigoare. Statul garantează, în conformitate cu legislaţia în vigoare, condiţii egale de funcţionare a întreprinderilor farmaceutice, indiferent de forma de proprietate a acestora. (3) Întreprinderile şi instituţiile farmaceutice pot înfiinţa filiale în conformitate cu legislaţia în vigoare.	Articolul 3 se completează cu alineatul $(4)^1$, cu următorul cuprins: „$(4)^1$ 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.”.	**Articolul 3.** Întreprinderi şi instituţii farmaceutice şi tipurile de proprietate asupra lor (1) La întreprinderile şi instituţiile farmaceutice se raportă întreprinderile farmaceutice industriale, întreprinderile (laboratoarele) de microproducţie farmaceutică, laboratoarele de control al calităţii medicamentelor, depozitele farmaceutice, farmaciile, instituţiile de cercetări farmaceutice, instituţiile farmaceutice ştiinţifico-practice. (2) Întreprinderile şi instituţiile farmaceutice pot fi de stat, private sau cu o formă mixtă de proprietate. Schimbarea formei de proprietate a întreprinderilor farmaceutice se efectuează în conformitate cu legislaţia în vigoare. Statul garantează, în conformitate cu legislaţia în vigoare, condiţii egale de funcţionare a întreprinderilor farmaceutice, indiferent de forma de proprietate a acestora. (3) Întreprinderile şi instituţiile farmaceutice pot înfiinţa filiale în conformitate cu legislaţia în vigoare. (4) Întreprinderile şi instituţiile farmaceutice vor activa în conformitate cu prevederile Regulilor de bune practici, aprobate de către Guvern.

	(4) Întreprinderile şi instituţiile farmaceutice vor activa în conformitate cu prevederile Regulilor de bune practici, aprobate de către Guvern.		(4)[1] 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.** Cercetări farmacologice şi farmaceutice (1) În scopul creării de medicamente noi se faccercetări orientate spre depistarea de substanţe active din punct de vedere biologic, studierea calităţilor lor farmacologice şi a acţiunii secundare, aprecierea inocuităţii, eficacităţii terapeutice, elaborarea formelor medicamentoase, metodelor de analiză a lor, a criteriilor de standardizare şi a documentaţiei analitico-normative. (2) Investigaţiile în vederea creării Medicamentelor noi se efectuează în instituţii de cercetări ştiinţifice, ştiinţifice de producţie, ştiinţifico-practice, de învăţământ, precum şi de către persoane fizice.	Articolul 9 se completează cu alineatul (2)[1] cu următorul cuprins: „(2)[1] Persoanele juridice 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.”.	**Articolul 9.** Cercetări farmacologice şi farmaceutice (1) În scopul creării de medicamente noi se faccercetări orientate spre depistarea de substanţe active din punct de vedere biologic, studierea calităţilor lor farmacologice şi a acţiunii secundare, aprecierea inocuităţii, eficacităţii terapeutice, elaborarea formelor medicamentoase, metodelor de analiză a lor, a criteriilor de standardizare şi a documentaţiei analitico-normative. (2) Investigaţiile în vederea creării medicamentelor noi se efectuează în instituţii de cercetări ştiinţifice, ştiinţifice de producţie, ştiinţifico-practice, de învăţământ, precum şi de către persoane fizice. (2)[1] Persoanele juridice 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.** Modul de efectuare a controlului de stat (1) Controlul de stat al calităţii medicamentelor şi produselor parafarmaceutice produse la întreprinderile şi instituţiile farmaceutice din republică se efectuează în conformitate cu cerinţele Farmacopeei şi altei documentaţii analitico-normative aprobate de Ministerul Sănătății. (2) Controlul calităţii medicamentelor, materiei prime medicamentoase şi produselor parafarmaceutice importate se efectuează în conformitate cu prevederile farmacopeelor în vigoare sau în corespundere cu cerinţele documentelor analitico-normative aprobate în modul stabilit de Ministerul Sănătății. (3) Controlul de stat al calităţii medicamentelor autohtone şi de import este exercitat de către Agenţia Medicamentului şi Dispozitivelor Medicale. (4) Organele abilitate de Guvern elaborează şi implementează sisteme informaţionale automatizate ce asigură plasarea pe piaţa farmaceutică doar a medicamentelor supuse controlului calităţii şi fabricate sau importate în mod legal.	Articolul 16 se completează cu alineatul (4)[1] cu următorul cuprins: „(4)[1] Supravegherea și controlul de stat al respectării de către întreprinderile și instituțiile farmaceutice a obligațiilor stabilite la art. 3 alin. (4)[1], precum și de către persoanele juridice care efectuează investigații în vederea creării medicamentelor noi a obligațiilor stabilite la art. 9 alin. (2)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”.	**Articolul 16.** Modul de efectuare a controlului de stat (1) Controlul de stat al calităţii medicamentelor şi produselor parafarmaceutice produse la întreprinderile şi instituţiile farmaceutice din republică se efectuează în conformitate cu cerinţele Farmacopeei şi altei documentaţii analitico-normative aprobate de Ministerul Sănătății. (2) Controlul calităţii medicamentelor, materiei prime medicamentoase şi produselor parafarmaceutice importate se efectuează în conformitate cu prevederile farmacopeelor în vigoare sau în corespundere cu cerinţele documentelor analitico-normative aprobate în modul stabilit de Ministerul Sănătății. (3) Controlul de stat al calităţii medicamentelor autohtone şi de import este exercitat de către Agenţia Medicamentului şi Dispozitivelor Medicale. (4) Organele abilitate de Guvern elaborează şi implementează sisteme informaţionale automatizate ce asigură plasarea pe piaţa farmaceutică doar a medicamentelor supuse controlului calităţii şi fabricate sau importate în mod legal. (4)[1] Supravegherea și controlul de stat al respectării de către întreprinderile și instituțiile

			farmaceutice a obligațiilor stabilite la art. 3 alin. (4)[1], precum și de către persoanele juridice care efectuează investigații în vederea creării medicamentelor noi a obligațiilor stabilite la art. 9 alin. (2)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.
Articolul 4 din Legea ocrotirii sănătății nr. 411/1995			
1.	**Articolul 4.** Prestatorii de servicii medicale (1) Prestatorii de servicii medicale pot fi publici sau privați. Prestatorii publici de servicii medicale sînt instituțiile medico-sanitare publice și autoritățile/instituțiile bugetare. (2) Instituţia medico-sanitară publică se instituie prin decizie a Ministerului Sănătății sau a autorităţii administraţiei publice locale, în baza nomenclatorului prestatorilor de servicii medicale aprobat conform alin. (5). Instituţia medico-sanitară publică departamentală se instituie prin decizie a autorităţii centrale de specialitate. (2[1]) Conducătorii instituţiilor medico-sanitare publice republicane, municipale, raionale sînt selectaţi prin concurs organizat de Ministerul Sănătății şi sînt numiţi în funcţie de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de raion). Eliberarea din funcţie a conducătorilor instituţiilor medico-sanitare publice republicane, municipale, raionale se efectuează de către persoana responsabilă a	Se completează cu alineatele (7)[1] și (7)[2], cu următorul cuprins: „(7)[1] 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. (7)[2] Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor prevăzute la alin. (7)[1] se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”	**Articolul 4.** Prestatorii de servicii medicale (1) Prestatorii de servicii medicale pot fi publici sau privați. Prestatorii publici de servicii medicale sînt instituțiile medico-sanitare publice și autoritățile/instituțiile bugetare. (2) Instituţia medico-sanitară publică se instituie prin decizie a Ministerului Sănătății sau a autorităţii administraţiei publice locale, în baza nomenclatorului prestatorilor de servicii medicale aprobat conform alin. (5). Instituţia medico-sanitară publică departamentală se instituie prin decizie a autorităţii centrale de specialitate. (2[1]) Conducătorii instituţiilor medico-sanitare publice republicane, municipale, raionale sînt selectaţi prin concurs organizat de Ministerul Sănătății şi sînt numiţi în funcţie de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de raion). Eliberarea din funcţie a conducătorilor instituţiilor medico-sanitare publice republicane, municipale, raionale se efectuează de către persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de

	fondatorului (respectiv, ministru, primar al municipiului, președinte de raion). Regulamentul privind numirea în funcţie a conducătorilor instituţiilor medico-sanitare publice în bază de concurs se aprobă de Guvern. (2^2) Conducătorul instituţiei medico-sanitare publice gestionează instituţia în baza unui contract de management încheiat cu persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de raion) pe o durată de 5 ani, conform contractului-tip de management al instituției medico-sanitare publice aprobat de Guvern. La expirarea termenului de 5 ani, funcția de conducător al instituției medico-sanitare publice devine vacantă. Funcţia de conducător al instituţiei medico-sanitare publice nu poate fi ocupată de către persoana care activează concomitent în cadrul unui prestator privat de servicii medicale sau farmaceutice. (3) Persoanele fizice şi persoanele juridice au dreptul să fondeze prestatori privați de servicii medicale şi poartă răspundere pentru asigurarea lor financiară şi tehnico-materială, pentru organizarea de asistenţă medicală şi pentru calitatea ei, conform legislaţiei în vigoare. (4) Prestatorii privați de servicii medicale și farmaceutice, cu excepția celor prevăzuți la art. 365, își desfăşoară activitatea în spaţiile ce le aparţin cu drept de proprietate privată sau în alte spaţii luate în locaţiune, inclusiv ale instituţiilor medico-sanitare publice, cu		raion). Regulamentul privind numirea în funcţie a conducătorilor instituţiilor medico-sanitare publice în bază de concurs se aprobă de Guvern. (2^2) Conducătorul instituţiei medico-sanitare publice gestionează instituţia în baza unui contract de management încheiat cu persoana responsabilă a fondatorului (respectiv, ministru, primar al municipiului, președinte de raion) pe o durată de 5 ani, conform contractului-tip de management al instituției medico-sanitare publice aprobat de Guvern. La expirarea termenului de 5 ani, funcția de conducător al instituției medico-sanitare publice devine vacantă. Funcţia de conducător al instituţiei medico-sanitare publice nu poate fi ocupată de către persoana care activează concomitent în cadrul unui prestator privat de servicii medicale sau farmaceutice. (3) Persoanele fizice şi persoanele juridice au dreptul să fondeze prestatori privați de servicii medicale şi poartă răspundere pentru asigurarea lor financiară şi tehnico-materială, pentru organizarea de asistenţă medicală şi pentru calitatea ei, conform legislaţiei în vigoare. (4) Prestatorii privați de servicii medicale și farmaceutice, cu excepția celor prevăzuți la art. 365, își desfăşoară activitatea în spaţiile ce le aparţin cu drept de proprietate privată sau în alte spaţii luate în locaţiune, inclusiv ale instituţiilor medico-sanitare publice, cu gen de activitate în domeniul ocrotirii sănătăţii, care corespund cerinţelor actelor legislative şi normative în vigoare privind parteneriatul public-privat.

	gen de activitate în domeniul ocrotirii sănătăţii, care corespund cerinţelor actelor legislative şi normative în vigoare privind parteneriatul public-privat. (5) Regulamentele şi nomenclatorul prestatorilor de servicii medicale, indiferent de tipul de proprietate şi forma juridică de organizare, precum şi lista serviciilor prestate de acestea, sînt aprobate de Ministerul Sănătății, cu excepţia celor ale organelor de drept şi ale organelor militare. (6) Parlamentul reorganizează, prin acte legislative, sistemul naţional de sănătate, domeniul medicamentului şi al activităţii farmaceutice. (7) Persoana responsabilă a fondatorului aprobă organigrama şi statele de personal ale prestatorului de servicii medicale.		(5) Regulamentele şi nomenclatorul prestatorilor de servicii medicale, indiferent de tipul de proprietate şi forma juridică de organizare, precum şi lista serviciilor prestate de acestea, sînt aprobate de Ministerul Sănătății, cu excepţia celor ale organelor de drept şi ale organelor militare. (6) Parlamentul reorganizează, prin acte legislative, sistemul naţional de sănătate, domeniul medicamentului şi al activităţii farmaceutice. (7) Persoana responsabilă a fondatorului aprobă organigrama şi statele de personal ale prestatorului de servicii medicale. (7)[1] 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. (7)[2] Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor prevăzute la alin. (7)[1] se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.
Codul navigaţiei maritime comerciale nr. 599/1999			

1.	-	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 legea respectivă, 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 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.”.	**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 legea respectivă, 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 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.
Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat			
1.	**Articolul 3.** Noţiuni principale *securitate cibernetică* – stare de normalitate a sistemului și resursei informaționale, rezultată în urma aplicării unui ansamblu de măsuri prin care este asigurată autenticitatea,	La articolul 3, definiția noțiunii „securitate cibernetică” va avea următorul cuprins „ – astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică”;	**Articolul 3.** Noţiuni principale *securitate cibernetică* — astfel cum este definită la art. 2 din Legea nr. 48/2023 privind securitatea cibernetică

	integritatea, confidențialitatea, disponibilitatea şi nonrepudierea datelor;		
2.	**Articolul 7[6].** Documentele sistemelor și resurselor informaționale de stat (3) Documentele sistemelor informaționale de stat sunt elaborate în conformitate cu cadrul normativ metodologic privind crearea, administrarea, mentenanța, dezvoltarea și scoaterea din exploatare a sistemelor informaționale de stat, aprobat de către Guvern.	Articolul 7[6] alineatul (3) se completează în final cu textul: „la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul informatizării și a resurselor informaționale de stat”.	**Articolul 7[6].** Documentele sistemelor și resurselor informaționale de stat (3) Documentele sistemelor informaționale de stat sunt elaborate în conformitate cu cadrul normativ metodologic privind crearea, administrarea, mentenanța, dezvoltarea și scoaterea din exploatare a sistemelor informaționale de stat, aprobat de către Guvern la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul informatizării și a resurselor informaționale de stat.
3.	**Articolul 10.** Securitatea sistemelor și resurselor informaționale de stat (1) Securitatea, inclusiv securitatea cibernetică, a sistemelor și resurselor informaționale de stat este asigurată de către autorităţile publice, instituţiile publice şi alte entități de stat, în limita competențelor acestora și în conformitate cu reglementările stabilite de către Guvern.	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.”	**Articolul 10.** Securitatea sistemelor și resurselor informaționale de stat (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
4.	**Articolul 21.** Politica informaţională de stat (1) Politica informaţională de stat este orientată spre crearea condiţiilor juridice, economice, organizatorice şi de altă natură, necesare asigurării unei dezvoltări armonioase a societăţii şi a statului.	La articolul 21: titlul articolului va avea următorul cuprins: „Articolul 21. Politica statului în domeniul informatizării și resurselor informaționale de stat”;	**Articolul 21.** Politica statului în domeniul informatizării și resurselor informaționale de stat Politica statului în domeniul informatizării și resurselor informaționale de stat este orientată spre crearea condiţiilor juridice, economice,

	(2) Politica privind resursele informaţionale de stat este elaborată de Ministerul Economiei şi aprobată de Guvern.	la alineatul (1) cuvintele „Politica informațională de stat” se substituie cu cuvintele „Politica statului în domeniul informatizării și resurselor informaționale de stat”; alineatul (1) devine alineat unic; alineatul (2) se abrogă.	organizatorice şi de altă natură, necesare asigurării unei dezvoltări armonioase a societăţii şi a statului.
5.	**Articolul 22.** Atribuţiile Guvernului În vederea executării prezentei legi, Guvernul: a) aprobă documente de politici și reglementări în domeniul informatizării, al sistemelor și resurselor informaționale de stat; b) stabilește împuternicirile autorităților și instituțiilor publice în domeniul creării, administrării, mentenanței, dezvoltării și utilizării sistemelor și resurselor informaționale de stat; c) aprobă crearea sistemelor și resurselor informaționale de stat; d) aprobă conceptele sistemelor informaționale de stat și regulamentele resurselor informaționale de stat; e) aprobă regulile și modul de găzduire a sistemelor informaționale de stat.	La articolul 22: literele a) și b) vor avea următorul cuprins: „a) asigură realizarea politicii statului în domeniul informatizării și resurselor informaționale de stat prin intermediul ministerelor și altor autorități administrative centrale; b) determină competența ministerelor, a altor autorități administrative centrale, a structurilor organizaționale din sfera de competență ale acestora și a altor autorități și instituții publice;”;	**Articolul 22.** Atribuţiile Guvernului În vederea executării prezentei legi, Guvernul: a) asigură realizarea politicii statului în domeniul informatizării și resurselor informaționale de stat prin intermediul ministerelor și altor autorități administrative centrale; b) determină competența ministerelor, a altor autorități administrative centrale, a structurilor organizaționale din sfera de competență ale acestora și a altor autorități și instituții publice; c) aprobă crearea sistemelor și resurselor informaționale de stat; d) aprobă conceptele sistemelor informaționale de stat și regulamentele resurselor informaționale de stat; e) aprobă regulile și modul de găzduire a sistemelor informaționale de stat.
6.	**Articolul 23.** Competențele de bază ale autorităților și instituțiilor publice în domeniul sistemelor și resurselor informaționale de stat (1) Ministerul Economiei este organul central de specialitate care elaborează documentele de politici și actele normative în domeniul informatizării, al sistemelor și resurselor	Articolul 23 se abrogă.	**Articolul 23.** - *abrogat;*

	informaționale de stat, precum și exercită și alte atribuții în conformitate cu regulamentul acestuia aprobat de către Guvern. (2) Instituția publică Agenția de Guvernare Electronică elaborează cadrul metodologic pentru administrarea, mentenanța, dezvoltarea și scoaterea din exploatare a sistemelor informaționale de stat, coordonează și monitorizează crearea, administrarea și dezvoltarea sistemelor informaționale de stat, asigură evidența acestora, efectuează auditul de securitate cibernetică a sistemelor informaționale de stat, precum și exercită și alte atribuții în conformitate cu statutul acesteia aprobat de către Guvern. (3) Instituţia publică Serviciul Tehnologia Informaţiei şi Securitate Cibernetică, în limita competențelor, administrează infrastructura tehnologiilor informaționale ale autorităților și instituțiilor publice, exercită atribuțiile administratorului tehnic și asigură mentenanța sistemelor informaționale de stat, asigură securitatea cibernetică a acestora, precum și exercită și alte atribuții în conformitate cu statutul acesteia aprobat de către Guvern. (4) Instituția publică Agenţia Servicii Publice exercită, în numele Guvernului, atribuțiile de posesor al resurselor informaționale de bază. (5) Alte autorităţi și instituții publice formează și utilizează resurse informaționale departamentale şi teritoriale în scopul exercitării atribuțiilor acestora şi participă la formarea resurselor informaționale de bază în		

	limita competențelor stabilite de către Guvern.		
Legea comunicațiilor electronice nr. 241/2007			
1.	**Art. 21. -** (1) În scopul asigurării securității și integrității rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului, furnizorii au obligația: a) de a lua toate măsurile tehnice și organizatorice adecvate pentru a administra riscurile care pot afecta securitatea rețelelor și serviciilor. Măsurile luate trebuie să asigure un nivel de securitate corespunzător riscului identificat și să prevină sau să minimizeze impactul incidentelor de securitate asupra utilizatorilor și rețelelor interconectate, avînd în vedere cele mai noi tehnologii; b) de a lua măsurile necesare pentru a garanta integritatea rețelelor și pentru a asigura continuitatea furnizării serviciilor prin intermediul acestor rețele; c) de a notifica Agenția și, după caz, organele împuternicite, în cel mai scurt timp, cu privire la orice caz de încălcare a securității sau pierdere a integrității care are un impact semnificativ asupra furnizării rețelelor publice de comunicații electronice și/sau serviciilor de comunicații electronice accesibile publicului; d) de a colabora între ei, după caz, pentru implementarea măsurilor prevăzute la lit. a) și b). (2) Măsurile minime de securitate pe care trebuie să le stabilească și să le implementeze furnizorii astfel încît să îndeplinească	Articolul 21 va avea următorul cuprins: „Articolul 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 alineatul (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.”	**Articolul 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 alineatul (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.

	obligațiile prevăzute la alin. (1) lit. a) și b) vor viza cel puțin următoarele domenii: a) politica de securitate și managementul riscului; b) securitatea resurselor umane; c) securitatea și integritatea rețelelor, infrastructurii asociate și informațiilor; d) managementul operațiunilor; e) managementul incidentelor; f) managementul continuității afacerii; g) monitorizare, testare și audit. (3) Agenția poate informa publicul cu privire la existența cazului specificat la alin. (1) lit. c) sau poate solicita furnizorului să informeze publicul cu privire la existența acestui caz atunci cînd consideră că este în interesul publicului. (4) Agenția poate stabili modalitatea de implementare a prevederilor alin. (1)–(3), inclusiv în legătură cu termenele de punere în aplicare, cu respectarea procedurii de consultare publică.		
2.	**Art. 22. -** (1) În vederea aplicării prevederilor art. 21, Agenția poate solicita furnizorilor de rețele publice de comunicații electronice și/sau servicii de comunicații electronice accesibile publicului: a) să furnizeze toate informațiile necesare evaluării securității și integrității rețelelor și serviciilor, inclusiv a politicilor interne de securitate aplicabile; b) să inițieze, pe cont propriu, dar nu mai des decît o dată pe an, un audit de securitate realizat de un organism calificat, independent și să transmită Agenției rezultatele auditului.	Articolul 22 se abrogă.	**Art. 22.** – *abrogat.*

<table>
<tr><td></td><td>(2) Agenția poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și/sau serviciilor, precum și respectarea acestora în cazurile de încălcare a securității rețelelor și/sau serviciilor ori de pierdere a integrității rețelelor, avînd posibilitatea de a impune în acest sens măsuri care vor viza stabilirea politicilor, strategiilor, proceselor și procedurilor de asigurare a securității și integrității rețelelor, infrastructurii asociate și informațiilor, resurselor umane, de asemenea poate verifica și evalua managementul operațiunilor, incidentelor, continuității afacerii și procesul de monitorizare.</td><td></td><td></td></tr>
<tr><td colspan="4">Punctul 1 din anexa la Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător</td></tr>
<tr><td>1.</td><td>-</td><td>Se completează cu poziția 13[1] cu următorul cuprins:
<table><tr><td>13[1]</td><td>Agenția pentru Securitate Cibernetică</td><td>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</td></tr></table></td><td><table><tr><td>13[1]</td><td>Agenția pentru Securitate Cibernetică</td><td>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</td></tr></table></td></tr>
<tr><td colspan="4">Legea nr. 171/2012 privind piața de capital</td></tr>
<tr><td>1.</td><td>Articolul 41. Cerinţe organizatorice generale</td><td>Se modifică după cum urmează:
Articolul 41 se completează cu alineatul (8)[1] cu următorul cuprins:</td><td>Articolul 41. Cerinţe organizatorice generale</td></tr>
</table>

	(1) Societatea de investiţii este obligată să îndeplinească următoarele cerinţe: a) să stabilească, să aplice şi să menţină proceduri decizionale şi o structură organizatorică care să specifice în mod exact şi documentat structurile ierarhice şi să repartizeze funcţii şi responsabilităţi; b) să garanteze că persoanele relevante ale societăţii de investiţii cunosc procedurile ce trebuie urmate pentru îndeplinirea adecvată a responsabilităţilor ce le revin; c) să stabilească, să aplice şi să menţină mecanisme adecvate de control intern concepute pentru a asigura respectarea deciziilor şi procedurilor existente la toate nivelurile societăţii de investiţii; d) să angajeze și să mențină personal care posedă cunoștințe, experiență și competențe profesionale, conform cerințelor stabilite de actele normative ale Comisiei Naționale; e) să stabilească, să aplice şi să menţină la toate nivelurile importante ale societăţii de investiţii un sistem eficient de raportare internă şi de comunicare a informaţiilor; f) să păstreze o înregistrare adecvată şi ordonată a operaţiunilor efectuate şi a organizării interne; g) să garanteze că îndeplinirea de către persoanele competente a mai multor funcţii nu împiedică şi nu este probabil să împiedice persoanele respective să îndeplinească o anumită funcţie în mod corect, onest şi profesionist; h) să stabilească, să aplice şi să menţină politici şi practici de remunerare care să promoveze şi să fie în concordanţă cu o gestiune adecvată şi eficace a riscurilor;	„(8)[1] 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 legii respective conform actelor normative de punere a acesteia în aplicare și conform altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. Supravegherea și controlul de stat al modului în care societățile de investiții îndeplinesc obligațiile respective se realizează de către autoritatea competentă conform Legii nr. 48/2023 privind securitatea cibernetică.”.	(1) Societatea de investiţii este obligată să îndeplinească următoarele cerinţe: a) să stabilească, să aplice şi să menţină proceduri decizionale şi o structură organizatorică care să specifice în mod exact şi documentat structurile ierarhice şi să repartizeze funcţii şi responsabilităţi; b) să garanteze că persoanele relevante ale societăţii de investiţii cunosc procedurile ce trebuie urmate pentru îndeplinirea adecvată a responsabilităţilor ce le revin; c) să stabilească, să aplice şi să menţină mecanisme adecvate de control intern concepute pentru a asigura respectarea deciziilor şi procedurilor existente la toate nivelurile societăţii de investiţii; d) să angajeze și să mențină personal care posedă cunoștințe, experiență și competențe profesionale, conform cerințelor stabilite de actele normative ale Comisiei Naționale; e) să stabilească, să aplice şi să menţină la toate nivelurile importante ale societăţii de investiţii un sistem eficient de raportare internă şi de comunicare a informaţiilor; f) să păstreze o înregistrare adecvată şi ordonată a operaţiunilor efectuate şi a organizării interne; g) să garanteze că îndeplinirea de către persoanele competente a mai multor funcţii nu împiedică şi nu este probabil să împiedice persoanele respective să îndeplinească o anumită funcţie în mod corect, onest şi profesionist; h) să stabilească, să aplice şi să menţină politici şi practici de remunerare care să promoveze şi să fie în concordanţă cu o gestiune adecvată şi eficace a riscurilor;

	i) la cererea Comisiei Naționale sau cel puțin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naționale, auditul tehnic al sistemelor informaționale utilizate. (2) Pentru îndeplinirea cerinţelor stabilite la alin. (1) lit. g), societăţile de investiţii iau în considerare natura, amploarea şi complexitatea activităţilor desfăşurate de ele, precum şi natura şi gama serviciilor şi activităţilor de investiţii întreprinse în cadrul activităţilor respective. (3) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină sisteme şi proceduri adecvate pentru păstrarea securităţii, integrităţii şi confidenţialităţii informaţiilor, ţinînd seama de natura informaţiilor în cauză. (4) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină o politică adecvată de continuitate a activităţii comerciale pentru a asigura, în caz de întrerupere a sistemelor şi a procedurilor lor, conservarea datelor şi funcţiilor fundamentale, precum şi continuarea serviciilor şi activităţilor de investiţii sau, în cazul cînd acest lucru nu este posibil, recuperarea la timp a datelor şi a funcţiilor respective şi reluarea în timp util a serviciilor şi a activităţilor de investiţii. (5) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină politici şi proceduri contabile care să le permită să		i) la cererea Comisiei Naționale sau cel puțin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naționale, auditul tehnic al sistemelor informaționale utilizate. (2) Pentru îndeplinirea cerinţelor stabilite la alin. (1) lit. g), societăţile de investiţii iau în considerare natura, amploarea şi complexitatea activităţilor desfăşurate de ele, precum şi natura şi gama serviciilor şi activităţilor de investiţii întreprinse în cadrul activităţilor respective. (3) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină sisteme şi proceduri adecvate pentru păstrarea securităţii, integrităţii şi confidenţialităţii informaţiilor, ţinînd seama de natura informaţiilor în cauză. (4) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină o politică adecvată de continuitate a activităţii comerciale pentru a asigura, în caz de întrerupere a sistemelor şi a procedurilor lor, conservarea datelor şi funcţiilor fundamentale, precum şi continuarea serviciilor şi activităţilor de investiţii sau, în cazul cînd acest lucru nu este posibil, recuperarea la timp a datelor şi a funcţiilor respective şi reluarea în timp util a serviciilor şi a activităţilor de investiţii. (5) Societăţile de investiţii sînt obligate să stabilească, să aplice şi să menţină politici şi proceduri contabile care să le permită să furnizeze, în timp util, autorităţii competente, la cererea acesteia, situaţiile financiare ce ar reflecta imaginea fidelă şi onestă a situaţiei financiare a societăţilor respective şi ar respecta

	furnizeze, în timp util, autorităţii competente, la cererea acesteia, situaţiile financiare ce ar reflecta imaginea fidelă şi onestă a situaţiei financiare a societăţilor respective şi ar respecta toate standardele şi normele de contabilitate în vigoare. (6) Societăţile de investiţii sînt obligate să monitorizeze şi să evalueze periodic caracterul adecvat şi eficienţa sistemelor şi mecanismelor lor de control intern şi ale acordurilor încheiate în conformitate cu alin. (1), (3)–(5) şi să adopte măsuri adecvate pentru remedierea eventualelor deficienţe. (7) Cadrele de conducere ale societăţii de investiţii şi, după caz, cadrele de supraveghere a cadrelor de conducere trebuie să evalueze şi să verifice periodic eficienţa politicilor, dispoziţiilor şi procedurilor puse în aplicare şi să adopte măsurile adecvate pentru remedierea eventualelor deficienţe. Această evaluare şi/sau verificare se va efectua în temeiul rapoartelor scrise prezentate de către persoanele responsabile cel puţin o dată pe an. (8) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină proceduri eficiente şi transparente pentru soluţionarea rezonabilă şi promptă a reclamaţiilor primite de la clienţii obişnuiţi sau potenţialii clienţi obişnuiţi şi să înregistreze fiecare reclamaţie şi măsurile adoptate în vederea soluţionării acesteia.		toate standardele şi normele de contabilitate în vigoare. (6) Societăţile de investiţii sînt obligate să monitorizeze şi să evalueze periodic caracterul adecvat şi eficienţa sistemelor şi mecanismelor lor de control intern şi ale acordurilor încheiate în conformitate cu alin. (1), (3)–(5) şi să adopte măsuri adecvate pentru remedierea eventualelor deficienţe. (7) Cadrele de conducere ale societăţii de investiţii şi, după caz, cadrele de supraveghere a cadrelor de conducere trebuie să evalueze şi să verifice periodic eficienţa politicilor, dispoziţiilor şi procedurilor puse în aplicare şi să adopte măsurile adecvate pentru remedierea eventualelor deficienţe. Această evaluare şi/sau verificare se va efectua în temeiul rapoartelor scrise prezentate de către persoanele responsabile cel puţin o dată pe an. (8) Societatea de investiţii este obligată să stabilească, să aplice şi să menţină proceduri eficiente şi transparente pentru soluţionarea rezonabilă şi promptă a reclamaţiilor primite de la clienţii obişnuiţi sau potenţialii clienţi obişnuiţi şi să înregistreze fiecare reclamaţie şi măsurile adoptate în vederea soluţionării acesteia. (8)[1] 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 legii respective conform actelor normative de

			punere a acesteia în aplicare și conform altor acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. Supravegherea și controlul de stat al modului în care societățile de investiții îndeplinesc obligațiile respective se realizează de către autoritatea competentă conform Legii nr. 48/2023 privind securitatea cibernetică.
2.	**Articolul 62.** Cerinţe privind activitatea operatorilor de piaţă (1) Operatorul de piaţă este obligat să elaboreze şi să aplice politici în scopul prestării serviciilor şi menţinerii activităţii la cele mai bune condiţii, inclusiv: a) de identificare şi administrare a conflictelor de interese ce pot apărea între deţinătorii de acţiuni în capitalul social al operatorului de piaţă, angajaţii operatorului de piaţă, membrii pieţei reglementate şi clienţii acestora, şi participanţii pieţei reglementate; b) de audit intern; c) privind securitatea, integritatea şi confidenţialitatea informaţiilor interne; d) privind identificarea şi gestionarea riscurilor. (2) Operatorul de piaţă este obligat: a) să dispună de dotarea tehnică corespunzătoare pentru a menţine funcţionarea sistemelor de tranzacţionare şi de finalizare a tranzacţiilor cu instrumente financiare; b) să dispună de resursele necesare pentru a asigura activitatea ordonată şi continuă a pieţei reglementate, avîndu-se în vedere	Se modifică după cum urmează: Articolul 62 se completează cu alineatul (3)[1] cu următorul cuprins: „(3)[1] 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. Supravegherea și controlul de stat al modului în care operatorii de piață îndeplinesc obligațiile respective se realizează de către autoritatea competentă conform Legii nr. 48/2023 privind securitatea cibernetică.”	**Articolul 62.** Cerinţe privind activitatea operatorilor de piaţă (1) Operatorul de piaţă este obligat să elaboreze şi să aplice politici în scopul prestării serviciilor şi menţinerii activităţii la cele mai bune condiţii, inclusiv: a) de identificare şi administrare a conflictelor de interese ce pot apărea între deţinătorii de acţiuni în capitalul social al operatorului de piaţă, angajaţii operatorului de piaţă, membrii pieţei reglementate şi clienţii acestora, şi participanţii pieţei reglementate; b) de audit intern; c) privind securitatea, integritatea şi confidenţialitatea informaţiilor interne; d) privind identificarea şi gestionarea riscurilor. (2) Operatorul de piaţă este obligat: a) să dispună de dotarea tehnică corespunzătoare pentru a menţine funcţionarea sistemelor de tranzacţionare şi de finalizare a tranzacţiilor cu instrumente financiare; b) să dispună de resursele necesare pentru a asigura activitatea ordonată şi continuă a pieţei reglementate, avîndu-se în vedere natura, volumul şi periodicitatea tranzacţiilor, precum şi riscurile la care sînt expuse;

	natura, volumul şi periodicitatea tranzacţiilor, precum şi riscurile la care sînt expuse; c) să elaboreze şi, în caz de necesitate, să aplice un plan de urgenţă privind recuperarea datelor în caz de disfuncţiuni şi de testare periodică a sistemelor backup; d) să instituie mecanisme şi proceduri ce vor asigura finalizarea eficientă şi la timp a tranzacţiilor încheiate în cadrul pieţei reglementate; e) să efectueze auditul obligatoriu al situațiilor financiare; f) la cererea Comisiei Naționale sau cel puțin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naționale, auditul tehnic al sistemelor informaționale utilizate. (3) Prevederile art. 39 alin. (4)–(6) şi art. 40 se aplică corespunzător operatorilor de piaţă.		c) să elaboreze şi, în caz de necesitate, să aplice un plan de urgenţă privind recuperarea datelor în caz de disfuncţiuni şi de testare periodică a sistemelor backup; d) să instituie mecanisme şi proceduri ce vor asigura finalizarea eficientă şi la timp a tranzacţiilor încheiate în cadrul pieţei reglementate; e) să efectueze auditul obligatoriu al situațiilor financiare; f) la cererea Comisiei Naționale sau cel puțin o dată la 4 ani, să efectueze, în conformitate cu actele normative ale Comisiei Naționale, auditul tehnic al sistemelor informaționale utilizate. (3) Prevederile art. 39 alin. (4)–(6) şi art. 40 se aplică corespunzător operatorilor de piaţă. „(3)[1] 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. Supravegherea și controlul de stat al modului în care operatorii de piață îndeplinesc obligațiile respective se realizează de către autoritatea competentă conform Legii nr. 48/2023 privind securitatea cibernetică.
Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova			
1.	-	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

		„**Articolul 37[1]. Asigurarea securității cibernetice** (2) 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 legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (3) 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.”.	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 legea respectivă, 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 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.
Legea nr. 303/2013 privind serviciul public de alimentare cu apă și de canalizare			
1.	**Articolul 9.** Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare se efectuează de către:	Articolul 9 se completează cu litera d)[1], cu următorul cuprins: „d)[1] autoritatea competentă la nivel național să exercite supravegherea și controlul de stat a respectării legislației în domeniul securității cibernetice.”;	**Articolul 9.** Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare Supravegherea şi controlul de stat al serviciului public de alimentare cu apă şi de canalizare se efectuează de către:

	a) serviciul supravegherii de stat a sănătăţii publice; b) organul de protecţie a mediului înconjurător; c) serviciul de administrare şi de supraveghere a resurselor de apă; d) organul de control asupra aplicării legislaţiei şi a documentelor normative în construcţii.		a) serviciul supravegherii de stat a sănătăţii publice; b) organul de protecţie a mediului înconjurător; c) serviciul de administrare şi de supraveghere a resurselor de apă; d) organul de control asupra aplicării legislaţiei şi a documentelor normative în construcţii; d)[1] autoritatea competentă la nivel național să exercite supravegherea și controlul de stat a respectării legislației în domeniul securității cibernetice.
2.	**Articolul 9[1].** Efectuarea controalelor (1) Agenția monitorizează și verifică, prin control, activitatea operatorilor pentru asigurarea respectării legislației din domeniu în desfășurarea activității licențiate, a respectării principiului costurilor necesare și justificate la calcularea tarifelor pentru serviciul de alimentare cu apă și de canalizare, avînd și alte competențe acordate prin prezenta lege. (2) În vederea asigurării prevederilor alin. (1), Agenția efectuează controale și stabilește, în funcție de complexitate, durata necesară pentru efectuarea acestora, care nu trebuie să depășească 90 de zile. Perioada de întocmire a raportului de control și de prezentare a acestuia operatorilor supuși controlului nu poate depăși 30 de zile lucrătoare de la data încheierii controlului. Rapoartele privind rezultatele controlului, întocmite de angajaţii Agenţiei, se înaintează Consiliului de administraţie spre examinare, care, prin hotărîre, se pronunță pe marginea acestora şi dispune, după caz, luarea de măsuri pentru	Articolul 9[1] se completează cu alineatul (3)[1], cu următorul cuprins: „(3)[1] 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.”	**Articolul 9[1].** Efectuarea controalelor (1) Agenția monitorizează și verifică, prin control, activitatea operatorilor pentru asigurarea respectării legislației din domeniu în desfășurarea activității licențiate, a respectării principiului costurilor necesare și justificate la calcularea tarifelor pentru serviciul de alimentare cu apă și de canalizare, avînd și alte competențe acordate prin prezenta lege. (2) În vederea asigurării prevederilor alin. (1), Agenția efectuează controale și stabilește, în funcție de complexitate, durata necesară pentru efectuarea acestora, care nu trebuie să depășească 90 de zile. Perioada de întocmire a raportului de control și de prezentare a acestuia operatorilor supuși controlului nu poate depăși 30 de zile lucrătoare de la data încheierii controlului. Rapoartele privind rezultatele controlului, întocmite de angajaţii Agenţiei, se înaintează Consiliului de administraţie spre examinare, care, prin hotărîre, se pronunță pe marginea acestora şi dispune, după caz, luarea de măsuri pentru înlăturarea abaterilor constatate şi/sau pentru aplicarea unor sancţiuni.

	înlăturarea abaterilor constatate şi/sau pentru aplicarea unor sancţiuni. (3) Agenţia efectuează controale planificate sau controale inopinate, din oficiu sau la cerere, în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activităţii de întreprinzător.		(3) Agenţia efectuează controale planificate sau controale inopinate, din oficiu sau la cerere, în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activităţii de întreprinzător. „(3)[1] 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.** Obligaţiile operatorului (1) Operatorul este obligat: a) să îndeplinească condiţiile stipulate în licenţă; b) să prezinte Agenţiei sau autorităţii administraţiei publice locale, după caz, calculele argumentate ale cheltuielilor suportate; c) să nu întrerupă furnizarea/prestarea serviciului public de alimentare cu apă și de canalizare, cu excepţia cazurilor de neplată, a motivelor tehnice şi de securitate prevăzute în lege, în licenţă și în contracte; d) să ţină contabilitatea în modul şi în condiţiile prevăzute de lege; e) să prezinte, în termenele stabilite, autorităţii administraţiei publice locale, autorităţii centrale de specialitate, precum şi Agenţiei, informaţia solicitată de acestea, să asigure accesul reprezentanţilor acestora la toate documentele ce conţin informaţii necesare pentru verificarea şi evaluarea funcţionării şi dezvoltării serviciului, să	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.”.	**Articolul 15.** Obligaţiile operatorului (1) Operatorul este obligat: a) să îndeplinească condiţiile stipulate în licenţă; b) să prezinte Agenţiei sau autorităţii administraţiei publice locale, după caz, calculele argumentate ale cheltuielilor suportate; c) să nu întrerupă furnizarea/prestarea serviciului public de alimentare cu apă şi de canalizare, cu excepţia cazurilor de neplată, a motivelor tehnice şi de securitate prevăzute în lege, în licenţă şi în contracte; d) să ţină contabilitatea în modul şi în condiţiile prevăzute de lege; e) să prezinte, în termenele stabilite, autorităţii administraţiei publice locale, autorităţii centrale de specialitate, precum şi Agenţiei, informaţia solicitată de acestea, să asigure accesul reprezentanţilor acestora la toate documentele ce conţin informaţii necesare pentru verificarea şi evaluarea funcţionării şi dezvoltării serviciului, să prezinte în termen Agenţiei şi autorităţii

	prezinte în termen Agenţiei şi autorităţii administraţiei publice locale rapoarte privind activitatea desfăşurată; f) să nu transmită altor persoane fizice sau juridice drepturi şi obligaţii aferente activităţii pe care operatorul o desfăşoară şi pentru care i s-a acordat licenţă şi s-a încheiat contract de delegare a gestiunii; g) să achite plăţile regulatorii în termenele stabilite prin lege; h) să prezinte anual spre avizare și aprobare tarifele pentru serviciul public de alimentare cu apă potabilă, pentru serviciul public de canalizare și de epurare a apelor uzate. (2) În raport cu consumatorii, operatorul are următoarele obligaţii: a) să asigure furnizarea/prestarea serviciului public de alimentare cu apă şi de canalizare tuturor consumatorilor din teritoriul în ale cărui limite a fost autorizat, cu respectarea prevederilor Regulamentului de organizare și furnizare/prestare a serviciului public de alimentare cu apă şi de canalizare și ale legislației în vigoare; b) să furnizeze serviciul public de alimentare cu apă şi de canalizare în locurile autorizate, ţinînd cont de punctele de delimitare a reţelelor şi instalaţiilor, în baza unui contract încheiat cu consumatorul, şi să respecte angajamentele contractuale; c) să asigure funcţionarea, la parametrii proiectaţi, a sistemelor publice de alimentare cu apă şi de canalizare, să respecte indicatorii de performanță a serviciului public de alimentare cu apă şi de canalizare stabiliţi de autoritatea publică locală şi să asigure		administraţiei publice locale rapoarte privind activitatea desfăşurată; f) să nu transmită altor persoane fizice sau juridice drepturi şi obligaţii aferente activităţii pe care operatorul o desfăşoară şi pentru care i s-a acordat licenţă şi s-a încheiat contract de delegare a gestiunii; g) să achite plăţile regulatorii în termenele stabilite prin lege; h) să prezinte anual spre avizare și aprobare tarifele pentru serviciul public de alimentare cu apă potabilă, pentru serviciul public de canalizare și de epurare a apelor uzate. (2) În raport cu consumatorii, operatorul are următoarele obligaţii: a) să asigure furnizarea/prestarea serviciului public de alimentare cu apă şi de canalizare tuturor consumatorilor din teritoriul în ale cărui limite a fost autorizat, cu respectarea prevederilor Regulamentului de organizare și furnizare/prestare a serviciului public de alimentare cu apă şi de canalizare și ale legislației în vigoare; b) să furnizeze serviciul public de alimentare cu apă şi de canalizare în locurile autorizate, ţinînd cont de punctele de delimitare a reţelelor şi instalaţiilor, în baza unui contract încheiat cu consumatorul, şi să respecte angajamentele contractuale; c) să asigure funcţionarea, la parametrii proiectaţi, a sistemelor publice de alimentare cu apă şi de canalizare, să respecte indicatorii de performanță a serviciului public de alimentare cu apă şi de canalizare stabiliţi de autoritatea publică locală şi să asigure continuitatea

	continuitatea serviciului respectiv la punctul de delimitare a reţelelor la parametrii fizici şi calitativi; d) să elibereze avize de racordare/branşare la reţeaua publică de apă şi de canalizare în termen de cel mult 20 de zile calendaristice din momentul de depunere a solicitării şi a prezentării documentelor necesare indicate în Regulamentul de organizare și funcționare a serviciului public de alimentare cu apă şi de canalizare; e) să informeze consumatorii, cel puţin cu 3 zile înainte, prin mass-media şi/sau prin afişare la scările blocurilor locative, despre orice întrerupere a furnizării apei şi/sau a preluării apelor uzate în cazul unor lucrări planificate de modernizare, reparaţie şi întreţinere; f) să întreprindă măsuri de remediere, în termenele stabilite prin actele normative în domeniu, a defecţiunilor produse în reţelele sale; g) să instaleze, să repare, să înlocuiască şi să verifice metrologic contoarele de apă conform prevederilor art. 26; h) să nu admită discriminarea consumatorilor, să calculeze plata pentru serviciul furnizat/prestat în baza tarifelor aprobate, a indicaţiilor contoarelor de apă, iar în lipsa acestora, pe durata verificării metrologice periodice, sau în cazul deteriorării din motive ce nu pot fi imputate consumatorului, să calculeze plata pentru volumul de apă consumată, reieşind din volumul mediu lunar, înregistrat în ultimele 3 luni pînă la verificare (deteriorare);		serviciului respectiv la punctul de delimitare a reţelelor la parametrii fizici şi calitativi; d) să elibereze avize de racordare/branşare la reţeaua publică de apă şi de canalizare în termen de cel mult 20 de zile calendaristice din momentul de depunere a solicitării şi a prezentării documentelor necesare indicate în Regulamentul de organizare și funcționare a serviciului public de alimentare cu apă şi de canalizare; e) să informeze consumatorii, cel puţin cu 3 zile înainte, prin mass-media şi/sau prin afişare la scările blocurilor locative, despre orice întrerupere a furnizării apei şi/sau a preluării apelor uzate în cazul unor lucrări planificate de modernizare, reparaţie şi întreţinere; f) să întreprindă măsuri de remediere, în termenele stabilite prin actele normative în domeniu, a defecţiunilor produse în reţelele sale; g) să instaleze, să repare, să înlocuiască şi să verifice metrologic contoarele de apă conform prevederilor art. 26; h) să nu admită discriminarea consumatorilor, să calculeze plata pentru serviciul furnizat/prestat în baza tarifelor aprobate, a indicaţiilor contoarelor de apă, iar în lipsa acestora, pe durata verificării metrologice periodice, sau în cazul deteriorării din motive ce nu pot fi imputate consumatorului, să calculeze plata pentru volumul de apă consumată, reieşind din volumul mediu lunar, înregistrat în ultimele 3 luni pînă la verificare (deteriorare); i) să informeze consumatorii cu privire la serviciul furnizat/prestat, inclusiv cu privire la eventualele riscuri, calitatea serviciului, condiţiile calitative şi cantitative de deversare a

	i) să informeze consumatorii cu privire la serviciul furnizat/prestat, inclusiv cu privire la eventualele riscuri, calitatea serviciului, condiţiile calitative şi cantitative de deversare a apelor uzate, modificările tarifului şi să prezinte, la cerere, consumatorilor informaţii cu privire la volumul de apă consumată şi referitor la eventualele penalităţi plătite de aceştia; j) să restituie consumatorilor plăţile facturate incorect şi să achite despăgubiri pentru prejudiciile cauzate din vina sa, în conformitate cu actele legislative şi cu alte acte normative în vigoare; k) să achite, în condiţiile legii, proprietarilor din vecinătatea sistemelor publice de alimentare cu apă şi de canalizare prejudiciile cauzate în rezultatul intervenţiilor de retehnologizare, reparaţie, revizie sau în caz de avarii. Proprietarul terenului afectat de exercitarea dreptului de servitute va fi despăgubit pentru prejudiciile cauzate. (3) La desfăşurarea activităţii, operatorul trebuie să respecte obligaţiile referitoare la securitatea, calitatea, eficienţa şi continuitatea furnizării serviciului public de alimentare cu apă şi de canalizare, normele de securitate şi de sănătate a muncii, normele de protecţie a mediului, precum şi prevederile contractelor încheiate cu consumatorii. (4) Operatorul este obligat să utilizeze mijloace electronice de comunicație, în măsura în care acestea sunt disponibile, funcționale și adecvate circumstanțelor, în raport cu consumatorii și potențialii		apelor uzate, modificările tarifului şi să prezinte, la cerere, consumatorilor informaţii cu privire la volumul de apă consumată şi referitor la eventualele penalităţi plătite de aceştia; j) să restituie consumatorilor plăţile facturate incorect şi să achite despăgubiri pentru prejudiciile cauzate din vina sa, în conformitate cu actele legislative şi cu alte acte normative în vigoare; k) să achite, în condiţiile legii, proprietarilor din vecinătatea sistemelor publice de alimentare cu apă şi de canalizare prejudiciile cauzate în rezultatul intervenţiilor de retehnologizare, reparaţie, revizie sau în caz de avarii. Proprietarul terenului afectat de exercitarea dreptului de servitute va fi despăgubit pentru prejudiciile cauzate. (3) La desfăşurarea activităţii, operatorul trebuie să respecte obligaţiile referitoare la securitatea, calitatea, eficienţa şi continuitatea furnizării serviciului public de alimentare cu apă şi de canalizare, normele de securitate şi de sănătate a muncii, normele de protecţie a mediului, precum şi prevederile contractelor încheiate cu consumatorii. (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.

	consumatori, în procesul de comunicare, de soluționare a petițiilor, de negociere, încheiere, executare, modificare și încetare a contractelor. Operatorul nu poate refuza sau ignora examinarea cererilor, reclamațiilor și sesizărilor din motiv că au fost depuse în formă electronică, dacă acestea întrunesc cerințele prevăzute de legislația ce reglementează documentele electronice.		(4) Operatorul este obligat să utilizeze mijloace electronice de comunicație, în măsura în care acestea sunt disponibile, funcționale și adecvate circumstanțelor, în raport cu consumatorii și potențialii consumatori, în procesul de comunicare, de soluționare a petițiilor, de negociere, încheiere, executare, modificare și încetare a contractelor. Operatorul nu poate refuza sau ignora examinarea cererilor, reclamațiilor și sesizărilor din motiv că au fost depuse în formă electronică, dacă acestea întrunesc cerințele prevăzute de legislația ce reglementează documentele electronice.
Articolul 14 din Legea comunicațiilor poștale nr. 36/2016			
1.	**Articolul 14.** Responsabilitatea furnizorilor de servicii poştale (1) Furnizorii de servicii poştale sînt responsabili faţă de utilizatori pentru: a) furnizarea serviciilor în condiţiile prevăzute de lege şi de contractul încheiat cu expeditorul; b) paguba care rezultă din pierderea ori deteriorarea totală sau parţială a trimiterii poştale survenită din momentul depunerii acesteia la oficiul poştal sau la punctul de acces şi pînă la livrarea către destinatar. (1^1) Furnizorii de servicii poștale sunt responsabili pentru utilizarea datelor cu caracter personal ale utilizatorilor. Datele cu caracter personal se utilizează numai în scopul pentru care au fost acumulate. Accesul la datele cu caracter personal se realizează în condițiile Legii nr. 133/2011 privind protecția	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 legea respectivă, 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.” .	**Articolul 14.** Responsabilitatea furnizorilor de servicii poştale (1) Furnizorii de servicii poştale sînt responsabili faţă de utilizatori pentru: a) furnizarea serviciilor în condiţiile prevăzute de lege şi de contractul încheiat cu expeditorul; b) paguba care rezultă din pierderea ori deteriorarea totală sau parţială a trimiterii poştale survenită din momentul depunerii acesteia la oficiul poştal sau la punctul de acces şi pînă la livrarea către destinatar. (1^1) Furnizorii de servicii poștale sunt responsabili pentru utilizarea datelor cu caracter personal ale utilizatorilor. Datele cu caracter personal se utilizează numai în scopul pentru care au fost acumulate. Accesul la datele cu caracter personal se realizează în condițiile Legii nr. 133/2011 privind protecția datelor cu caracter personal. Fără a aduce atingere

	datelor cu caracter personal. Fără a aduce atingere prevederilor prezentului alineat, furnizorul de serviciu poștal universal transferă în mod electronic date cu caracter personal operatorilor desemnați ai țărilor de destinație sau de tranzit, care au nevoie de aceste date pentru a asigura serviciul lor. (2) Pierderile indirecte, beneficiile nerealizate sau daunele morale nu vor fi luate în considerare la calcularea despăgubirii ce urmează a fi plătită de către furnizorii de servicii poştale. (3) Furnizorul de serviciu poştal universal este responsabil pentru trimiterile poştale internaţionale în conformitate cu prevederile tratatelor internaţionale la care Republica Moldova este parte, inclusiv cu obligaţiile care rezultă din actele Uniunii Poştale Universale şi prezenta lege. (4) Furnizorul de serviciu poştal universal poartă răspundere pentru trimiterile poştale interne şi acordă despăgubiri din mijloacele proprii după cum urmează: 1) în caz de pierdere totală, furt total sau deteriorare totală: a) în mărimea sumei ce constituie 5 tarife de recomandare – pentru o trimitere poştală care face obiectul serviciului de trimitere recomandată; b) în mărimea sumei tarifului plătit – pentru o trimitere poştală care face obiectul serviciului de trimitere cu predare atestată;		prevederilor prezentului alineat, furnizorul de serviciu poștal universal transferă în mod electronic date cu caracter personal operatorilor desemnați ai țărilor de destinație sau de tranzit, care au nevoie de aceste date pentru a asigura serviciul lor. (2) Pierderile indirecte, beneficiile nerealizate sau daunele morale nu vor fi luate în considerare la calcularea despăgubirii ce urmează a fi plătită de către furnizorii de servicii poştale. (3) Furnizorul de serviciu poştal universal este responsabil pentru trimiterile poştale internaţionale în conformitate cu prevederile tratatelor internaţionale la care Republica Moldova este parte, inclusiv cu obligaţiile care rezultă din actele Uniunii Poştale Universale şi prezenta lege. (4) Furnizorul de serviciu poştal universal poartă răspundere pentru trimiterile poştale interne şi acordă despăgubiri din mijloacele proprii după cum urmează: 1) în caz de pierdere totală, furt total sau deteriorare totală: a) în mărimea sumei ce constituie 5 tarife de recomandare – pentru o trimitere poştală care face obiectul serviciului de trimitere recomandată; b) în mărimea sumei tarifului plătit – pentru o trimitere poştală care face obiectul serviciului de trimitere cu predare atestată; c) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată;

	c) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; d) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, pînă la momentul livrării la destinatar; e) în mărimea valorii rambursului – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, după livrarea acesteia destinatarului, cînd furnizorul de servicii poştale a omis încasarea rambursului de la destinatar; f) în mărimea sumei ce constituie 5 tarife – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată, indiferent de greutate; 2) în caz de pierdere parțială, furt parțial sau deteriorare parţială: a) în mărimea valorii declarate pentru partea lipsă sau pentru partea deteriorată, înscrisă de expeditor în nota de inventar – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; b) în mărimea cotei-părţi corespunzătoare greutăţii lipsă din valoarea declarată – pentru o trimitere poştală depusă fără notă de inventar, care face obiectul serviciului de trimitere cu valoare declarată; c) în mărimea cotei-părţi din suma ce constituie 5 tarife, stabilită în raport cu greutatea lipsă sau cu greutatea conţinutului deteriorat – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată; 3) în caz de nerespectare a termenelor de distribuire – în mărimea sumei ce constituie		d) în mărimea valorii declarate – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, pînă la momentul livrării la destinatar; e) în mărimea valorii rambursului – pentru o trimitere poştală care face obiectul serviciului de trimitere contra ramburs, după livrarea acesteia destinatarului, cînd furnizorul de servicii poştale a omis încasarea rambursului de la destinatar; f) în mărimea sumei ce constituie 5 tarife – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată, indiferent de greutate; 2) în caz de pierdere parțială, furt parțial sau deteriorare parţială: a) în mărimea valorii declarate pentru partea lipsă sau pentru partea deteriorată, înscrisă de expeditor în nota de inventar – pentru o trimitere poştală care face obiectul serviciului de trimitere cu valoare declarată; b) în mărimea cotei-părţi corespunzătoare greutăţii lipsă din valoarea declarată – pentru o trimitere poştală depusă fără notă de inventar, care face obiectul serviciului de trimitere cu valoare declarată; c) în mărimea cotei-părţi din suma ce constituie 5 tarife, stabilită în raport cu greutatea lipsă sau cu greutatea conţinutului deteriorat – pentru un colet poştal care nu face obiectul serviciului de trimitere cu valoare declarată; 3) în caz de nerespectare a termenelor de distribuire – în mărimea sumei ce constituie 5% din suma tarifului de expediere – pentru fiecare zi de întîrziere, însă nu mai mult de suma totală a tarifului de expediere.

	5% din suma tarifului de expediere – pentru fiecare zi de întîrziere, însă nu mai mult de suma totală a tarifului de expediere. (5) Pe lîngă despăgubirile prevăzute la alin. (4) pct. 1), se restituie şi tarifele încasate la depunerea trimiterii poştale la oficiul poştal, cu excepţia taxelor de recomandare şi de asigurare. (6) Furnizorul de servicii poştale poartă răspundere pentru prestarea necorespunzătoare a serviciilor de plăţi poştale şi acordă despăgubiri din mijloacele proprii după cum urmează: a) în caz de neplată a mandatului poştal, a sumelor referitoare la serviciile aferente transferurilor de mijloace băneşti şi a sumelor referitoare la serviciul de intermediere a transferurilor de mijloace băneşti – în mărimea sumei depuse; b) în caz de netransferare a mijloacelor băneşti pe contul bancar al destinatarului – în mărimea sumei viramentului netransferat. (7) Furnizorul de servicii poştale poartă răspundere, conform contractelor încheiate cu utilizatorii, pentru pierderea, deteriorarea, lipsa conţinutului, nelivrarea sau încălcarea termenului de livrare a trimiterilor poştale. (7[1]) Furnizorul de serviciu poștal universal rămâne responsabil dacă destinatarul sau, în caz de retur la origine, expeditorul unui colet sau al unei trimiteri cu valoare declarată anunță furnizorul de serviciu poștal universal care i-a înmânat trimiterea că a constatat un		(5) Pe lîngă despăgubirile prevăzute la alin. (4) pct. 1), se restituie şi tarifele încasate la depunerea trimiterii poştale la oficiul poştal, cu excepţia taxelor de recomandare şi de asigurare. (6) Furnizorul de servicii poştale poartă răspundere pentru prestarea necorespunzătoare a serviciilor de plăţi poştale şi acordă despăgubiri din mijloacele proprii după cum urmează: a) în caz de neplată a mandatului poştal, a sumelor referitoare la serviciile aferente transferurilor de mijloace băneşti şi a sumelor referitoare la serviciul de intermediere a transferurilor de mijloace băneşti – în mărimea sumei depuse; b) în caz de netransferare a mijloacelor băneşti pe contul bancar al destinatarului – în mărimea sumei viramentului netransferat. (7) Furnizorul de servicii poştale poartă răspundere, conform contractelor încheiate cu utilizatorii, pentru pierderea, deteriorarea, lipsa conţinutului, nelivrarea sau încălcarea termenului de livrare a trimiterilor poştale. (7[1]) Furnizorul de serviciu poștal universal rămâne responsabil dacă destinatarul sau, în caz de retur la origine, expeditorul unui colet sau al unei trimiteri cu valoare declarată anunță furnizorul de serviciu poștal universal care i-a înmânat trimiterea că a constatat un prejudiciu, cu condiția că destinatarul sau, după caz, expeditorul nu s-a deplasat de la ghișeul oficiului poștal care i-a înmânat trimiterea poștală.

	prejudiciu, cu condiția că destinatarul sau, după caz, expeditorul nu s-a deplasat de la ghișeul oficiului poștal care i-a înmânat trimiterea poștală. (8) Furnizorul de servicii poştale nu poartă răspundere pentru trimiterile poştale în cazul în care paguba a fost cauzată din vina expeditorului ori ca urmare a circumstanţelor de forţă majoră sau a situaţiilor excepţionale, precum şi pentru trimiterile poştale care au fost primite fără obiecţii de către destinatar.		(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 legea respectivă, 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. (8) Furnizorul de servicii poştale nu poartă răspundere pentru trimiterile poştale în cazul în care paguba a fost cauzată din vina expeditorului ori ca urmare a circumstanţelor de forţă majoră sau a situaţiilor excepţionale, precum şi pentru trimiterile poştale care au fost primite fără obiecţii de către destinatar.
Legea nr. 209/2016 privind deşeurile			
1.	**Articolul 18.** Obligaţiile gestionarilor de deşeuri (1) Responsabilitatea pentru gestionarea deşeurilor revine după cum urmează: a) producătorul inițial sau alt deținător de deşeuri are obligaţia să asigure efectuarea operațiunii de tratare a deşeurilor prin mijloace proprii sau prin transferarea	Articolul 18 se completează cu alineatul (5)[1] cu următorul cuprins: „(5)[1] 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 legea respectivă, de actele	**Articolul 18.** Obligaţiile gestionarilor de deşeuri (1) Responsabilitatea pentru gestionarea deşeurilor revine după cum urmează: a) producătorul inițial sau alt deținător de deşeuri are obligaţia să asigure efectuarea operațiunii de tratare a deşeurilor prin mijloace proprii sau prin transferarea deșeurilor în

	deşeurilor în vederea efectuării acestei operaţiuni unui agent, unei unităţi sau întreprinderi care desfăşoară activităţi de tratare a deşeurilor ori unei unităţi publice sau private de colectare a deşeurilor, cu respectarea art. 3 şi 4; b) producătorii şi deţinătorii de deşeuri îşi organizează sistemul propriu de tratare/eliminare a deşeurilor dacă deşeurile nu pot fi preluate de unităţi specializate din sistemul organizat în acest scop, cu respectarea art. 4. Livrarea şi primirea deşeurilor, inclusiv a deşeurilor periculoase, în vederea eliminării lor se fac numai în bază de contract. (2) Atunci cînd deșeurile sînt transferate de la producătorul sau deţinătorul iniţial către un agent, către o unitate sau o întreprindere menţionată la alin. (1) lit. a) în vederea efectuării unor operaţiuni de tratare preliminară, acesta nu este scutit, de regulă, de responsabilitatea pentru realizarea operaţiunilor de valorificare sau de eliminare completă. (3) Ținînd cont de prevederile, procedurile şi regimurile de control pentru transferul de deşeuri, în funcţie de originea, destinaţia şi itinerarul transferului, de tipul de deşeu transferat şi de tipul de tratament care se aplică deşeului la destinaţie, în contractul menționat la alin. (1) se vor preciza condiţiile cu privire la responsabilitate, îndeosebi în cazurile în care producătorului iniţial îi revine responsabilitatea pentru întregul lanţ al procesului de tratare sau în cazurile în care	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.”;	vederea efectuării acestei operaţiuni unui agent, unei unităţi sau întreprinderi care desfăşoară activităţi de tratare a deşeurilor ori unei unităţi publice sau private de colectare a deşeurilor, cu respectarea art. 3 şi 4; b) producătorii şi deţinătorii de deşeuri îşi organizează sistemul propriu de tratare/eliminare a deşeurilor dacă deşeurile nu pot fi preluate de unităţi specializate din sistemul organizat în acest scop, cu respectarea art. 4. Livrarea şi primirea deşeurilor, inclusiv a deşeurilor periculoase, în vederea eliminării lor se fac numai în bază de contract. (2) Atunci cînd deșeurile sînt transferate de la producătorul sau deţinătorul iniţial către un agent, către o unitate sau o întreprindere menţionată la alin. (1) lit. a) în vederea efectuării unor operaţiuni de tratare preliminară, acesta nu este scutit, de regulă, de responsabilitatea pentru realizarea operaţiunilor de valorificare sau de eliminare completă. (3) Ținînd cont de prevederile, procedurile şi regimurile de control pentru transferul de deşeuri, în funcţie de originea, destinaţia şi itinerarul transferului, de tipul de deşeu transferat şi de tipul de tratament care se aplică deşeului la destinaţie, în contractul menționat la alin. (1) se vor preciza condiţiile cu privire la responsabilitate, îndeosebi în cazurile în care producătorului iniţial îi revine responsabilitatea pentru întregul lanţ al procesului de tratare sau în cazurile în care responsabilitatea producătorului şi a deţinătorului se poate împărţi

	responsabilitatea producătorului şi a deţinătorului se poate împărţi sau delega între actorii din lanţul procesului de tratare. (4) Prin actele normative aprobate de Guvern în vederea implementării prezentei legi se va stabili, în conformitate cu art. 14, dacă responsabilitatea cu privire la organizarea activităţilor de gestionare a anumitor deşeuri revine, parţial sau în totalitate, producătorului produsului din care derivă deşeul respectiv şi dacă distribuitorii respectivului produs trebuie să împartă această responsabilitate. (5) Unitățile și întreprinderile specializate în colectarea sau transportul de deșeuri livrează deşeurile colectate la instalaţiile de tratare, respectînd prevederile art. 4 şi ale cap. VI.		sau delega între actorii din lanţul procesului de tratare. (4) Prin actele normative aprobate de Guvern în vederea implementării prezentei legi se va stabili, în conformitate cu art. 14, dacă responsabilitatea cu privire la organizarea activităţilor de gestionare a anumitor deşeuri revine, parţial sau în totalitate, producătorului produsului din care derivă deşeul respectiv şi dacă distribuitorii respectivului produs trebuie să împartă această responsabilitate. (5) Unitățile și întreprinderile specializate în colectarea sau transportul de deșeuri livrează deşeurile colectate la instalaţiile de tratare, respectînd prevederile art. 4 şi ale cap. VI. (5)[1] 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 legea respectivă, 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.** Competenţele privind activităţile de control în domeniul gestionării deşeurilor (1) Autorităţile teritoriale de mediu inspectează și iau măsuri pentru respectarea de către cei implicaţi în gestionarea deşeurilor	Articolul 31 se completează cu alineatul (4)[1], cu următorul cuprins: „(4)[1] Supravegherea și controlul de stat al modului în care persoanele juridice care desfășoară activități de gestionare a deșeurilor realizează	**Articolul 31.** Competenţele privind activităţile de control în domeniul gestionării deşeurilor (1) Autorităţile teritoriale de mediu inspectează şi iau măsuri pentru respectarea de către cei implicaţi în gestionarea deşeurilor a legislației de mediu și a condițiilor de autorizare stabilite conform legii.

	a legislației de mediu și a condițiilor de autorizare stabilite conform legii. (2) Autorităţile teritoriale pentru sănătate publică exercită monitorizarea departamentală a cerinţelor de gestionare a deşeurilor rezultate din activităţile medicale. (4) Autorităţile vamale şi reprezentanții Inspectoratului pentru Protecția Mediului și ai subdiviziunilor teritoriale ale acestuia controlează încărcăturile şi iau măsuri pentru asigurarea conformităţii cu documentele însoţitoare şi pentru respectarea prevederilor legale referitoare la îndeplinirea condițiilor de export, import și tranzit ale deşeurilor.	obligațiile stabilite la art. 18 alin. (5)[1] se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică”.	(2) Autorităţile teritoriale pentru sănătate publică exercită monitorizarea departamentală a cerinţelor de gestionare a deşeurilor rezultate din activităţile medicale. (4) Autorităţile vamale şi reprezentanții Inspectoratului pentru Protecția Mediului și ai subdiviziunilor teritoriale ale acestuia controlează încărcăturile şi iau măsuri pentru asigurarea conformităţii cu documentele însoţitoare şi pentru respectarea prevederilor legale referitoare la îndeplinirea condițiilor de export, import și tranzit ale deşeurilor. (4)[1] 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. (5)[1] se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.
Articolul 16 din Legea nr. 102/2017 cu privire la dispozitivele medicale			
1.	**Articolul 16.** Vigilența dispozitivelor medicale (1) Producătorii de dispozitive medicale, reprezentanții acestora, persoanele juridice ce comercializează dispozitivele medicale, importatorii cu sediul înregistrat în Republica Moldova și utilizatorii de dispozitive medicale sînt obligați: a) să stabilească și să mențină un sistem propriu de vigilență a dispozitivelor medicale, care să asigure colectarea, evaluarea și	Se completează cu alineatele (3)[1] și (3)[2], cu următorul cuprins: „(3)[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	**Articolul 16.** Vigilența dispozitivelor medicale (1) Producătorii de dispozitive medicale, reprezentanții acestora, persoanele juridice ce comercializează dispozitivele medicale, importatorii cu sediul înregistrat în Republica Moldova și utilizatorii de dispozitive medicale sînt obligați: a) să stabilească și să mențină un sistem propriu de vigilență a dispozitivelor medicale, care să asigure colectarea, evaluarea și schimbul de date cu privire la complicațiile legate de dispozitivele

	schimbul de date cu privire la complicațiile legate de dispozitivele medicale sau cu privire la incidentele cu implicarea acestora, și să colaboreze în acest sens cu Agenția; b) în termen de 2 zile lucrătoare, să informeze Agenția despre orice complicație sau incident de care sînt conștienți. (2) Agenţia în colaborare cu producătorul evaluează, după caz, nivelul de risc al unui incident sau al unei complicații raportate. După efectuarea investigației, Agenția informează părțile interesate – autoritatea publică centrală, organismul recunoscut, producătorul, consumatorul și/sau utilizatorul – despre complicațiile sau incidentele pentru care s-au luat sau trebuie să se ia măsurile corespunzătoare, inclusiv retragerea dispozitivului de pe piață. (3) Reglementarea sistemului de vigilență a dispozitivelor medicale este aprobată prin act normativ departamental, în care se stabilesc condițiile de funcționare integrală și conținutul detaliat al raportării complicaţiilor sau incidentelor cu implicarea dispozitivelor medicale.	stabilesc cerințe specifice de securitate a rețelelor și sistemelor informatice. (3)[2] Supravegherea și controlul de stat al respectării de către producătorii de dispozitive medicale a obligațiilor stabilite la alin. (3)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”.	medicale sau cu privire la incidentele cu implicarea acestora, și să colaboreze în acest sens cu Agenția; b) în termen de 2 zile lucrătoare, să informeze Agenția despre orice complicație sau incident de care sînt conștienți. (2) Agenţia în colaborare cu producătorul evaluează, după caz, nivelul de risc al unui incident sau al unei complicații raportate. După efectuarea investigației, Agenția informează părțile interesate – autoritatea publică centrală, organismul recunoscut, producătorul, consumatorul și/sau utilizatorul – despre complicațiile sau incidentele pentru care s-au luat sau trebuie să se ia măsurile corespunzătoare, inclusiv retragerea dispozitivului de pe piață. (3) Reglementarea sistemului de vigilență a dispozitivelor medicale este aprobată prin act normativ departamental, în care se stabilesc condițiile de funcționare integrală și conținutul detaliat al raportării complicaţiilor sau incidentelor cu implicarea dispozitivelor medicale. (3)[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. (3)[2] Supravegherea și controlul de stat al respectării de către producătorii de dispozitive medicale a obligațiilor stabilite la alin. (3)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”.
Legea nr. 120/2017 cu privire la prevenirea și combaterea terorismului			
1.	**Articolul 3.** Noţiuni principale În sensul prezentei legi, următoarele noţiuni principale semnifică: *act terorist* – infracţiune prevăzută la art. 278 din Codul penal al Republicii Moldova; *activitate teroristă (activități teroriste)* – activități care includ: – planificarea, pregătirea, tentativa de săvîrşire şi săvîrşirea unui act terorist sau a unei alte fapte ce constituie infracţiune cu caracter terorist; – constituirea unei formaţiuni armate ilegale, a unei organizaţii criminale, a unui grup organizat în scopul săvîrşirii uneia sau mai multor infracţiuni cu caracter terorist; – recrutarea, favorizarea, înarmarea, instruirea şi utilizarea teroriştilor; – ralierea la organizaţiile teroriste sau participarea la activitatea acestor organizaţii; – finanţarea pregătirii sau comiterii unui act terorist ori a unei alte infracţiuni cu caracter terorist, finanţarea unei organizaţii	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, 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	**Articolul 3.** Noţiuni principale În sensul prezentei legi, următoarele noţiuni principale semnifică: *act terorist* – infracţiune prevăzută la art. 278 din Codul penal al Republicii Moldova; *activitate teroristă (activități teroriste)* – activități care includ: – planificarea, pregătirea, tentativa de săvîrşire şi săvîrşirea unui act terorist sau a unei alte fapte ce constituie infracţiune cu caracter terorist; – constituirea unei formaţiuni armate ilegale, a unei organizaţii criminale, a unui grup organizat în scopul săvîrşirii uneia sau mai multor infracţiuni cu caracter terorist; – recrutarea, favorizarea, înarmarea, instruirea şi utilizarea teroriştilor; – ralierea la organizaţiile teroriste sau participarea la activitatea acestor organizaţii; – finanţarea pregătirii sau comiterii unui act terorist ori a unei alte infracţiuni cu caracter terorist, finanţarea unei organizaţii teroriste, a unui grup terorist sau a unui terorist, precum şi

	teroriste, a unui grup terorist sau a unui terorist, precum şi acordarea de sprijin acestora pe alte căi; – acordarea de suport informaţional sau de alt ordin în procesul planificării, pregătirii sau comiterii unui act terorist ori a unei alte fapte ce constituie infracţiune cu caracter terorist; – instigarea în scop terorist, justificarea publică a terorismului, propaganda ideilor terorismului, răspîndirea de materiale sau informaţii ce îndeamnă la activităţi teroriste sau îndreptăţesc desfăşurarea unor astfel de activităţi; – oricare dintre acţiunile menţionate efectuate prin intermediul sistemelor informaţionale şi al reţelelor de comunicaţii electronice; – orice alte fapte ce constituie infracţiuni cu caracter terorist; *activitate teroristă internaţională* – activități teroriste înfăptuite: – de un terorist, de un grup terorist sau de o organizaţie teroristă pe teritoriul a două sau mai multor state, aducînd prejudicii intereselor acestor state şi/sau unor organizaţii internaţionale; – de cetăţenii unui stat împotriva cetăţenilor unui alt stat sau pe teritoriul unui alt stat; – în cazul în care atît teroristul, cît şi victima terorismului sînt cetăţeni ai aceluiaşi stat sau ai unor state diferite, dar infracţiunea a fost săvîrşită în afara teritoriilor acestor state; *combaterea terorismului* – măsuri şi acţiuni ofensive întreprinse de autorităţile	au în gestiunea lor obiective incluse în Nomenclatorul național al infrastructurii critice;”.	acordarea de sprijin acestora pe alte căi; – acordarea de suport informaţional sau de alt ordin în procesul planificării, pregătirii sau comiterii unui act terorist ori a unei alte fapte ce constituie infracţiune cu caracter terorist; – instigarea în scop terorist, justificarea publică a terorismului, propaganda ideilor terorismului, răspîndirea de materiale sau informaţii ce îndeamnă la activităţi teroriste sau îndreptăţesc desfăşurarea unor astfel de activităţi; – oricare dintre acţiunile menţionate efectuate prin intermediul sistemelor informaţionale şi al reţelelor de comunicaţii electronice; – orice alte fapte ce constituie infracţiuni cu caracter terorist; *activitate teroristă internaţională* – activități teroriste înfăptuite: – de un terorist, de un grup terorist sau de o organizaţie teroristă pe teritoriul a două sau mai multor state, aducînd prejudicii intereselor acestor state şi/sau unor organizaţii internaţionale; – de cetăţenii unui stat împotriva cetăţenilor unui alt stat sau pe teritoriul unui alt stat; – în cazul în care atît teroristul, cît şi victima terorismului sînt cetăţeni ai aceluiaşi stat sau ai unor state diferite, dar infracţiunea a fost săvîrşită în afara teritoriilor acestor state; *combaterea terorismului* – măsuri şi acţiuni ofensive întreprinse de autorităţile competente în scopul descoperirii şi curmării activităţilor teroriste şi al atenuării urmărilor acestora;

	competente în scopul descoperirii şi curmării activităţilor teroriste şi al atenuării urmărilor acestora; *criză teroristă* – situaţie creată în timpul sau ca urmare a unui act terorist sau a unei alte fapte ce constituie infracţiune cu caracter terorist, prin care se creează un pericol iminent pentru viaţa şi securitatea cetăţenilor, pentru interesele societăţii sau ale statului; *exerciţiu antiterorist* – complex de măsuri specifice, teoretice şi practice, desfăşurate de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul instruirii forţelor operaţionale, determinării eficienţei măsurilor de prevenire şi combatere a activităţilor teroriste, a nivelului de pregătire a Comandamentului Operaţional Antiterorist în rezolvarea practică a unor situaţii de criză teroristă simulate; *grup terorist* – două sau mai multe persoane care s-au asociat în scopul de a desfăşura o activitate teroristă; *infracţiune cu caracter terorist* – una din infracţiunile prevăzute la art.134[11] din Codul penal al Republicii Moldova; *infrastructură critică* – element, sistem sau o componentă a acestuia, aflat pe teritoriul Republicii Moldova, care este esenţial pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, a siguranţei, a securităţii și a bunăstării sociale şi economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii; *intervenţie contrateroristă* – complex		*criză teroristă* – situaţie creată în timpul sau ca urmare a unui act terorist sau a unei alte fapte ce constituie infracţiune cu caracter terorist, prin care se creează un pericol iminent pentru viaţa şi securitatea cetăţenilor, pentru interesele societăţii sau ale statului; *exerciţiu antiterorist* – complex de măsuri specifice, teoretice şi practice, desfăşurate de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul instruirii forţelor operaţionale, determinării eficienţei măsurilor de prevenire şi combatere a activităţilor teroriste, a nivelului de pregătire a Comandamentului Operaţional Antiterorist în rezolvarea practică a unor situaţii de criză teroristă simulate; *grup terorist* – două sau mai multe persoane care s-au asociat în scopul de a desfăşura o activitate teroristă; *infracţiune cu caracter terorist* – una din infracţiunile prevăzute la art.134[11] din Codul penal al Republicii Moldova; *infrastructură critică* – element, sistem sau o componentă a acestuia, aflat pe teritoriul Republicii Moldova, care este esenţial pentru menţinerea funcţiilor vitale ale societăţii, a sănătăţii, a siguranţei, a securităţii și a bunăstării sociale şi economice a persoanelor şi a cărui perturbare sau distrugere ar avea un impact semnificativ la nivel naţional ca urmare a incapacităţii de a menţine respectivele funcţii; *intervenţie contrateroristă* – complex de măsuri ofensive realizate în cadrul unei operaţii antiteroriste, în scopul capturării sau anihilării teroriştilor şi/sau eliberării ostaticilor, în cazul în care metodele defensive de înlăturare a pericolului terorist nu au atins rezultatul scontat;

	de măsuri ofensive realizate în cadrul unei operaţii antiteroriste, în scopul capturării sau anihilării teroriştilor şi/sau eliberării ostaticilor, în cazul în care metodele defensive de înlăturare a pericolului terorist nu au atins rezultatul scontat; *luare de ostatici* – luarea sau reţinerea unei/unor persoane în calitate de ostatic/ostatici şi ameninţarea cu omorul, cu vătămarea integrităţii corporale sau a sănătăţii acesteia/acestora ori cu reţinerea în continuare a persoanei/persoanelor în această calitate cu scopul de a sili statul, organizaţia internaţională, persoana juridică sau fizică ori un grup de persoane să săvîrşească sau să se abţină de la săvîrşirea vreunei acţiuni în calitate de condiţie pentru eliberarea ostaticului; *operaţie antiteroristă* – ansamblu de măsuri planificate şi coordonate, întreprinse de către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul curmării activităţii teroriste, eliberării ostaticilor şi dirijării acţiunilor urgente de răspuns la survenirea unei crize teroriste; *organizaţie teroristă* – organizaţie creată în scopul desfăşurării de activităţi teroriste sau organizaţie care admite recurgerea la terorism în activitatea sa. Organizaţia se consideră teroristă dacă măcar una din subdiviziunile sale structurale desfăşoară o activitate teroristă; *paşaport antiterorist* – document complex ce cuprinde informaţii despre starea şi nivelul de protecţie, eventualele pericole şi ameninţări cu tentă teroristă la adresa obiectivelor din infrastructura critică în cazul		*luare de ostatici* – luarea sau reţinerea unei/unor persoane în calitate de ostatic/ostatici şi ameninţarea cu omorul, cu vătămarea integrităţii corporale sau a sănătăţii acesteia/acestora ori cu reţinerea în continuare a persoanei/persoanelor în această calitate cu scopul de a sili statul, organizaţia internaţională, persoana juridică sau fizică ori un grup de persoane să săvîrşească sau să se abţină de la săvîrşirea vreunei acţiuni în calitate de condiţie pentru eliberarea ostaticului; *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, 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; *operaţie antiteroristă* – ansamblu de măsuri planificate şi coordonate, întreprinse de

	unor eventuale acte teroriste sau al altor infracţiuni cu caracter terorist pe teritoriul Republicii Moldova. Modelul paşaportului antiterorist se aprobă prin ordin al directorului Serviciului de Informaţii şi Securitate al Republicii Moldova; *prevenirea terorismului* – ansamblu de măsuri specifice cu caracter permanent, întreprinse cu anticipaţie de către autorităţile abilitate prin lege cu atribuţii de prevenire a terorismului, bazate pe acţiuni informative, educative, organizatorice, de pază, de protecţie, de informare şi relaţii publice, de optimizare a cadrului legislativ, de cooperare naţională şi internaţională în scopul identificării şi înlăturării factorilor de risc şi a ameninţărilor cu tentă teroristă; *protecţia antiteroristă a infrastructurii critice* – ansamblu de măsuri de ordin juridic, organizatoric, economico-financiar, ingineresc, de regim, de ordin operativ, informativ, contrainformativ etc., întreprinse de către autorităţile administraţiei publice, de alte organizaţii şi întreprinderi din cadrul infrastructurii critice, precum şi de către alte subdiviziuni sau de persoane special împuternicite de către acestea, care au drept scop asigurarea funcţionalităţii, continuităţii şi integrităţii infrastructurii critice, pentru a descuraja, diminua şi neutraliza o ameninţare, un risc sau un punct vulnerabil; *terorism* – fenomen cu un grad înalt de pericol social, caracterizat printr-o ideologie radicală şi o practică de influenţare prin violenţă a luării unor decizii de către autorităţi şi instituţii publice sau organizaţii internaţionale, însoţite de intimidarea		către autorităţile cu atribuţii în domeniul prevenirii şi combaterii terorismului în scopul curmării activităţii teroriste, eliberării ostaticilor şi dirijării acţiunilor urgente de răspuns la survenirea unei crize teroriste; *organizaţie teroristă* – organizaţie creată în scopul desfăşurării de activităţi teroriste sau organizaţie care admite recurgerea la terorism în activitatea sa. Organizaţia se consideră teroristă dacă măcar una din subdiviziunile sale structurale desfăşoară o activitate teroristă; *paşaport antiterorist* – document complex ce cuprinde informaţii despre starea şi nivelul de protecţie, eventualele pericole şi ameninţări cu tentă teroristă la adresa obiectivelor din infrastructura critică în cazul unor eventuale acte teroriste sau al altor infracţiuni cu caracter terorist pe teritoriul Republicii Moldova. Modelul paşaportului antiterorist se aprobă prin ordin al directorului Serviciului de Informaţii şi Securitate al Republicii Moldova; *prevenirea terorismului* – ansamblu de măsuri specifice cu caracter permanent, întreprinse cu anticipaţie de către autorităţile abilitate prin lege cu atribuţii de prevenire a terorismului, bazate pe acţiuni informative, educative, organizatorice, de pază, de protecţie, de informare şi relaţii publice, de optimizare a cadrului legislativ, de cooperare naţională şi internaţională în scopul identificării şi înlăturării factorilor de risc şi a ameninţărilor cu tentă teroristă; *protecţia antiteroristă a infrastructurii critice* – ansamblu de măsuri de ordin juridic, organizatoric, economico-financiar, ingineresc, de regim, de ordin operativ, informativ,

	populaţiei şi/sau de alte acţiuni violente ilegale; *terorist* – persoană implicată sub orice formă într-o activitate teroristă; *test antiterorist* – complex de măsuri cu caracter public şi/sau secret, realizate de Serviciul de Informaţii şi Securitate al Republicii Moldova în scopul verificării şi evaluării eficienţei sistemului şi mecanismului de protecţie antiteroristă; *zonă de desfăşurare a operaţiei antiteroriste* – construcţie, mijloc de transport sau teritoriu/spaţiu geografic în limitele căruia se desfăşoară o operaţie antiteroristă şi se introduce un regim juridic special; *zonă de risc* – stat sau regiune vulnerabilă sub aspectul securităţii ca urmare a conflictelor armate derulate sau a activităţii teroriste desfăşurate în acea zonă de către organizaţii sau entităţi recunoscute drept teroriste/paramilitare de către organizațiile internaţionale ori regionale la care Republica Moldova este parte. Statele sau regiunile care constituie zone de risc urmează a fi desemnate prin hotărîre a Parlamentului.		contrainformativ etc., întreprinse de către autorităţile administraţiei publice, de alte organizaţii şi întreprinderi din cadrul infrastructurii critice, precum şi de către alte subdiviziuni sau de persoane special împuternicite de către acestea, care au drept scop asigurarea funcţionalităţii, continuităţii şi integrităţii infrastructurii critice, pentru a descuraja, diminua şi neutraliza o ameninţare, un risc sau un punct vulnerabil; *terorism* – fenomen cu un grad înalt de pericol social, caracterizat printr-o ideologie radicală şi o practică de influenţare prin violenţă a luării unor decizii de către autorităţi şi instituţii publice sau organizaţii internaţionale, însoţite de intimidarea populaţiei şi/sau de alte acţiuni violente ilegale; *terorist* – persoană implicată sub orice formă într-o activitate teroristă; *test antiterorist* – complex de măsuri cu caracter public şi/sau secret, realizate de Serviciul de Informaţii şi Securitate al Republicii Moldova în scopul verificării şi evaluării eficienţei sistemului şi mecanismului de protecţie antiteroristă; *zonă de desfăşurare a operaţiei antiteroriste* – construcţie, mijloc de transport sau teritoriu/spaţiu geografic în limitele căruia se desfăşoară o operaţie antiteroristă şi se introduce un regim juridic special; *zonă de risc* – stat sau regiune vulnerabilă sub aspectul securităţii ca urmare a conflictelor armate derulate sau a activităţii teroriste desfăşurate în acea zonă de către organizaţii sau entităţi recunoscute drept teroriste/paramilitare de către organizațiile internaţionale ori regionale la care Republica

			Moldova este parte. Statele sau regiunile care constituie zone de risc urmează a fi desemnate prin hotărîre a Parlamentului.
2.	**Articolul 20.** Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice (1) Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice are drept scop: a) verificarea nivelului de pregătire a personalului în ceea ce privește asigurarea protecţiei antiteroriste; b) determinarea capacităţii de pază şi protecţie a obiectivelor infrastructurii critice; c) identificarea vulnerabilităţilor şi a factorilor de risc la adresa infrastructurii critice. (2) Controlul asupra respectării prevederilor actelor normative privind protecţia antiteroristă a infrastructurii critice se exercită planificat, inopinat şi repetat de către reprezentanţii Centrului Antiterorist, fie în mod separat, fie împreună cu reprezentanţii altor autorităţi în limitele legale. (3) Controlul se efectuează conform prevederilor legislaţiei în vigoare şi planurilor anuale aprobate de directorul Serviciului de Informaţii şi Securitate. (4) Priorităţile şi frecvenţa controalelor obiectivelor din cadrul infrastructurii critice se stabilesc de către Serviciul de Informaţii şi Securitate. (5) Rezultatele fiecărui control se consemnează în paşaportul antiterorist al	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 $(2)^1$.”	**Articolul 20.** Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice (1) Controlul privind asigurarea protecţiei antiteroriste a infrastructurii critice are drept scop: a) verificarea nivelului de pregătire a personalului în ceea ce privește asigurarea protecţiei antiteroriste; b) determinarea capacităţii de pază și protecție a obiectivelor infrastructurii critice; c) identificarea vulnerabilităţilor şi a factorilor de risc la adresa infrastructurii critice. (2) Controlul asupra respectării prevederilor actelor normative privind protecţia antiteroristă a infrastructurii critice se exercită planificat, inopinat şi repetat de către reprezentanţii Centrului Antiterorist, fie în mod separat, fie împreună cu reprezentanţii altor autorităţi în limitele legale. $(2)^1$ 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.

	obiectivului, cu informarea gestionarului obiectivului.		(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]. (3) Controlul se efectuează conform prevederilor legislaţiei în vigoare şi planurilor anuale aprobate de directorul Serviciului de Informaţii şi Securitate. (4) Priorităţile şi frecvenţa controalelor obiectivelor din cadrul infrastructurii critice se stabilesc de către Serviciul de Informaţii şi Securitate. (5) Rezultatele fiecărui control se consemnează în paşaportul antiterorist al obiectivului, cu informarea gestionarului obiectivului.
Articolul 21 din Legea 174/2017 cu privire la energetică			
1.	(4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege şi legile sectoriale, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activității întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2).	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”;	(4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activității întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2).

2.	**Articolul 21.** Principii de activitate (1) Toate întreprinderile energetice îşi desfăşoară activitatea în conformitate cu principiul eficienței economice, cu respectarea parametrilor şi indicatorilor de calitate, stabiliţi în prezenta lege și în legile sectoriale. Preţurile şi tarifele, inclusiv cele reglementate, aplicate de întreprinderile energetice se stabilesc în conformitate cu legile sectoriale. (2) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale, organizaţiile necomerciale nu au dreptul: a) să intervină în activitatea întreprinderilor energetice; b) să distragă personalul întreprinderilor energetice de la îndeplinirea atribuțiilor de serviciu; c) să se implice în relaţiile contractuale dintre întreprinderile energetice şi consumatori, utilizatorii de sistem, cu excepțiile stabilite în prezenta lege și în legile sectoriale. (3) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale sînt obligate să notifice Guvernul cu privire la înstrăinarea obiectelor energetice aflate în proprietatea lor cu cel puţin 6 luni	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 responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de legea respectivă, 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.”.	**Articolul 21.** Principii de activitate (1) Toate întreprinderile energetice îşi desfăşoară activitatea în conformitate cu principiul eficienței economice, cu respectarea parametrilor şi indicatorilor de calitate, stabiliţi în prezenta lege și în legile sectoriale. Preţurile şi tarifele, inclusiv cele reglementate, aplicate de întreprinderile energetice se stabilesc în conformitate cu legile sectoriale. (2) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale, organizaţiile necomerciale nu au dreptul: a) să intervină în activitatea întreprinderilor energetice; b) să distragă personalul întreprinderilor energetice de la îndeplinirea atribuțiilor de serviciu; c) să se implice în relaţiile contractuale dintre întreprinderile energetice şi consumatori, utilizatorii de sistem, cu excepțiile stabilite în prezenta lege și în legile sectoriale. (3) Organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, autorităţile de reglementare, alte autorităţi publice, autorităţile administraţiei publice locale sînt obligate să notifice Guvernul cu privire la înstrăinarea obiectelor energetice aflate în proprietatea lor cu cel puţin 6 luni înainte de încheierea actelor juridice de înstrăinare. (4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale

	înainte de încheierea actelor juridice de înstrăinare. (4) Măsurile întreprinse de Agenţie, de organele centrale de specialitate, alte autorităţi ale administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege şi legile sectoriale, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activității întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2). (5) Obiectele energetice pot fi construite și admise în exploatare în conformitate cu Legea nr. 163/2010 privind autorizarea executării lucrărilor de construcţie. Exploatarea obiectelor energetice se efectuează doar după obținerea de către întreprinderile energetice a licențelor, a autorizațiilor, a altor acte permisive, eliberate în termenele și în condițiile stabilite prin lege. (6) Întreprinderile energetice, indiferent de tipul de proprietate, inclusiv distribuitorii de energie termică, sînt obligate să prezinte Agenţiei planuri, informații și rapoarte în termenele și în condițiile stabilite în legile sectoriale. (7) Întreprinderile energetice sînt obligate să efectueze în termen lucrările curente de exploatare şi de reparaţie a obiectelor energetice, cu respectarea actelor normative şi		administraţiei publice centrale, de autorităţile de reglementare, de alte autorităţi publice, de autorităţile administraţiei publice locale în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi, inclusiv privind licenţierea, autorizarea, monitorizarea şi supravegherea activității întreprinderilor energetice, nu se consideră a fi un amestec în activitatea întreprinderilor energetice în sensul alin. (2). (5) Obiectele energetice pot fi construite și admise în exploatare în conformitate cu Legea nr. 163/2010 privind autorizarea executării lucrărilor de construcţie. Exploatarea obiectelor energetice se efectuează doar după obținerea de către întreprinderile energetice a licențelor, a autorizațiilor, a altor acte permisive, eliberate în termenele și în condițiile stabilite prin lege. (6) Întreprinderile energetice, indiferent de tipul de proprietate, inclusiv distribuitorii de energie termică, sînt obligate să prezinte Agenţiei planuri, informații și rapoarte în termenele și în condițiile stabilite în legile sectoriale. (7) Întreprinderile energetice sînt obligate să efectueze în termen lucrările curente de exploatare şi de reparaţie a obiectelor energetice, cu respectarea actelor normative şi a documentelor normativ-tehnice cu privire la calitate, securitate, inclusiv securitatea industrială, precum şi cu privire la protecţia mediului, astfel încît consumatorii să fie aprovizionaţi cu energie în mod fiabil și continuu.

	a documentelor normativ-tehnice cu privire la calitate, securitate, inclusiv securitatea industrială, precum şi cu privire la protecţia mediului, astfel încît consumatorii să fie aprovizionaţi cu energie în mod fiabil și continuu. (8) Întreprinderile energetice au drept de acces la terenurile terţilor, cu condiţia obţinerii acordului proprietarilor terenurilor respective, pentru efectuarea lucrărilor de construcţie, exploatare, întreţinere, reabilitare, modernizare, inclusiv de retehnologizare, a obiectelor energetice. Efectuarea lucrărilor menţionate trebuie să fie coordonată cu proprietarii terenurilor, cu excepţia lucrărilor necesare pentru prevenirea producerii avariilor, incendiilor, electrocutărilor şi/sau a exploziilor ori pentru înlăturarea consecințelor acestora. După finalizarea lucrărilor menţionate, întreprinderile energetice sînt obligate să asigure degajarea terenului şi repunerea lui în situaţia iniţială în termenele convenite cu proprietarii terenurilor respective. Întreprinderile energetice sînt obligate să se folosească cu bună-credinţă de drepturile stabilite în prezentul articol şi să achite proprietarului de teren sau de alte bunuri proprietate privată despăgubirea cuvenită pentru pagubele produse la efectuarea lucrărilor menţionate, inclusiv în cazul înlăturării consecinţelor avariilor, incendiilor, electrocutărilor şi/sau ale exploziilor. (9) Producătorii care exploatează centralele electrice, centralele termice, care funcţionează		(7)[1] Întreprinderile energetice, identificate 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 legea respectivă, 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.”. (8) Întreprinderile energetice au drept de acces la terenurile terţilor, cu condiţia obţinerii acordului proprietarilor terenurilor respective, pentru efectuarea lucrărilor de construcţie, exploatare, întreţinere, reabilitare, modernizare, inclusiv de retehnologizare, a obiectelor energetice. Efectuarea lucrărilor menţionate trebuie să fie coordonată cu proprietarii terenurilor, cu excepţia lucrărilor necesare pentru prevenirea producerii avariilor, incendiilor, electrocutărilor şi/sau a exploziilor ori pentru înlăturarea consecințelor acestora. După finalizarea lucrărilor menţionate, întreprinderile energetice sînt obligate să asigure degajarea terenului şi repunerea lui în situaţia iniţială în termenele convenite cu proprietarii terenurilor respective. Întreprinderile energetice

	pe bază de combustibili fosili, cu excepţia celor care desfăşoară activitate sezonieră şi/sau care produc energie electrică, energie termică exclusiv pentru necesităţi proprii, sînt obligaţi să menţină rezerve de combustibili la nivel suficient pentru a asigura securitatea aprovizionării cu energie, în condiţiile stabilite de Guvern. (10) Consumatorii care dispun de centrală electrică sînt în drept să livreze în reţelele electrice surplusul de energie electrică în condițiile stabilite în Legea nr. 107/2016 cu privire la energia electrică și în Legea nr. 10/2016 privind promovarea utilizării energiei din surse regenerabile.		sînt obligate să se folosească cu bună-credinţă de drepturile stabilite în prezentul articol şi să achite proprietarului de teren sau de alte bunuri proprietate privată despăgubirea cuvenită pentru pagubele produse la efectuarea lucrărilor menţionate, inclusiv în cazul înlăturării consecinţelor avariilor, incendiilor, electrocutărilor şi/sau ale exploziilor. (9) Producătorii care exploatează centralele electrice, centralele termice, care funcţionează pe bază de combustibili fosili, cu excepţia celor care desfăşoară activitate sezonieră şi/sau care produc energie electrică, energie termică exclusiv pentru necesităţi proprii, sînt obligaţi să menţină rezerve de combustibili la nivel suficient pentru a asigura securitatea aprovizionării cu energie, în condiţiile stabilite de Guvern. (10) Consumatorii care dispun de centrală electrică sînt în drept să livreze în reţelele electrice surplusul de energie electrică în condițiile stabilite în Legea nr. 107/2016 cu privire la energia electrică și în Legea nr. 10/2016 privind promovarea utilizării energiei din surse regenerabile.
Legea nr. 202/2017 privind activitatea băncilor			
1.	**Articolul 38.** Cadrul de administrare a activității (1) Fiecare bancă trebuie să dispună de un cadru de administrare a activității riguros conceput, care să includă o structură organizatorică clară, cu linii de responsabilitate bine definite, transparente şi	Articolul 38 se completează cu alineatul $(4)^1$, cu următorul cuprins: „$(4)^1$ În vederea protecției rețelelor și sistemelor informatice pe care le deține, banca, identificată ca furnizor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, este	**Articolul 38.** Cadrul de administrare a activității (1) Fiecare bancă trebuie să dispună de un cadru de administrare a activității riguros conceput, care să includă o structură organizatorică clară, cu linii de responsabilitate bine definite, transparente şi coerente, procese eficace de identificare, administrare, monitorizare şi

	coerente, procese eficace de identificare, administrare, monitorizare şi raportare a riscurilor la care este sau ar putea fi expusă (simulări de criză), un proces de evaluare a adecvării capitalului la riscuri, un proces de evaluare a adecvării lichidităţii, mecanisme adecvate de control intern, inclusiv proceduri administrative şi contabile riguroase, politici şi practici de remunerare care să promoveze şi să fie în concordanță cu o administrare sănătoasă şi eficace a riscurilor. (2) Cadrul de administrare a activității, procesele şi mecanismele prevăzute la alin. (1) trebuie să fie cuprinzătoare şi adaptate la natura, amploarea și complexitatea riscurilor inerente modelului de afaceri şi activităților desfășurate de bancă. Mecanismele de control intern trebuie să asigure cel puţin organizarea funcțiilor de administrare a riscurilor, de asigurare a conformității și de audit intern. (3) Principiile, criteriile tehnice şi alte elemente aferente cerințelor specificate la alin. (1) și (2) care trebuie avute în vedere de către bănci se stabilesc prin actele normative emise în aplicarea prezentei legi. (4) În sensul alin. (1)–(3) sînt avute în vedere riscuri precum: riscul de credit şi al contrapărții, riscul rezidual, riscul de concentrare, riscul de securitizare, riscul de piață, riscul de rată a dobînzii din activități în afara portofoliului de tranzacționare, riscul operațional, care include și riscul denaturării securității și integrității sistemelor informaționale, riscul de lichiditate şi riscul	responsabilă pentru realizarea obligațiilor de asigurare a securității cibernetice stabilite de articolele 11 și 12 din legea respectivă, de actele normative de punere în aplicare a acestora și de actele normative care stabilesc cerințe specifice de asigurare a securității cibernetice în domeniul bancar.”.	raportare a riscurilor la care este sau ar putea fi expusă (simulări de criză), un proces de evaluare a adecvării capitalului la riscuri, un proces de evaluare a adecvării lichidităţii, mecanisme adecvate de control intern, inclusiv proceduri administrative şi contabile riguroase, politici şi practici de remunerare care să promoveze și să fie în concordanță cu o administrare sănătoasă şi eficace a riscurilor. (2) Cadrul de administrare a activității, procesele şi mecanismele prevăzute la alin. (1) trebuie să fie cuprinzătoare şi adaptate la natura, amploarea şi complexitatea riscurilor inerente modelului de afaceri şi activităților desfășurate de bancă. Mecanismele de control intern trebuie să asigure cel puţin organizarea funcțiilor de administrare a riscurilor, de asigurare a conformității și de audit intern. (3) Principiile, criteriile tehnice şi alte elemente aferente cerințelor specificate la alin. (1) și (2) care trebuie avute în vedere de către bănci se stabilesc prin actele normative emise în aplicarea prezentei legi. (4) În sensul alin. (1)–(3) sînt avute în vedere riscuri precum: riscul de credit şi al contrapărții, riscul rezidual, riscul de concentrare, riscul de securitizare, riscul de piață, riscul de rată a dobînzii din activități în afara portofoliului de tranzacționare, riscul operațional, care include și riscul denaturării securității și integrității sistemelor informaționale, riscul de lichiditate şi riscul efectului de levier excesiv, precum şi, după caz, subcategorii ale acestor riscuri.

	efectului de levier excesiv, precum și, după caz, subcategorii ale acestor riscuri. (5) Banca este obligată să raporteze anual cu privire la condițiile în care se desfășoară cadrul de administrare a activității băncii, în conformitate cu actele normative ale Băncii Naționale a Moldovei. (6) Prezentul articol se aplică cu respectarea dispozițiilor art. 59 pe bază individuală și consolidată.		(4)[1] În vederea protecției rețelelor și sistemelor informatice pe care le deține, banca, identificată ca furnizor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, este responsabilă pentru realizarea obligațiilor de asigurare a securității cibernetice stabilite de articolele 11 și 12 din legea respectivă, de actele normative de punere în aplicare a acestora și de actele normative care stabilesc cerințe specifice de asigurare a securității cibernetice în domeniul bancar. (5) Banca este obligată să raporteze anual cu privire la condițiile în care se desfășoară cadrul de administrare a activității băncii, în conformitate cu actele normative ale Băncii Naționale a Moldovei. (6) Prezentul articol se aplică cu respectarea dispozițiilor art. 59 pe bază individuală și consolidată.
2.	**Articolul 138.** Competențe de supraveghere și de sancționare (1) În exercitarea funcţiilor sale, Banca Naţională a Moldovei deține competența să dispună, faţă de o bancă, faţă de acționarii acesteia, faţă de membrii organului de conducere al băncii, faţă de persoanele care dețin funcții-cheie în cadrul băncii, care încalcă dispoziţiile prezentei legi, ale actelor normative sau ale altor acte emise în aplicarea acesteia, referitoare la supraveghere sau la condiţiile de desfăşurare a activităţii, măsuri potrivit prevederilor art. 139 şi/sau să aplice sancţiuni şi măsuri sancţionatoare potrivit prevederilor art. 141.	Articolul 138 se completează cu alineatul (6)[1], cu următorul cuprins: „(6)[1] Supravegherea și controlul de stat al respectării de către bancă a obligațiilor stabilite la art. 38 alin. (4)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și actele normative de punere a acesteia în aplicare. În exercitarea funcției de supraveghere și control de stat, autoritatea competentă la nivel național în domeniul	**Articolul 138.** Competențe de supraveghere și de sancționare (1) În exercitarea funcţiilor sale, Banca Naţională a Moldovei deține competența să dispună, faţă de o bancă, faţă de acționarii acesteia, faţă de membrii organului de conducere al băncii, faţă de persoanele care dețin funcții-cheie în cadrul băncii, care încalcă dispoziţiile prezentei legi, ale actelor normative sau ale altor acte emise în aplicarea acesteia, referitoare la supraveghere sau la condiţiile de desfăşurare a activităţii, măsuri potrivit prevederilor art. 139 şi/sau să aplice sancţiuni şi măsuri sancţionatoare potrivit prevederilor art. 141.

	(2) Banca Naţională a Moldovei îşi exercită competenţele de supraveghere şi de aplicare a măsurilor, sancţiunilor şi măsurilor sancţionatoare, potrivit prevederilor prezentei legi, în oricare dintre următoarele modalităţi: a) în mod direct; b) în colaborare cu alte autorităţi; c) prin sesizarea autorităţilor judiciare competente. (3) Banca Naţională a Moldovei are competenţa de a colecta toate informaţiile necesare şi de a efectua toate cercetările necesare în exercitarea funcţiilor sale. (4) Fără a aduce atingere prevederilor prezentei legi şi ale actelor normative emise în aplicarea acesteia, competenţa prevăzută la alin. (3) include: a) competenţa de a solicita furnizarea tuturor informaţiilor necesare de la orice persoană fizică sau juridică prevăzută la alin. (5), pentru îndeplinirea atribuţiilor care revin Băncii Naţionale a Moldovei, inclusiv a informaţiilor care trebuie furnizate, în scopuri de supraveghere şi în scopuri statistice, la intervale regulate şi în formatele specificate; b) competenţa de a efectua toate cercetările necesare pentru îndeplinirea atribuţiilor care revin Băncii Naţionale a Moldovei în legătură cu orice persoană fizică sau juridică prevăzută la alin. (5); c) competenţa de a efectua toate inspecţiile necesare la sediile persoanelor juridice menţionate la alin. (5) şi la sediul oricărei alte societăți incluse în supravegherea consolidată	securității cibernetice informează în termen de 5 zile Banca Națională a Moldovei despre orice încălcare depistată și sancțiune aplicată”.	(2) Banca Naţională a Moldovei îşi exercită competenţele de supraveghere şi de aplicare a măsurilor, sancţiunilor şi măsurilor sancţionatoare, potrivit prevederilor prezentei legi, în oricare dintre următoarele modalităţi: a) în mod direct; b) în colaborare cu alte autorităţi; c) prin sesizarea autorităţilor judiciare competente. (3) Banca Naţională a Moldovei are competenţa de a colecta toate informaţiile necesare şi de a efectua toate cercetările necesare în exercitarea funcţiilor sale. (4) Fără a aduce atingere prevederilor prezentei legi şi ale actelor normative emise în aplicarea acesteia, competenţa prevăzută la alin. (3) include: a) competenţa de a solicita furnizarea tuturor informaţiilor necesare de la orice persoană fizică sau juridică prevăzută la alin. (5), pentru îndeplinirea atribuţiilor care revin Băncii Naţionale a Moldovei, inclusiv a informaţiilor care trebuie furnizate, în scopuri de supraveghere şi în scopuri statistice, la intervale regulate şi în formatele specificate; b) competenţa de a efectua toate cercetările necesare pentru îndeplinirea atribuţiilor care revin Băncii Naţionale a Moldovei în legătură cu orice persoană fizică sau juridică prevăzută la alin. (5); c) competenţa de a efectua toate inspecţiile necesare la sediile persoanelor juridice menţionate la alin. (5) şi la sediul oricărei alte societăți incluse în supravegherea consolidată

	pentru care Banca Naţională a Moldovei este supraveghetor consolidant, cu condiţia acordului prealabil al autorităţilor competente implicate. (5) În sensul prevederilor alin. (4), sînt supuse obligaţiei de a furniza informaţii: a) băncile cu sediul în Republica Moldova și sucursalele băncilor străine; b) societăţile financiare holding cu sediul în Republica Moldova; c) societăţile financiare holding mixte cu sediul în Republica Moldova; d) societăţile financiare holding cu activitate mixtă cu sediul în Republica Moldova; e) persoanele fizice care sînt persoane afiliate societăților menţionate la lit. a)–d); f) persoanele terţe către care societățile menţionate la lit. a)–d) au externalizat anumite funcţii operaţionale sau activităţi. (6) Competenţa prevăzută la alin. (4) lit. b) include dreptul: a) de a solicita prezentarea de documente; b) de a examina evidenţele şi registrele persoanelor menţionate la alin. (5) şi de a ridica fotocopii sau extrase ale acestor evidenţe şi registre; c) de a obţine explicaţii scrise sau verbale de la orice persoană prevăzută la alin. (5) sau de la reprezentanţii ori personalul acesteia; d) de a intervieva orice altă persoană, cu consimţământul acesteia, în scopul colectării de informaţii referitoare la obiectul unei cercetări;		pentru care Banca Naţională a Moldovei este supraveghetor consolidant, cu condiţia acordului prealabil al autorităţilor competente implicate. (5) În sensul prevederilor alin. (4), sînt supuse obligaţiei de a furniza informaţii: a) băncile cu sediul în Republica Moldova și sucursalele băncilor străine; b) societăţile financiare holding cu sediul în Republica Moldova; c) societăţile financiare holding mixte cu sediul în Republica Moldova; d) societăţile financiare holding cu activitate mixtă cu sediul în Republica Moldova; e) persoanele fizice care sînt persoane afiliate societăților menţionate la lit. a)–d); f) persoanele terţe către care societățile menţionate la lit. a)–d) au externalizat anumite funcţii operaţionale sau activităţi. (6) Competenţa prevăzută la alin. (4) lit. b) include dreptul: a) de a solicita prezentarea de documente; b) de a examina evidenţele şi registrele persoanelor menţionate la alin. (5) şi de a ridica fotocopii sau extrase ale acestor evidenţe şi registre; c) de a obţine explicaţii scrise sau verbale de la orice persoană prevăzută la alin. (5) sau de la reprezentanţii ori personalul acesteia; d) de a intervieva orice altă persoană, cu consimţământul acesteia, în scopul colectării de informaţii referitoare la obiectul unei cercetări; e) de a avea acces la sistemele informaţionale şi de a solicita prezentarea de informații din bazele de date aferente.

	e) de a avea acces la sistemele informaţionale şi de a solicita prezentarea de informații din bazele de date aferente.		(6)[1] Supravegherea și controlul de stat al respectării de către bancă a obligațiilor stabilite la art. 38 alin. (4)[1], se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și actele normative de punere a acesteia în aplicare. În exercitarea funcției de supraveghere și control de stat, autoritatea competentă la nivel național în domeniul securității cibernetice informează în termen de 5 zile Banca Națională a Moldovei despre orice încălcare depistată și sancțiune aplicată.
Articolul 8 din Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate			
1.	**Articolul 8**. Securitatea și confidențialitatea schimbului de date (1) Securitatea și confidențialitatea schimbului de date sînt asigurate de către toți participanții la schimbul de date și de către deținătorul platformei de interoperabilitate, pe domeniile lor de competență, în conformitate cu cerințele de securitate aplicabile categoriei respective de date. (2) Pentru asigurarea securității și confidențialității la realizarea schimbului de date, precum și la accesarea informației cu accesibilitate limitată, suplimentar măsurilor de securitate standard, platforma de interoperabilitate oferă posibilitatea transportării datelor în formă criptată. Criptarea și decriptarea datelor sînt asigurate de către furnizorul de date și, respectiv,	Se completează cu alineatul (3)[1] cu următorul cuprins: „(3)[1] 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 legea respectivă.”	**Articolul 8**. Securitatea și confidențialitatea schimbului de date (1) Securitatea și confidențialitatea schimbului de date sînt asigurate de către toți participanții la schimbul de date și de către deținătorul platformei de interoperabilitate, pe domeniile lor de competență, în conformitate cu cerințele de securitate aplicabile categoriei respective de date. (2) Pentru asigurarea securității și confidențialității la realizarea schimbului de date, precum și la accesarea informației cu accesibilitate limitată, suplimentar măsurilor de securitate standard, platforma de interoperabilitate oferă posibilitatea transportării datelor în formă criptată. Criptarea și decriptarea datelor sînt asigurate de către furnizorul de date și, respectiv, consumatorul de date.

	consumatorul de date. (3) Participanții la schimbul de date sînt 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.		(3) Participanții la schimbul de date sînt 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. (3)[1] 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 legea respectivă.
Articolul 17 din Legea nr.270/2018 privind sistemul unitar de salarizare în sectorul bugetar			
1.	**Articolul 17.** Sporuri cu caracter specific (1) Personalul din unitățile bugetare beneficiază, după caz, de sporuri specifice grupului ocupațional sau categoriei de personal în modul stabilit de Guvern. Pentru autoritatea responsabilă de exercitarea controlului parlamentar, modul de acordare a sporului cu caracter specific se aprobă de Biroul permanent al Parlamentului. (2) Suma anuală a sporurilor cu caracter specific incluse în partea variabilă a salariului lunar nu va depăși: a) pentru personalul din domeniile învățământului, cercetării, culturii, tineretului, sportului, asistenței sociale – 10% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific;	Se completează cu alineatul 2[1], cu următorul cuprins: (2)[1] Personalul autorității competente în domeniul securității cibernetice conform Legii nr. 48/2023 privind securitatea cibernetică beneficiază de sporuri cu caracter specific incluse în partea variabilă a salariului lunar, după cum urmează: a) pentru personalul încadrat în funcțiile publice din cadrul subdiviziunii interne care exercită nemijlocit funcția de echipă națională de răspuns la incidente de securitate cibernetică – în mărime de 600% din suma anuală a salariilor de bază ale personalului acestei subdiviziuni; b) pentru personalul încadrat în celelalte funcții publice – în mărime de 200% din suma anuală a salariilor de bază ale personalului încadrat în aceste funcții publice.”.	**Articolul 17.** Sporuri cu caracter specific (1) Personalul din unitățile bugetare beneficiază, după caz, de sporuri specifice grupului ocupațional sau categoriei de personal în modul stabilit de Guvern. Pentru autoritatea responsabilă de exercitarea controlului parlamentar, modul de acordare a sporului cu caracter specific se aprobă de Biroul permanent al Parlamentului. (2) Suma anuală a sporurilor cu caracter specific incluse în partea variabilă a salariului lunar nu va depăși: a) pentru personalul din domeniile învățământului, cercetării, culturii, tineretului, sportului, asistenței sociale – 10% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b) pentru personalul din domeniul apărării naționale, securității statului și ordinii publice –

	b) pentru personalul din domeniul apărării naționale, securității statului și ordinii publice – 20% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b[1]) prin derogare de la prevederile lit. b), pentru personalul din domeniul apărării naționale, securității statului și ordinii publice implicat în activități speciale de combatere a terorismului – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; c) pentru personalul medical, inclusiv care deține funcții publice cu statut special, din autoritățile/ instituțiile/ structurile medicale, din Centrul de Medicină Legală și din instituțiile de asistență socială – 60% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d) pentru personalul din autoritatea responsabilă de exercitarea controlului parlamentar, de stabilirea, coordonarea și monitorizarea implementării politicilor și priorităților Președintelui Republicii Moldova – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d[1]) - *abrogată.* e) pentru personalul din autoritatea responsabilă de controlul constituționalității – 60% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; f) pentru personalul din autoritatea responsabilă de activitatea de monitorizare informațională, comunicare strategică și		20% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; b[1]) prin derogare de la prevederile lit. b), pentru personalul din domeniul apărării naționale, securității statului și ordinii publice implicat în activități speciale de combatere a terorismului – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; c) pentru personalul medical, inclusiv care deține funcții publice cu statut special, din autoritățile/ instituțiile/ structurile medicale, din Centrul de Medicină Legală și din instituțiile de asistență socială – 60% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d) pentru personalul din autoritatea responsabilă de exercitarea controlului parlamentar, de stabilirea, coordonarea și monitorizarea implementării politicilor și priorităților Președintelui Republicii Moldova – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; d[1]) - *abrogată.* e) pentru personalul din autoritatea responsabilă de controlul constituționalității – 60% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific; f) pentru personalul din autoritatea responsabilă de activitatea de monitorizare informațională, comunicare strategică și combatere a dezinformării – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific.

	combatere a dezinformării – 40% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific. (3) Pentru autoritățile responsabile de administrarea veniturilor fiscale și vamale și responsabile de certificare, supraveghere și control în domeniul aviației civile, limitele sporurilor cu caracter specific se aprobă de Guvern.		(2)[1] Personalul autorității competente în domeniul securității cibernetice conform Legii nr. 48/2023 privind securitatea cibernetică beneficiază de sporuri cu caracter specific incluse în partea variabilă a salariului lunar, după cum urmează: a) pentru personalul încadrat în funcțiile publice din cadrul subdiviziunii interne care exercită nemijlocit funcția de echipă națională de răspuns la incidente de securitate cibernetică – în mărime de 600% din suma anuală a salariilor de bază ale personalului acestei subdiviziuni; b) pentru personalul încadrat în celelalte funcții publice – în mărime de 200% din suma anuală a salariilor de bază ale personalului încadrat în aceste funcții publice. (3) Pentru autoritățile responsabile de administrarea veniturilor fiscale și vamale și responsabile de certificare, supraveghere și control în domeniul aviației civile, limitele sporurilor cu caracter specific se aprobă de Guvern.
Legea nr. 277/2018 privind substanțele chimice			
1.	**Articolul 11.** Competențele altor autorități ale administrației publice centrale (1) Ministerul Sănătății: a) inițiază și promovează, împreună cu celelalte autorități competente, actele normative referitoare la protecția sănătății umane, inclusiv a lucrătorilor care desfășoară activități ori se află în locuri de muncă în care sînt prezente substanțe sau amestecuri	Articolul 11 se completează cu alineatul (4)[1], cu următorul cuprins: „(4)[1] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la articolul 12 alineatul (5)[1] se exercită de către autoritatea competentă în domeniul securității cibernetice în limitele stabilite de Legea nr.	**Articolul 11.** Competențele altor autorități ale administrației publice centrale (1) Ministerul Sănătății: a) inițiază și promovează, împreună cu celelalte autorități competente, actele normative referitoare la protecția sănătății umane, inclusiv a lucrătorilor care desfășoară activități ori se află în locuri de muncă în care sînt prezente substanțe sau amestecuri chimice periculoase, și

	chimice periculoase, și la evaluarea și controlul riscului pe care îl prezintă pentru om substanțele și amestecurile chimice periculoase; b) identifică, evaluează și gestionează riscurile pentru sănătatea umană aferente substanțelor și amestecurilor chimice plasate pe piața Republicii Moldova; c) evaluează pericolele și riscurile pentru sănătatea umană în cadrul procedurii de autorizare a produselor de protecție a plantelor, a produselor biocide și a altor produse chimice menționate la art. 23 alin. (1) lit. a)–e), precum și în alte cazuri în care este necesară evaluarea pericolelor și riscurilor pentru sănătatea umană; d) organizează cercetări toxico-igienice ale substanțelor și amestecurilor chimice periculoase; e) asigură evaluarea eficacității în cadrul procedurii de autorizare a produselor biocide menționate la art. 23 alin. (1) lit. b); f) autorizează produsele biocide menționate la art. 23 alin. (1) lit. b), utilizînd platforma unică de autorizare a produselor chimice periculoase, stabilită în conformitate cu prezenta lege; g) asigură monitorizarea, evidența, raportarea și cercetarea cazurilor de otrăviri cu substanțele chimice periculoase, luînd măsuri de prevenire a acestora; h) asigură informarea și sensibilizarea publicului și a agenților economici privind pericolele și riscurile pe care le prezintă produsele menționate la art. 23 alin. (1) lit. a)–e) pentru sănătatea umană;	48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a acesteia.”	la evaluarea și controlul riscului pe care îl prezintă pentru om substanțele și amestecurile chimice periculoase; b) identifică, evaluează și gestionează riscurile pentru sănătatea umană aferente substanțelor și amestecurilor chimice plasate pe piața Republicii Moldova; c) evaluează pericolele și riscurile pentru sănătatea umană în cadrul procedurii de autorizare a produselor de protecție a plantelor, a produselor biocide și a altor produse chimice menționate la art. 23 alin. (1) lit. a)–e), precum și în alte cazuri în care este necesară evaluarea pericolelor și riscurilor pentru sănătatea umană; d) organizează cercetări toxico-igienice ale substanțelor și amestecurilor chimice periculoase; e) asigură evaluarea eficacității în cadrul procedurii de autorizare a produselor biocide menționate la art. 23 alin. (1) lit. b); f) autorizează produsele biocide menționate la art. 23 alin. (1) lit. b), utilizînd platforma unică de autorizare a produselor chimice periculoase, stabilită în conformitate cu prezenta lege; g) asigură monitorizarea, evidența, raportarea și cercetarea cazurilor de otrăviri cu substanțele chimice periculoase, luînd măsuri de prevenire a acestora; h) asigură informarea și sensibilizarea publicului și a agenților economici privind pericolele și riscurile pe care le prezintă produsele menționate la art. 23 alin. (1) lit. a)–e) pentru sănătatea umană; i) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Ministerul Mediului în procesul de implementare a

	i) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Ministerul Mediului în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; j) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și regulamentelor aprobate în temeiul acesteia; k) sesizează, prin intermediul Agenției Naționale pentru Sănătate Publică, Agenția Națională de Reglementare a Activităților Nucleare, Radiologice și Chimice și Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legi speciale în domeniul sănătății publice și protecției muncii. (2) Inspectoratul General pentru Situații de Urgență al Ministerului Afacerilor Interne: a) acordă asistență specializată Serviciului Vamal și altor instituții abilitate cu atribuții în combaterea traficului și utilizării ilicite a substanțelor și amestecurilor chimice periculoase; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia;		tratatelor internaționale de mediu aferente prezentei legi; j) cooperează, prin intermediul Agenției Naționale pentru Sănătate Publică, cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și regulamentelor aprobate în temeiul acesteia; k) sesizează, prin intermediul Agenției Naționale pentru Sănătate Publică, Agenția Națională de Reglementare a Activităților Nucleare, Radiologice și Chimice și Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legi speciale în domeniul sănătății publice și protecției muncii. (2) Inspectoratul General pentru Situații de Urgență al Ministerului Afacerilor Interne: a) acordă asistență specializată Serviciului Vamal și altor instituții abilitate cu atribuții în combaterea traficului și utilizării ilicite a substanțelor și amestecurilor chimice periculoase; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu

	c) sesizează Inspectoratul pentru Protecția Mediului asupra încălcărilor prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legile speciale în domeniul protecției civile; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova”. (3) Serviciul Vamal al Ministerului Finanțelor: a) realizează controlul și admiterea introducerii pe/scoaterii de pe teritoriul Republicii Moldova a substanțelor și amestecurilor chimice în baza actelor permisive eliberate de Agenția Națională în conformitate cu prevederile prezentei legi și în baza procedurii menționate la art. 18 alin. (2); b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele		competențele atribuite de legile speciale în domeniul protecției civile; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova”. (3) Serviciul Vamal al Ministerului Finanțelor: a) realizează controlul și admiterea introducerii pe/scoaterii de pe teritoriul Republicii Moldova a substanțelor și amestecurilor chimice în baza actelor permisive eliberate de Agenția Națională în conformitate cu prevederile prezentei legi și în baza procedurii menționate la art. 18 alin. (2); b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de Codul vamal al Republicii Moldova; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova”.

	atribuite de Codul vamal al Republicii Moldova; d) cooperează cu Agenția Națională în procesul de implementare a tratatelor internaționale de mediu aferente prezentei legi; e) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova”. (4) Agenția Națională pentru Siguranța Alimentelor: a) efectuează supravegherea și controlul producerii, importului, comercializării, utilizării și depozitării produselor de protecție a plantelor în conformitate cu legislația în domeniul protecției plantelor; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legislația specială în domeniul produselor de protecție a plantelor; d) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova”.		(4) Agenția Națională pentru Siguranța Alimentelor: a) efectuează supravegherea și controlul producerii, importului, comercializării, utilizării și depozitării produselor de protecție a plantelor în conformitate cu legislația în domeniul protecției plantelor; b) cooperează cu Inspectoratul pentru Protecția Mediului în procesul de supraveghere și control al executării prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia; c) sesizează Inspectoratul pentru Protecția Mediului asupra cazurilor de încălcare a prevederilor prezentei legi și ale regulamentelor aprobate în temeiul acesteia, care sînt depistate în cadrul controlului efectuat în conformitate cu competențele atribuite de legislația specială în domeniul produselor de protecție a plantelor; d) deține mandat cu dreptul de a primi date din Sistemul informațional automatizat „Registrul produselor chimice plasate pe piața Republicii Moldova”. (4)[1] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la articolul 12 alineatul (5)[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.

2.	**Articolul 12.** Obligațiile generale ale operatorilor din lanțul de aprovizionare (1) Producătorii și importatorii de substanțe și amestecuri chimice sînt obligați: a) să identifice și să evalueze proprietățile periculoase și posibilele riscuri pentru om și mediu ale produselor chimice pe care le furnizează; b) să dispună de informații privind identificarea, proprietățile periculoase și posibilele riscuri ale produselor chimice pe care le furnizează; c) să ofere utilizatorilor și altor persoane care manipulează produsul chimic informații privind rezultatele evaluării și alte informații disponibile și relevante privind proprietățile periculoase ale produsului chimic, privind riscurile și măsurile de siguranță; d) să actualizeze permanent informațiile disponibile privind produsele chimice. (2) Pentru a evalua proprietățile periculoase ale substanțelor și amestecurilor chimice, producătorii și importatorii de substanțe și amestecuri chimice sînt obligați să efectueze testări în laboratoare care respectă principiile bunei practici de laborator, stabilite de Guvern, în următoarele cazuri: a) substanța sau amestecul chimic plasat pe piață constituie un produs nou autohton; b) producătorii și importatorii nu dețin informațiile necesare conform alin. (1) lit. b) și nu există date disponibile pentru evaluarea corespunzătoare a substanței sau amestecului chimic fără efectuarea testelor de laborator;	Articolul 12 se completează cu alineatul $(5)^1$, cu următorul cuprins: „$(5)^1$ 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 legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.”.	**Articolul 12.** Obligațiile generale ale operatorilor din lanțul de aprovizionare (1) Producătorii și importatorii de substanțe și amestecuri chimice sînt obligați: a) să identifice și să evalueze proprietățile periculoase și posibilele riscuri pentru om și mediu ale produselor chimice pe care le furnizează; b) să dispună de informații privind identificarea, proprietățile periculoase și posibilele riscuri ale produselor chimice pe care le furnizează; c) să ofere utilizatorilor și altor persoane care manipulează produsul chimic informații privind rezultatele evaluării și alte informații disponibile și relevante privind proprietățile periculoase ale produsului chimic, privind riscurile și măsurile de siguranță; d) să actualizeze permanent informațiile disponibile privind produsele chimice. (2) Pentru a evalua proprietățile periculoase ale substanțelor și amestecurilor chimice, producătorii și importatorii de substanțe și amestecuri chimice sînt obligați să efectueze testări în laboratoare care respectă principiile bunei practici de laborator, stabilite de Guvern, în următoarele cazuri: a) substanța sau amestecul chimic plasat pe piață constituie un produs nou autohton; b) producătorii și importatorii nu dețin informațiile necesare conform alin. (1) lit. b) și nu există date disponibile pentru evaluarea corespunzătoare a substanței sau amestecului chimic fără efectuarea testelor de laborator; c) în literatura științifică de specialitate au apărut date cu privire la potențialele proprietăți

	c) în literatura științifică de specialitate au apărut date cu privire la potențialele proprietăți periculoase ale substanței sau ale substanțelor componente ale amestecului chimic; d) nu există alte mijloace de obținere a informației necesare pentru evaluarea substanței sau amestecului fără efectuarea testelor. (3) Testările menționate la alin. (2) se efectuează în conformitate cu metodele indicate în Regulamentul privind stabilirea metodelor de testare a substanțelor chimice și în alte acte normative aprobate de Guvern. (4) Orice operator din lanțul de aprovizionare al unei substanțe sau al unui amestec este obligat: a) să transmită operatorului sau distribuitorului situat imediat în amontele lanțului de aprovizionare informațiile furnizate de către producători și importatori; b) să informeze operatorul sau distribuitorul situat imediat în amontele lanțului de aprovizionare despre noile informații pe care le-a identificat cu privire la pericolele și riscurile produselor chimice și măsurile de siguranță. (5) În scopul prevenirii sau al evitării producerii unei daune sănătății umane și mediului, toate persoanele fizice sau juridice care manipulează produse chimice trebuie să ia măsurile de protecție necesare pe care le-au identificat ele însele sau care le-au fost		periculoase ale substanței sau ale substanțelor componente ale amestecului chimic; d) nu există alte mijloace de obținere a informației necesare pentru evaluarea substanței sau amestecului fără efectuarea testelor. (3) Testările menționate la alin. (2) se efectuează în conformitate cu metodele indicate în Regulamentul privind stabilirea metodelor de testare a substanțelor chimice și în alte acte normative aprobate de Guvern. (4) Orice operator din lanțul de aprovizionare al unei substanțe sau al unui amestec este obligat: a) să transmită operatorului sau distribuitorului situat imediat în amontele lanțului de aprovizionare informațiile furnizate de către producători și importatori; b) să informeze operatorul sau distribuitorul situat imediat în amontele lanțului de aprovizionare despre noile informații pe care le-a identificat cu privire la pericolele și riscurile produselor chimice și măsurile de siguranță. (5) În scopul prevenirii sau al evitării producerii unei daune sănătății umane și mediului, toate persoanele fizice sau juridice care manipulează produse chimice trebuie să ia măsurile de protecție necesare pe care le-au identificat ele însele sau care le-au fost comunicate în conformitate cu prezentul articol. (5)[1] 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

	comunicate în conformitate cu prezentul articol.		stabilite de legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.
Legea nr. 306/2018 privind siguranța alimentelor			
1.	**Articolul 7.** Cerințele generale privind siguranța alimentelor (1) Siguranța produselor alimentare și a materialelor care vin în contact cu produsele alimentare se asigură prin: a) reglementarea și controlul de stat în domeniul asigurării inofensivității acestora; b) luarea de către operatorii din domeniul alimentar a unor măsuri organizatorice, agrochimice, veterinare, tehnologice, sanitar-antiepidemice și fitosanitare în vederea respectării reglementărilor aplicabile în domeniul alimentar; c) controlul inofensivității produselor alimentare și a materialelor care vin în contact cu produsele alimentare, efectuat de către operatorii din domeniul alimentar pe tot lanțul alimentar, inclusiv prin aplicarea principiilor de analiză a riscurilor în punctele critice de control (HACCP – Hazard Analysis and Critical Control Points). (2) Cerințele privind asigurarea inofensivității produselor alimentare sînt impuse prin Acordul privind aplicarea de măsuri sanitare și fitosanitare (SPS) al Organizației Mondiale a Comerțului, la care Republica Moldova este parte. Acestea sînt stabilite în baza evaluării riscurilor pentru sănătatea umană și sînt executorii.	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 legea respectivă, 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.”.	**Articolul 7.** Cerințele generale privind siguranța alimentelor (1) Siguranța produselor alimentare și a materialelor care vin în contact cu produsele alimentare se asigură prin: a) reglementarea și controlul de stat în domeniul asigurării inofensivității acestora; b) luarea de către operatorii din domeniul alimentar a unor măsuri organizatorice, agrochimice, veterinare, tehnologice, sanitar-antiepidemice și fitosanitare în vederea respectării reglementărilor aplicabile în domeniul alimentar; c) controlul inofensivității produselor alimentare și a materialelor care vin în contact cu produsele alimentare, efectuat de către operatorii din domeniul alimentar pe tot lanțul alimentar, inclusiv prin aplicarea principiilor de analiză a riscurilor în punctele critice de control (HACCP – Hazard Analysis and Critical Control Points). (2) Cerințele privind asigurarea inofensivității produselor alimentare sînt impuse prin Acordul privind aplicarea de măsuri sanitare și fitosanitare (SPS) al Organizației Mondiale a Comerțului, la care Republica Moldova este parte. Acestea sînt stabilite în baza evaluării riscurilor pentru sănătatea umană și sînt executorii.

	(3) Cerințele menționate la alin. (2) se bazează pe rezultatele cercetărilor științifice privind particularitățile de alimentație și nutriție și starea de sănătate a populației, pe identificarea și estimarea inofensivității și a pericolelor pe care le pot prezenta produsele alimentare și materialele care vin în contact cu produsele alimentare, pe evaluarea și analiza riscurilor de a periclita sănătatea umană ca urmare a consumului acestora, pe estimarea consecințelor sociale și economice ale consumului de produse alimentare periculoase și/sau nesigure. (4) Produsele alimentare și materialele care vin în contact cu produsele alimentare ce respectă reglementările din domeniul alimentar se consideră că nu prezintă riscuri pentru sănătatea umană. (5) Conformitatea unui produs alimentar cu cerințele specifice aplicabile acelui produs alimentar nu împiedică organul de control abilitat să restricționeze introducerea lui pe piață ori să solicite retragerea lui de pe piață în cazul în care există suspiciuni că, în pofida acestei conformități, produsul alimentar respectiv nu prezintă siguranță. (6) Se interzice producerea și/sau introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare care: a) nu corespund reglementărilor aplicabile din domeniul alimentar;		(3) Cerințele menționate la alin. (2) se bazează pe rezultatele cercetărilor științifice privind particularitățile de alimentație și nutriție și starea de sănătate a populației, pe identificarea și estimarea inofensivității și a pericolelor pe care le pot prezenta produsele alimentare și materialele care vin în contact cu produsele alimentare, pe evaluarea și analiza riscurilor de a periclita sănătatea umană ca urmare a consumului acestora, pe estimarea consecințelor sociale și economice ale consumului de produse alimentare periculoase și/sau nesigure. (4) Produsele alimentare și materialele care vin în contact cu produsele alimentare ce respectă reglementările din domeniul alimentar se consideră că nu prezintă riscuri pentru sănătatea umană. (5) Conformitatea unui produs alimentar cu cerințele specifice aplicabile acelui produs alimentar nu împiedică organul de control abilitat să restricționeze introducerea lui pe piață ori să solicite retragerea lui de pe piață în cazul în care există suspiciuni că, în pofida acestei conformități, produsul alimentar respectiv nu prezintă siguranță. (6) Se interzice producerea și/sau introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare care: a) nu corespund reglementărilor aplicabile din domeniul alimentar; b) sînt periculoase și pot afecta sănătatea umană în condiții normale de folosire a acestora de către consumator, ținînd cont de informația

	b) sînt periculoase și pot afecta sănătatea umană în condiții normale de folosire a acestora de către consumator, ținînd cont de informația cuprinsă în etichetă sau pusă la dispoziția consumatorului în alt mod; c) sînt improprii consumului uman, fiind contaminate și/sau impure, sau prezentînd semne de alterare; d) sînt falsificate; e) nu au inclusă pe ambalaj sau pe etichetă informația prevăzută la art. 8 din Legea nr. 279/2017 privind informarea consumatorului cu privire la produsele alimentare; f) au termenul de valabilitate expirat; g) nu permit să le fie determinată originea și nu asigură trasabilitatea acestora; h) nu corespund cerințelor de comercializare cu amănuntul, aprobate de către Guvern. (7) Produsele alimentare și materialele care vin în contact cu produsele alimentare prevăzute la alin. (6), care se consideră neconforme reglementărilor aplicate în domeniul alimentar, sînt supuse utilizării condiționate sau nimicirii. (8) Atunci cînd se determină dacă un aliment prezintă sau nu siguranță, trebuie să se aibă în vedere: a) condițiile de folosire a alimentului de către consumator și la fiecare etapă a lanțului alimentar; b) informațiile furnizate consumatorului, inclusiv cele de pe etichetă sau alte informații general disponibile pentru consumator în vederea evitării unor anumite efecte negative		cuprinsă în etichetă sau pusă la dispoziția consumatorului în alt mod; c) sînt improprii consumului uman, fiind contaminate și/sau impure, sau prezentînd semne de alterare; d) sînt falsificate; e) nu au inclusă pe ambalaj sau pe etichetă informația prevăzută la art. 8 din Legea nr. 279/2017 privind informarea consumatorului cu privire la produsele alimentare; f) au termenul de valabilitate expirat; g) nu permit să le fie determinată originea și nu asigură trasabilitatea acestora; h) nu corespund cerințelor de comercializare cu amănuntul, aprobate de către Guvern. (7) Produsele alimentare și materialele care vin în contact cu produsele alimentare prevăzute la alin. (6), care se consideră neconforme reglementărilor aplicate în domeniul alimentar, sînt supuse utilizării condiționate sau nimicirii. (8) Atunci cînd se determină dacă un aliment prezintă sau nu siguranță, trebuie să se aibă în vedere: a) condițiile de folosire a alimentului de către consumator și la fiecare etapă a lanțului alimentar; b) informațiile furnizate consumatorului, inclusiv cele de pe etichetă sau alte informații general disponibile pentru consumator în vederea evitării unor anumite efecte negative asupra sănătății ale alimentului respectiv sau ale categoriei respective de alimente.

	asupra sănătății ale alimentului respectiv sau ale categoriei respective de alimente. (9) Atunci cînd se determină dacă un aliment dăunează sănătății, trebuie să se ia în considerare: a) efectul probabil imediat și/sau de scurtă durată, și/sau de lungă durată al acestuia atît asupra persoanei care îl consumă, cît și asupra generațiilor viitoare; b) efectele toxice cumulative probabile ale acestuia; c) sensibilitatea alimentară a unei anumite categorii de consumatori, în cazul în care alimentul respectiv îi este destinat. (10) Produsele alimentare trebuie să satisfacă necesitățile fiziologice ale omului în substanțe nutritive și în energie, să fie inofensive, să nu conțină contaminanți, microorganisme și alte organisme ori substanțe biologice în cantități care să depășească valorile-limită stabilite în reglementările din domeniu alimentar, să nu prezinte în alt mod pericol pentru om, să fie produse și introduse pe piață în condiții de igienă conform prevederilor Legii nr. 296/2017 privind cerințele generale de igienă a produselor alimentare. (11) Producerea, transportul, depozitarea și introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare se efectuează în spații și în condiții ce corespund cerințelor prezentei legi, iar operatorii din domeniul alimentar dețin autorizații sanitar-veterinare de funcționare eliberate în conformitate cu art.		(9) Atunci cînd se determină dacă un aliment dăunează sănătății, trebuie să se ia în considerare: a) efectul probabil imediat și/sau de scurtă durată, și/sau de lungă durată al acestuia atît asupra persoanei care îl consumă, cît și asupra generațiilor viitoare; b) efectele toxice cumulative probabile ale acestuia; c) sensibilitatea alimentară a unei anumite categorii de consumatori, în cazul în care alimentul respectiv îi este destinat. (10) Produsele alimentare trebuie să satisfacă necesitățile fiziologice ale omului în substanțe nutritive și în energie, să fie inofensive, să nu conțină contaminanți, microorganisme și alte organisme ori substanțe biologice în cantități care să depășească valorile-limită stabilite în reglementările din domeniu alimentar, să nu prezinte în alt mod pericol pentru om, să fie produse și introduse pe piață în condiții de igienă conform prevederilor Legii nr. 296/2017 privind cerințele generale de igienă a produselor alimentare. (11) Producerea, transportul, depozitarea și introducerea pe piață a produselor alimentare și a materialelor care vin în contact cu produsele alimentare se efectuează în spații și în condiții ce corespund cerințelor prezentei legi, iar operatorii din domeniul alimentar dețin autorizații sanitar-veterinare de funcționare eliberate în conformitate cu art. 18 din Legea nr. 221/2007 privind activitatea sanitar-veterinară sau dețin certificate de înregistrare în domeniul siguranței alimentelor eliberate în conformitate

	18 din Legea nr. 221/2007 privind activitatea sanitar-veterinară sau dețin certificate de înregistrare în domeniul siguranței alimentelor eliberate în conformitate cu art. 231 din Legea nr. 50/2013 cu privire la controalele oficiale pentru verificarea conformității cu legislația privind hrana pentru animale și produsele alimentare și cu normele de sănătate și de bunăstare a animalelor. (12) Operatorii din domeniul alimentar vor întreprinde măsurile de rigoare pentru a elimina riscul de contaminare sau de deteriorare a alimentelor și de transformare a acestora în produse periculoase pentru consumatori. (13) În cazul în care un produs alimentar care nu prezintă siguranță face parte dintr-un transport, dintr-un lot sau dintr-o livrare de mărfuri alimentare de la o sursă sau din aceeași clasă ori având aceeași descriere, se presupune că toate produsele alimentare din respectivul transport, lot sau din respectiva livrare nu prezintă siguranță, cu excepția cazurilor în care se constată, în urma unei evaluări detaliate, că nu s-a identificat nicio dovadă care să indice că restul transportului, lotului sau al livrării nu prezintă siguranță.		cu art. 231 din Legea nr. 50/2013 cu privire la controalele oficiale pentru verificarea conformității cu legislația privind hrana pentru animale și produsele alimentare și cu normele de sănătate și de bunăstare a animalelor. (12) Operatorii din domeniul alimentar vor întreprinde măsurile de rigoare pentru a elimina riscul de contaminare sau de deteriorare a alimentelor și de transformare a acestora în produse periculoase pentru consumatori. (13) În cazul în care un produs alimentar care nu prezintă siguranță face parte dintr-un transport, dintr-un lot sau dintr-o livrare de mărfuri alimentare de la o sursă sau din aceeași clasă ori avînd aceeași descriere, se presupune că toate produsele alimentare din respectivul transport, lot sau din respectiva livrare nu prezintă siguranță, cu excepția cazurilor în care se constată, în urma unei evaluări detaliate, că nu s-a identificat nicio dovadă care să indice că restul transportului, lotului sau al livrării nu prezintă siguranță. (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 legea respectivă, 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.** Responsabilități privind siguranța alimentelor	Articolul 8 se completează cu alineatul (9)[1], cu următorul cuprins:	**Articolul 8.** Responsabilități privind siguranța alimentelor

	(1) Operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale sînt responsabili pe întregul lanț alimentar de respectarea reglementărilor din domeniul alimentar. (2) În cazul în care operatorul din domeniul alimentar consideră sau are motive întemeiate să considere că un produs alimentar pe care l-a importat, produs, procesat, fabricat sau distribuit nu satisface cerințele de siguranță și poate fi dăunător pentru sănătatea umană, el inițiază imediat procedurile de retragere a produsului alimentar de pe piață, dacă produsul respectiv a ieșit de sub controlul său, și informează imediat în acest sens Agenția Națională pentru Siguranța Alimentelor. Operatorul informează, în mod eficient și precis, consumatorul în legătură cu motivul retragerii produsului alimentar și retrage de la consumator produsele deja livrate, atunci cînd alte măsuri nu sînt suficiente pentru a atinge un nivel ridicat de protecție a sănătății. (3) Operatorul din domeniul alimentar informează imediat organul de control abilitat cu privire la acțiunile întreprinse pentru prevenirea riscurilor asupra consumatorului final și nu împiedică ori descurajează orice persoană să coopereze cu autoritățile administrației publice în cazul în care aceasta ar putea preveni, reduce sau elimina un risc prezentat de un produs alimentar. (4) Operatorii din domeniul alimentar cooperează cu organul de control abilitat la acțiunile întreprinse pentru evitarea sau	„(9)[1] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la articolul 7 alineatul (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.	(1) Operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale sînt responsabili pe întregul lanț alimentar de respectarea reglementărilor din domeniul alimentar. (2) În cazul în care operatorul din domeniul alimentar consideră sau are motive întemeiate să considere că un produs alimentar pe care l-a importat, produs, procesat, fabricat sau distribuit nu satisface cerințele de siguranță și poate fi dăunător pentru sănătatea umană, el inițiază imediat procedurile de retragere a produsului alimentar de pe piață, dacă produsul respectiv a ieșit de sub controlul său, și informează imediat în acest sens Agenția Națională pentru Siguranța Alimentelor. Operatorul informează, în mod eficient și precis, consumatorul în legătură cu motivul retragerii produsului alimentar și retrage de la consumator produsele deja livrate, atunci cînd alte măsuri nu sînt suficiente pentru a atinge un nivel ridicat de protecție a sănătății. (3) Operatorul din domeniul alimentar informează imediat organul de control abilitat cu privire la acțiunile întreprinse pentru prevenirea riscurilor asupra consumatorului final și nu împiedică ori descurajează orice persoană să coopereze cu autoritățile administrației publice în cazul în care aceasta ar putea preveni, reduce sau elimina un risc prezentat de un produs alimentar. (4) Operatorii din domeniul alimentar cooperează cu organul de control abilitat la acțiunile întreprinse pentru evitarea sau

	reducerea riscurilor prezentate de un produs alimentar introdus pe piață. (5) Controlul de stat privind asigurarea inofensivității și a calității produselor alimentare și ale materialelor care vin în contact cu produsele alimentare aflate în uz la toate etapele lanțului alimentar se efectuează de către Agenția Națională pentru Siguranța Alimentelor. În acest scop, agenția nominalizată monitorizează și verifică respectarea cerințelor prevăzute în reglementările din domeniul alimentar de către operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale pe întregul lanț alimentar. (6) Controlul de stat al operatorilor din domeniul alimentar și operatorilor din domeniul hranei pentru animale care practică activitate de întreprinzător se planifică, se efectuează și se înregistrează în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător. (7) Prin derogare de la prevederile alin. (5), controlul și supravegherea de stat privind asigurarea inofensivității și calității produselor alimentare comercializate în farmacii, privind siguranța și calitatea materialelor care vin în contact cu produsele alimentare introduse pe piață și privind etichetarea nutrițională și înscrierea mențiunilor de sănătate pe produsele alimentare se efectuează de către Agenția Națională pentru Sănătate Publică în		reducerea riscurilor prezentate de un produs alimentar introdus pe piață. (5) Controlul de stat privind asigurarea inofensivității și a calității produselor alimentare și ale materialelor care vin în contact cu produsele alimentare aflate în uz la toate etapele lanțului alimentar se efectuează de către Agenția Națională pentru Siguranța Alimentelor. În acest scop, agenția nominalizată monitorizează și verifică respectarea cerințelor prevăzute în reglementările din domeniul alimentar de către operatorii din domeniul alimentar și operatorii din domeniul hranei pentru animale pe întregul lanț alimentar. (6) Controlul de stat al operatorilor din domeniul alimentar și operatorilor din domeniul hranei pentru animale care practică activitate de întreprinzător se planifică, se efectuează și se înregistrează în conformitate cu prevederile Legii nr. 131/2012 privind controlul de stat asupra activității de întreprinzător. (7) Prin derogare de la prevederile alin. (5), controlul și supravegherea de stat privind asigurarea inofensivității și calității produselor alimentare comercializate în farmacii, privind siguranța și calitatea materialelor care vin în contact cu produsele alimentare introduse pe piață și privind etichetarea nutrițională și înscrierea mențiunilor de sănătate pe produsele alimentare se efectuează de către Agenția Națională pentru Sănătate Publică în conformitate cu atribuțiile stabilite de legislația națională.

	conformitate cu atribuțiile stabilite de legislația națională. (8) La elaborarea sau adaptarea reglementărilor din domeniul alimentar se iau în considerare normele și recomandările internaționale, inclusiv cele ale Comisiei Codex Alimentarius și ale Uniunii Europene. (9) Operatorii din domeniul alimentar care produc, achiziționează, depozitează, transportă și introduc pe piață produse alimentare sau prestează servicii de alimentație publică trebuie să respecte prevederile Legii nr. 296/2017 privind cerințele generale de igienă a produselor alimentare și să efectueze măsuri de asigurare a siguranței produselor respective.		(8) La elaborarea sau adaptarea reglementărilor din domeniul alimentar se iau în considerare normele și recomandările internaționale, inclusiv cele ale Comisiei Codex Alimentarius și ale Uniunii Europene. (9) Operatorii din domeniul alimentar care produc, achiziționează, depozitează, transportă și introduc pe piață produse alimentare sau prestează servicii de alimentație publică trebuie să respecte prevederile Legii nr. 296/2017 privind cerințele generale de igienă a produselor alimentare și să efectueze măsuri de asigurare a siguranței produselor respective. (9)[1] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la articolul 7 alineatul (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.
Articolul 22 din Legea nr. 192/2019 privind securitatea aeronautică			
1.	(1) Asigurarea securităţii cibernetice în domeniul aviaţiei civile reprezintă o atribuţie a autorităţii administrative de implementare şi realizare a politicilor în domeniul aviaţiei civile, precum şi a instituţiei publice responsabile de implementarea politicii statului în domeniul securităţii cibernetice la nivel naţional.	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.”	(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.	(1) Asigurarea securităţii cibernetice în domeniul aviaţiei civile reprezintă o atribuţie a autorităţii administrative de implementare şi realizare a politicilor în domeniul aviaţiei civile, precum şi a instituţiei publice responsabile de implementarea politicii statului în domeniul securităţii cibernetice la nivel naţional. (2) Operatorii aeronautici şi entităţile aeronautice evaluează riscurile la adresa securităţii cibernetice, conform procedurii aprobate de către autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile. În baza evaluării respective, operatorii aeronautici şi entităţile aeronautice elaborează şi implementează măsurile corespunzătoare de protecţie în scopul asigurării confidenţialităţii, integrităţii şi accesibilităţii sistemelor informaţionale şi a reţelelor de comunicaţii electronice de importanţă critică, precum şi a datelor utilizate în aviaţia civilă, a căror afectare poate pune în pericol siguranţa şi securitatea aviaţiei civile.	Se completează cu alineatele $(2)^1$ și $(2)^2$ cu următorul cuprins: „$(2)^1$ 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 legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. $(2)^2$ Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul $(2)^1$ 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.”	(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) Operatorii aeronautici şi entităţile aeronautice evaluează riscurile la adresa securităţii cibernetice, conform procedurii aprobate de către autoritatea administrativă de implementare şi realizare a politicilor în domeniul aviaţiei civile. În baza evaluării respective, operatorii aeronautici şi entităţile aeronautice elaborează şi implementează măsurile corespunzătoare de protecţie în scopul asigurării confidenţialităţii, integrităţii şi accesibilităţii sistemelor informaţionale şi a reţelelor de comunicaţii electronice de importanţă critică, precum şi a datelor utilizate în aviaţia civilă, a căror afectare poate pune în pericol siguranţa şi securitatea aviaţiei civile. $(2)^1$ 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 legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.

			(2)[2] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la alineatul (2)[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.
Codul transportului feroviar nr. 19/2022			
1.	**Articolul 26.** Activitatea de supraveghere a siguranței feroviare (1) Autoritatea Feroviară efectuează supravegherea continuă a respectării condițiilor: a) de desfășurare a activității de transport feroviar de către întreprinderile feroviare; b) de certificare a siguranței feroviare pentru întreprinderile feroviare; c) de autorizare în materie de siguranță a Administratorului infrastructurii; d) de aplicare a sistemului de management al siguranței. (2) Activitatea de supraveghere a siguranței feroviare se realizează prin evaluarea situațiilor economico-financiare semestriale ale entităților din domeniul transportului feroviar, a rapoartelor privind incidentele și accidentele feroviare, a procesului de întreținere a vehiculelor feroviare și a procesului de întreținere a infrastructurii feroviare. (3) Întreprinderile feroviare și Administratorul infrastructurii achită plăți pentru supravegherea respectării condițiilor	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 articolul 89 alineatul (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.”	**Articolul 26.** Activitatea de supraveghere a siguranței feroviare (1) Autoritatea Feroviară efectuează supravegherea continuă a respectării condițiilor: a) de desfășurare a activității de transport feroviar de către întreprinderile feroviare; b) de certificare a siguranței feroviare pentru întreprinderile feroviare; c) de autorizare în materie de siguranță a Administratorului infrastructurii; d) de aplicare a sistemului de management al siguranței. (1)[1] Supravegherea și controlul de stat al modului în care sunt respectate obligațiile stabilite la articolul 89 alineatul (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) Activitatea de supraveghere a siguranței feroviare se realizează prin evaluarea situațiilor economico-financiare semestriale ale entităților din domeniul transportului feroviar, a rapoartelor privind incidentele și accidentele

	stabilite la alin. (1). Aceste plăți constituie venituri colectate de Autoritatea Feroviară pentru finanțarea cheltuielilor aprobate în bugetul acesteia. (4) Nomenclatorul serviciilor de supraveghere a siguranței feroviare, mărimea plăților, precum și modul de achitare a acestor plăți se stabilesc de Guvern.		feroviare, a procesului de întreținere a vehiculelor feroviare și a procesului de întreținere a infrastructurii feroviare. (3) Întreprinderile feroviare și Administratorul infrastructurii achită plăți pentru supravegherea respectării condițiilor stabilite la alin. (1). Aceste plăți constituie venituri colectate de Autoritatea Feroviară pentru finanțarea cheltuielilor aprobate în bugetul acesteia. (4) Nomenclatorul serviciilor de supraveghere a siguranței feroviare, mărimea plăților, precum și modul de achitare a acestor plăți se stabilesc de Guvern.
2.	**Articolul 89.** Principii de bază în gestionarea siguranței feroviare (1) Ministerul, Autoritatea Feroviară (în calitate de autoritate națională de siguranță feroviară), Administratorul infrastructurii și întreprinderile feroviare, fiecare în conformitate cu propriile responsabilități, asigură următoarele: a) menținerea și îmbunătățirea în mod continuu a siguranței feroviare, acordând prioritate prevenirii accidentelor atunci când aceasta este judicios și fezabil; b) aplicarea, într-o manieră transparentă și nediscriminatorie, a normelor de siguranță feroviară; c) dezvoltarea unui sistem feroviar uniform; d) abordări bazate pe sistem privind măsurile de dezvoltare și îmbunătățire a siguranței feroviare.	Articolul 89 se completează cu alineatul $(3)^1$ cu următorul cuprins: „$(3)^1$ Administratorul infrastructurii și întreprinderile feroviare, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice.”	**Articolul 89.** Principii de bază în gestionarea siguranței feroviare (1) Ministerul, Autoritatea Feroviară (în calitate de autoritate națională de siguranță feroviară), Administratorul infrastructurii și întreprinderile feroviare, fiecare în conformitate cu propriile responsabilități, asigură următoarele: a) menținerea și îmbunătățirea în mod continuu a siguranței feroviare, acordând prioritate prevenirii accidentelor atunci când aceasta este judicios și fezabil; b) aplicarea, într-o manieră transparentă și nediscriminatorie, a normelor de siguranță feroviară; c) dezvoltarea unui sistem feroviar uniform; d) abordări bazate pe sistem privind măsurile de dezvoltare și îmbunătățire a siguranței feroviare. (2) Administratorul infrastructurii și întreprinderile feroviare sunt responsabile de funcționarea în siguranță a sistemului feroviar și

	(2) Administratorul infrastructurii și întreprinderile feroviare sunt responsabile de funcționarea în siguranță a sistemului feroviar și de controlul riscurilor asociate, pun în aplicare măsurile necesare de control al riscurilor, cooperează în vederea aplicării normelor și a standardelor naționale și internaționale de siguranță feroviară și stabilesc sisteme de management al siguranței. (3) Administratorul infrastructurii și întreprinderile feroviare răspund de părțile componente ale sistemului feroviar și de funcționarea în siguranță a acestora, inclusiv de furnizarea de materiale și contractarea de servicii, față de utilizatori, clienți și angajați. (4) Răspunderea Administratorului infrastructurii și a întreprinderilor feroviare prevăzută la alin. (3) nu-i scutește de răspundere pe producătorii de piese integrale și de elemente constitutive de interoperabilitate ale subsistemelor individuale, pe entitățile responsabile cu întreținerea vehiculelor feroviare, pe deținătorii de vehicule feroviare și pe furnizorii de alte servicii necesare vehiculelor feroviare, de structuri, instalații, echipamente, materiale. Toate acestea trebuie să fie conforme cu cerințele și condițiile stipulate privind utilizarea lor, astfel încât Administratorul infrastructurii sau întreprinderile feroviare să le poată folosi în siguranță în sistemul feroviar.		de controlul riscurilor asociate, pun în aplicare măsurile necesare de control al riscurilor, cooperează în vederea aplicării normelor și a standardelor naționale și internaționale de siguranță feroviară și stabilesc sisteme de management al siguranței. (3) Administratorul infrastructurii și întreprinderile feroviare răspund de părțile componente ale sistemului feroviar și de funcționarea în siguranță a acestora, inclusiv de furnizarea de materiale și contractarea de servicii, față de utilizatori, clienți și angajați. (3)[1] Administratorul infrastructurii și întreprinderile feroviare, identificate ca furnizori de servicii potrivit Legii nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligațiilor de asigurare a securității cibernetice stabilite de legea respectivă, de actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice. (4) Răspunderea Administratorului infrastructurii și a întreprinderilor feroviare prevăzută la alin. (3) nu-i scutește de răspundere pe producătorii de piese integrale și de elemente constitutive de interoperabilitate ale subsistemelor individuale, pe entitățile responsabile cu întreținerea vehiculelor feroviare, pe deținătorii de vehicule feroviare și pe furnizorii de alte servicii necesare vehiculelor feroviare, de structuri, instalații, echipamente, materiale. Toate acestea trebuie să fie conforme cu cerințele și condițiile stipulate privind utilizarea lor, astfel încât Administratorul

			infrastructurii sau întreprinderile feroviare să le poată folosi în siguranță în sistemul feroviar.
Articolul 39 din Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere			
1.	**Articolul 39.** Cerințe de Securitate aplicabile prestatorilor de servicii de încredere (1) Prestatorii de servicii de încredere calificați și necalificați aplică măsurile tehnice și organizaționale corespunzătoare pentru gestionarea riscurilor la adresa securității serviciilor de încredere pe care le prestează. (2) Prestatorii de servicii de încredere calificați și necalificați notifică organului de supraveghere și control, nu mai târziu de 24 de ore din momentul constatării, încălcarea securității sau pierderea integrității care are un impact semnificativ asupra serviciului de încredere prestat sau asupra datelor cu caracter personal păstrate de aceștia. În cazul în care încălcarea securității sau pierderea integrității este de natură să afecteze în mod negativ o persoană fizică sau juridică căreia i-a fost prestat serviciul de încredere, prestatorul de servicii de încredere notifică și persoanei fizice sau juridice respective încălcarea securității sau pierderea integrității, fără întârzieri nejustificate. (3) Organul de supraveghere și control notificat informează publicul sau solicită prestatorului de servicii de încredere să facă acest lucru în cazul în care consideră că dezvăluirea încălcării securității sau pierderea integrității servește interesului public.	Articolul 39 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 prin 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 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. (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.”	**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 prin 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 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. (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.”