



Comisia securitate națională, apărare și ordine publică

Raport asupra proiectului de lege pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr.48/2023 privind securitatea cibernetică) (nr.41 din 14.02.2024), lectura II.

În temeiul atribuțiilor funcționale stabilite de Regulamentul Parlamentului, Comisia securitate națională, apărare și ordine publică, a examinat în cadrul ședinței sale din data de 21 martie a.c., amendamentele, obiecțiile și propunerile parvenite asupra prezentului proiect de lege.

Scopul principal al acestuia este modificarea cadrului legislativ în vigoare în vederea punerii în aplicare a unor reglementări prevăzute de Legea privind securitatea cibernetică, adoptată de Parlament la data de 16 martie 2023.

Sinteza amendamentelor cu decizia argumentată a Comisiei și proiectul definitivat sunt parte integrantă al prezentului raport.

Totodată, în vederea asigurării unei proces transparent de examinare al amendamentelor, la data de 20 martie Comisia a organizat consultări publice difuzate inclusiv live, la care au participat autorii proiectului, deputați și funcționari din cadrul altor comisii permanente, reprezentanți ai Băncii Naționale, ai proiectului Moldova Cybersecurity Rapid Assistance și ai Agenției Securitate Cibernetică.

Astfel, în rezultatul discuțiilor, la propunerea autorilor proiectului, Comisia a acceptat excluderea prevederilor stabilite la alineatele (7) și (8) al articolului 38² ce stabilește gestionarea riscurilor de tehnologie a informației și a comunicațiilor (TIC), de securitate a informației și de continuitate a activității, din Legea nr. 202/2017 privind activitatea băncilor.

Reieșind din cele sus-menționate, cu votul majorității membrilor săi, Comisia se pronunță pentru adoptarea prezentului proiect de lege de către plenul Parlamentului, în lectura a doua.

Lilian CARP
Președintele Comisiei

Ex: Vitalie Lungu
consultant principal
022 820 519

LEGE

pentru modificarea unor acte normative

Parlamentul adoptă prezenta lege organică.

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

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

„(5) Întreprinderile și instituțiile farmaceutice, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de legea respectivă.

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

„(3) Persoanele care efectuează investigații în vederea creării medicamentelor noi, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de legea respectivă.”

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

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

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

„(8) Prestatorii de servicii medicale, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de Legea nr. 48/2023 privind securitatea cibernetică.

(9) Supravegherea și controlul de stat al respectării de către prestatorii de servicii medicale a obligațiilor menționate la alin. (8) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetică potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

Art. III. – Codul navigației maritime comerciale al Republicii Moldova, aprobat prin Legea nr. 599/1999 (Monitorul Oficial al Republicii Moldova, 2001, nr. 1–4, art. 2), cu modificările ulterioare, se completează cu articolul 9¹ cu următorul cuprins:

„Articolul 9¹. Asigurarea securității cibernetică
în navigația maritimă comercială

(1) Persoanele juridice care desfășoară navigație maritimă comercială ce ține de transportul de mărfuri și/sau de pasageri, căpitaniile porturilor, administrațiile porturilor maritime și întreprinderile și unitățile economice menționate la art. 80 alin. (2) din prezentul cod, precum și persoanele juridice care operează serviciul de trafic maritim, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de legea respectivă.

(2) Supravegherea și controlul de stat al respectării obligațiilor menționate la alin. (1) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetică, în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

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

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

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

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

„(1) În scopul asigurării securității sistemelor și resurselor informaționale de stat, autoritățile publice, instituțiile publice și alte entități de stat sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de Legea nr. 48/2023 privind securitatea cibernetică.”

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

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

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

1. Articolul 21 va avea următorul cuprins:

„**Art. 21.** – (1) În scopul asigurării securității și integrității rețelelor publice de comunicații electronice și a serviciilor de comunicații electronice accesibile publicului, furnizorii de rețele și/sau servicii de comunicații electronice accesibile publicului sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de Legea nr. 48/2023 privind securitatea cibernetică.

(2) Supravegherea și controlul de stat al respectării obligațiilor menționate la alin. (1) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.

(3) În exercitarea supravegherii și controlului de stat al respectării prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul legii respective, informează Agenția, în termen de 5 zile, despre încălcările constatate și, după caz, despre sancțiunile aplicate.”

2. Articolul 22 se abrogă.

Art. VI. – Compartimentul „**1. Lista organelor de control și domeniile aferente acestora**” 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 13¹ 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 prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a legii respective
-----------------	---------------------------------------	--

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

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

„(9) Societățile de investiții, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.

(10) Supravegherea și controlul de stat al respectării de către societățile de investiții a obligațiilor menționate la alin. (9) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

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

„(4) Operatorii de piață, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.

(5) Supravegherea și controlul de stat al respectării de către operatorii de piață a obligațiilor menționate la alin. (4) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

Art. VIII. – Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova (Monitorul Oficial al Republicii Moldova, 2013, nr. 238–242, art. 672), cu modificările ulterioare, se completează cu articolul 37¹ cu următorul cuprins:

„**Articolul 37¹.** 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 în calitate

de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de legea respectivă.

(2) Supravegherea și controlul de stat al respectării obligațiilor menționate la alin. (1) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetică în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

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

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

„e) autoritatea competentă la nivel național în domeniul securității cibernetică, în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a legii respective.”

2. Articolul 9¹ se completează cu alineatul (4) cu următorul cuprins:

„(4) Supravegherea și controlul de stat al respectării de către operatori a obligațiilor menționate la art. 15 alin. (3)¹ din prezenta lege sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetică potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

3. Articolul 15 se completează cu alineatul (3¹) cu următorul cuprins:

„(3¹) Operatorul, identificat în calitate de furnizor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, este responsabil de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de Legea nr. 48/2023 privind securitatea cibernetică.”

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 (7²) cu următorul cuprins:

„(7²) Furnizorii de servicii poștale, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetică prevăzute de legea respectivă. Supravegherea și controlul de stat al respectării obligațiilor menționate în prezentul alineat sunt exercitate de către autoritatea

competență la nivel național în domeniul securității cibernetice potrivit Legii nr. 48/2023 privind securitatea cibernetică.”

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

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

„(6) Persoanele juridice care desfășoară activități de gestionare a deșeurilor, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.”

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

„(5) Supravegherea și controlul de stat al respectării a de către persoanele juridice care desfășoară activități de gestionare a deșeurilor a obligațiilor menționate la art. 18 alin. (6) din prezenta lege, sunt exercitate 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 (1¹) și (1²) cu următorul cuprins:

„(1¹) Producătorii de dispozitive medicale, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.

(1²) Supravegherea și controlul de stat al respectării de către producătorii de dispozitive medicale a obligațiilor menționate la alin. (1¹) din prezentul articol sunt exercitate 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. La articolul 3, după noțiunea „luare de ostatici” se introduc două noțiuni noi cu următorul cuprins:

„obiectiv al infrastructurii critice – obiectiv de importanță vitală din domeniul administrației publice, al tehnologiei informației și comunicațiilor electronice, al comunicațiilor poștale, de infrastructură, din domeniul energiei, cel socioeconomic, al sănătății, al culturii și educației, al industriei, al ecologiei, din sistemul informațional al țării în ansamblu, din infrastructura complexului militar și de apărare sau a organelor apărării naționale, ale securității statului ori ale asigurării ordinii publice, ale cărui perturbare sau distrugere pot avea un impact negativ pentru siguranța, securitatea, bunăstarea socială și economică a statului, pot afecta anumite servicii esențiale, pot pune în pericol viața, sănătatea oamenilor și/sau pot avea efecte negative asupra mediului;

operator – minister, altă autoritate sau instituție publică, persoană juridică, indiferent de tipul de proprietate și forma juridică de organizare, care are în gestiune 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 operatori a obligațiilor privind asigurarea securității cibernetice prevăzute de Legea nr. 48/2023 privind securitatea cibernetică și de actele normative de punere în aplicare a legii respective sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu legea respectivă.

(2)² Autoritatea competentă indicată la alin. (2)¹ informează, în termen de 5 zile, Centrul Antiterorist despre încălcările legislației constatate în cadrul controlului exercitat asupra operatorilor vizând modul în care aceștia respectă obligațiile privind asigurarea securității cibernetice stabilite de actele normative menționate la alin. (2)¹.”

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

la alineatul (4), cuvintele „în conformitate cu prezenta lege și legile sectoriale” se substituie cu textul „în conformitate cu prezenta lege, cu legile sectoriale și cu alte legi”;

articolul se completează cu alineatele (7)¹ și (7)² cu următorul cuprins:

„(7)¹ Întreprinderile energetice, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt

responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.

(7²) Supravegherea și controlul de stat al respectării obligațiilor menționate la alin. (7¹) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

Art. XV. – Legea nr. 202/2017 privind activitatea băncilor (Monitorul Oficial al Republicii Moldova, 2017, nr. 434–439, art. 727), cu modificările ulterioare, se completează cu articolul 38² cu următorul cuprins:

„Articolul 38². Gestionarea riscurilor aferente tehnologiei informației și a comunicațiilor, securității informației și continuității activității

(1) Fiecare bancă trebuie să dispună de personal, de sisteme și de servicii eficiente în domeniul tehnologiei informației și a comunicațiilor (în continuare – TIC) care să asigure, proporțional cu natura, amploarea și complexitatea riscurilor inerente modelului de afaceri și activităților desfășurate de bancă, activitatea acesteia. În acest scop, banca stabilește competențe și responsabilități, aprobă și pune în aplicare o strategie privind TIC și securitatea informației, precum și planuri de acțiuni în vederea atingerii obiectivelor strategiei respective.

(2) Banca trebuie să instituie un cadru de administrare a continuității activității, în măsură să asigure capacitatea de funcționare în mod continuu, cu asigurarea protejării tuturor informațiilor, inclusiv în vederea limitării pierderilor de informații în cazul întreruperii severe activității. În acest scop, banca identifică riscurile aferente continuității activității la care este expusă și aprobă și pune în aplicare planuri de asigurare a continuității activității.

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

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

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

(6) Banca Națională a Moldovei stabilește în actele sale normative cerințele specifice privind punerea în aplicare a prevederilor alin. (1)–(5).

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

„(4) Obligația stabilită la alin. (3) din prezentul articol nu scutește participanții la schimbul de date, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, de îndeplinirea obligațiilor de notificarea prevăzute de legea respectivă.”

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

1. Articolul 17 alineatul (2) se completează cu litera b²) cu următorul cuprins:

„b²) pentru personalul din autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică – 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific;”.

2. La anexa nr. 3, notele de la tabelul 2 se completează cu punctul 18 cu următorul cuprins:

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

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

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

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

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

„(5) Supravegherea și controlul de stat al respectării obligațiilor stabilite la art. 12 alin. (6) din prezenta lege sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

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

„(6) Furnizorul unei substanțe sau al unui amestec chimic, identificat în calitate de furnizor de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, este responsabil de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.”

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 (14) cu următorul cuprins:

„(14) Întreprinderile din domeniul alimentar, identificate în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabile de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.”

2. Articolul 8 se completează cu alineatul (10) cu următorul cuprins:

„(10) Supravegherea și controlul de stat al respectării obligațiilor menționate la art. 7 alin. (13¹) din prezenta lege sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

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:

alineatul (1) va avea următorul cuprins:

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

articolul se completează cu alineatele (3) și (4) cu următorul cuprins:

„(3) Operatorii aeronautici și entitățile aeronautice, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.

(4) Supravegherea și controlul de stat al respectării obligațiilor specificate la alin. (3) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice în limitele stabilite de Legea nr. 48/2023 privind securitatea cibernetică.”

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 (5) cu următorul cuprins:

„(5) Supravegherea și controlul de stat al respectării obligațiilor menționate la art. 89 alin. (3¹) din prezenta lege sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice, în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.”

2. Articolul 89 se completează cu alineatul (3¹) cu următorul cuprins:

„(3¹) Administratorul infrastructurii și întreprinderile feroviare, identificați în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili de îndeplinirea obligațiilor privind asigurarea securității cibernetice prevăzute de legea respectivă.”

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 îndeplinesc obligațiile privind asigurarea securității cibernetice prevăzute de Legea nr. 48/2023 privind securitatea cibernetică.

(2) Supravegherea și controlul de stat al respectării obligațiilor menționate la alin. (1) din prezentul articol sunt exercitate de către autoritatea competentă la nivel național în domeniul securității cibernetice, în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică.

(3) În exercitarea supravegherii și controlului de stat al respectării de către prestatorii de servicii de încredere a prevederilor Legii nr. 48/2023 privind securitatea cibernetică, autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul legii respective, informează, în termen de 5 zile, organul de supraveghere și control despre încălcările constatate și, după caz, despre sancțiunile aplicate.”

Art. XXIII. – Prezenta lege intră în vigoare la data de 1 ianuarie 2025, cu excepția prevederilor art. XVII care intră în vigoare la data publicării prezentei legi în Monitorul Oficial al Republicii Moldova.

PREȘEDINTELE PARLAMENTULUI

SINTEZA
amendamentelor, propunerilor și obiecțiilor
la proiectul de Lege pentru modificarea unor acte normative
(modificarea cadrului legal în conformitate cu Legea nr.48/2023 privind securitatea cibernetică)
(nr.41 din 14.02.2024), lectura II.

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
1.	Direcția Generală Juridică a Secretariatului Parlamentului	<p>Potrivit Legii nr. 100/2017 cu privire la actele normative, reținem că, practica de elaborare a actelor normative, impune anumite rigori juridice, lingvistice și semantice, acestea urmând să asigure sistematizarea și unificarea actelor normative.</p> <p>Ca obiecție generală asupra proiectului de lege, relevăm necesitatea revizuirii formulilor de trimitere utilizate pe tot cuprinsul proiectului de lege, întru evitarea interpretărilor eronate a normelor proiectului, mai ales, în partea ce ține de stabilirea obligațiilor ce necesită a fi îndeplinite de către furnizorii de servicii identificați în temeiul Legii nr. 48/2023 privind securitatea cibernetică.</p> <p>Astfel, pentru a fi în corespundere cu prevederile art. 55 alin. (5) al Legii nr. 100/2017 și ale Metodologiei de tehnică legislativă aplicată la redactarea proiectelor de acte normative, aprobată prin Hotărârea Biroului permanent nr. 3/2022, care stipulează expres că, dacă trimiterile la alte acte normative sunt necesare acestea trebuie să desemneze actul normativ sau dispoziția concretă la care se face referire.</p> <p>Prin urmare, evidențiem următoarele formule utilizate în proiectul de lege: "în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi" (art. XIV pct. 1 din proiect); "actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetică" (art. I pct. I, art. II, art. III, art. IV, art. V pct. 1, art. VII pct. 1, art. VIII, art. IX pct.3, art. XI pct. 1, art. XII, art. XIV pct.2 , art. XVII pct. 2, art. XIX pct. 1, art. XX pct. 2, art. XXI pct. 2 și art. XXII din proiect). Rațiunea excluderii formulei subliniate mai sus, ca fiind de prisos, rezidă din prevederile Legii nr. 48/2023 și reiese însăși din obiectul de reglementare al acesteia, care la art. 1 stipulează expres că: "Prezenta lege</p>	Se acceptă.

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		<p>reglementează cadrul normativ, organizațional și de cooperare în domeniul securității cibernetice, stabilește competența autorităților și instituțiilor publice în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme în scopul asigurării securității rețelelor și sistemelor informatice, care sunt esențiale pentru funcționarea societății, și al gestionării incidentelor cibernetice.” Totodată, prevederile art. 11 alin. (4) lit. b) din Legea nr. 48/2023 stabilește că aceste cerințe specifice de securitate se aprobă de Guvern la propunerea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.</p> <p>Concludent, întru respectarea principiilor clarității și previzibilității, considerăm necesar excluderea formulei prezentate spre examinare, ca fiind de prisos.</p>	
2.	Direcția Generală Juridică a Secretariatului Parlamentului	<p>Pentru un spor de rigoare juridică și claritate normativă, recomandăm precizarea și uniformizarea noțiunii: autoritate competentă la nivel național în domeniul securității cibernetice, utilizată în proiect. Menționăm că, prin prisma proiectului de lege, sunt utilizate două formulări: autoritatea competentă în domeniul securității cibernetice și autoritatea competentă la nivel național în domeniul securității cibernetice funcției de supraveghere. Astfel, la aplicarea normei, pot apărea interpretări eronate în partea ce ține de exercitarea funcției de control și supraveghere a autorității vizate față de furnizorii de servicii identificați de aceasta.</p>	Se acceptă.
3.	Direcția Generală Juridică a Secretariatului Parlamentului	<p>La Art. V pct. 1, redacția alin.(3) a art. 21 din Legea comunicațiilor electronice nr. 241/2007, se atestă o formă repetitivă a normelor de trimitere. Autorul utilizează atât norma de trimitere - Legea nr. 48/2023, cât și formula – în temeiul acestei legi. Această obiecție este valabilă și pentru Art. XXII alin.(3) din proiect.</p>	Se acceptă.
4.	Direcția Generală Juridică a Secretariatului	<p>La Art. XII din proiect, reiterăm precizările expuse în expertiza juridică a Ministerului Justiției privind completarea Legii cu un articol distinct, privind asigurarea securității cibernetice de către producătorii de</p>	Cu titlu de precizare menționăm faptul lipsei de motivare a obiecției Ministerului Justiției, așa cu o cere

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
	Parlamentului	dispozitive medicale. Rațiunea observației rezidă din prevederile art. 63 alin.(2) din Legea nr. 100/2017, și presupune o condiție generală de modificare a actului normativ.	legea (art. 33 alin. (2), aceasta nu a fost acceptată, deoarece insistă pe o soluție care vine în contradicție cu prevederile art. 63 alin. (2). Or, vigilența dispozitivelor medicale, reieșind din conținutul acestui articol include gestionarea incidentelor și managementul riscurilor ce țin de utilizarea/ exploatarea dispozitivului medical. Articolul nu specifică categoria de incidente sau natura riscurilor. Ținând cont de faptul că acest domeniu este unul de criticalitate înaltă din perspectiva securității cibernetice, este evident că aceste categorii includ și gestionarea incidentelor cibernetice și managementul riscurilor de securitate cibernetică. Anume din această perspectivă completările propuse sunt cel mai indicat să fie efectuate anume la art. 16. Expunerea propunerilor de modificare a legii respective într-un articol separat, în viziunea noastră, este nejustificată atât din punct de vedere formal tehnico-legislativ, cât și din punctul de vedere al conținutului și fondului de reglementare al acestor propuneri.
5.	Direcția Generală Juridică a Secretariatului Parlamentului	La Art. XV, ce presupune modificarea Legii nr. 202/2017, art. 38 ² alin.(2) verbele se vor utiliza la timpul prezent. Suplimentar, norma de trimitere menționată la alin.(7) "actul normativ menționat la alin.(6)", pentru o rigoare sporită, se va reda în formula: "cerințelor specifice	Se acceptă. Suplimentar, în contextul fondului observațiilor de mai sus ale Direcției Juridice a Secretariatului

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		menționate la alin.(6)". Această obiecție este valabilă și pentru alineatul (8).	Parlamentului, textul „actul normativ prevăzut la alineatul (6) și actele normative de punere în aplicare a” a fost înlocuit cu textul „prevederile prezentei legi și ale”.
6.	Direcția Generală Juridică a Secretariatului Parlamentului	<p>Cu referință la Art. XVII, ce privește stabilirea pentru personalul Agenției pentru Securitate Cibernetică a sporului cu caracter specific în mărime de 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific, plus majorarea claselor de salarizare cu: 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”, și cu 25 de clase succesive – pentru funcțiile publice de execuție, apreciem ca fiind o acțiune excesivă și nejustificată, în raport cu alte categorii de personal din serviciul public.</p> <p>În susținerea concluziei date, reținem și constatările expuse în expertiza anticorupție, care a subliniat asupra respectării principiului: nediscriminare, echitate și coerență, în sensul asigurării tratamentului egal și a remunerării egale pentru muncă de valoare egală din Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar.</p> <p>Principial, reiterăm că Legea nr. 270/2018, prevede că sistemul unitar de salarizare presupune de asemenea și respectarea principiilor: transparenței și sustenabilității financiare. În acest sens, transparența presupune că mecanismul de stabilire a salariilor și a altor drepturi de natură salarială face parte din categoria informațiilor de interes public, iar nota informativă nu demonstrează că raportul sarcinilor și obiectivelor entității în raport cu alte autorități publice, este substanțial mai superior. Prin urmare, pentru a nu crea inechitate între personalul altor instituții bugetare care activează în condiții similare, considerăm necesară revizuirea acesteia.</p>	<p>O provocare serioasă în asigurarea eficienței în funcționarea unei astfel de entități este salarizarea personalului, iar admiterea unei discrepante mari între angajații Agenției ar putea periclita atingerea obiectivelor pentru care aceasta a fost instituită.</p> <p>În acest sens, 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</p>

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
			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 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”.
7.	Banca Națională a Moldovei (scr.nr.31-002/13/878)	<p>Cu referire la proiectul de lege pentru modificarea unor acte normative (aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibernetică), număr unic 957/MDED/2023, remis spre reexaminare prin scrisoarea Ministerului Dezvoltării Economice și Digitalizării al Republicii Moldova nr. 11/2-48 din 03.01.2024, Banca Națională a Moldovei (BNM) supune atenției Dvs următoarele:</p> <p>Art. 2 (2) din Directiva (UE) 2022/2555 consacră aplicabilitatea acesteia entităților administrației publice („Indiferent de dimensiunea lor, prezenta directivă se aplică, de asemenea, entităților de tipul celor menționate în anexa I sau II, în cazul în care:... entitatea este o entitate a administrației publice”). Totodată, potrivit art. 6 pct. 35 din Directivă, termenul de entitate a administrației publice nu include băncile centrale („entitate a administrației publice” înseamnă o entitate recunoscută ca atare într-un stat membru în conformitate cu dreptul intern, cu excepția sistemului judiciar, a parlamentelor și a băncilor centrale”). Corespunzător, Directiva 2022/2555 exceptează expres băncile centrale din domeniul de aplicare a acesteia.</p>	<p>Precizăm că băncile centrale nu sunt excluse „expres” din domeniul de aplicare al Directivei NIS2. Punctul 35 al art. 6 din directiva respectivă exclude aceste entități, de rând cu parlamentele și autoritățile din sistemul judiciar din noțiunea de „entitate a administrației publice”.</p> <p>În ce privește argumentarea anterioară la opinia BNM de excludere a acesteia din domeniul de aplicare al Legii nr. 48/2023, relevăm că argumentarea precum că armonizarea parțială a legislației naționale a stat la baza neaplicării prevederilor pct. 35 din art. 6 al Directivei NIS2 este una eronată. Este probabil ca această interpretare inexactă să fie datorată mai degrabă tendinței autorului proiectului de a</p>

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		<p>Potrivit argumentelor autorilor proiectului, enunțate în sinteza propunerilor, recomandărilor și obiecțiilor, prevederile art. 6 pct. 35 din Directiva 2022/2555 nu au fost transpuse în Legea 48/2023 din motiv că prin această lege s-a urmărit obiectivul de transpunere parțială (și nu deplină) a prevederilor Directivei (UE) 2022/2555. Având în vedere impactul anticipat al Legii 48/2023, în redacția curentă, asupra autonomiei BNM (cel puțin în virtutea competențelor extensive de solicitare informații, supraveghere și control deținute de autoritatea competentă la nivel național în domeniul securității cibernetice), pe de o parte, precum și necesitatea de armonizare deplină a sistemului juridic național cu legislația Uniunii Europene, în lumina deciziei Consiliului European din 14 decembrie 2023, pe de altă parte, opinăm că este importantă, la această etapă, transpunerea integrală a prevederilor Directivei (UE) 2022/2555, care au fost omise la etapa de elaborare a proiectului de lege privind securitatea. Totodată, ținând cont de obiectivul comun de asigurare a unui cadru național uniform și robust de asigurare a securității cibernetice, precum și în vederea asigurării capacității Agenției Naționale de Securitate Cibernetică (ANSC) de a accesa informațiile necesare pentru realizarea atribuțiilor acesteia, propunem introducerea în Legea nr. 48/2023 a unor prevederi care stabilesc modul și condițiile în care are loc schimbul de informații dintre BNM și ANSC. Drept reper pot servi prevederile art. 12 alin. (9) din Legea nr. 618/1995 securității statului, potrivit cărora „...Banca Națională a Moldovei furnizează informații și date în condițiile unui acord încheiat cu Consiliul Suprem de Securitate...”.</p>	<p>argumenta de o manieră mai generală neacceptarea unei astfel de excepții. Caracterul parțial de armonizarea a legislației țării noastre la prevederile Directivei NIS2 este o premisă necesară emiterii raționamentului conform căruia excepția băncilor centrale de la prevederile Directivei NIS2 nu poate fi extrapolată la nivel național, deoarece Republica Moldova nu este un stat membru al UE și, prin urmare BNM nu este parte a sistemului european de supraveghere a băncilor centrale oferit de cadrul normativ existent la nivel supranațional al UE. În concluzie, această excepție va putea fi operată doar atunci când, dat fiind statutul de stat membru al UE, R. Moldova va transpune integral nu doar Directiva NIS2, dar și Regulamentul DORA și, mai ales, alte acte legislative europene relevante atât domeniului financiar bancar, cât și celui de securitate cibernetică cu incidență în acest sector.</p> <p>De asemenea, inclusiv în contextul celor expuse mai sus relevăm și principiul armonizării minime, statuat de art. 5 al Directivei NIS2. Deși acesta este aplicabil statelor membre ale UE, totuși extrapolarea acestuia Republicii Moldova ar trebui</p>

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
			realizată cel puțin pentru perioada de până la armonizarea legislației naționale la actele UE în domeniul asigurării rezilienței cibernetice a sistemului financiar-bancar, în mod special al celor care reglementează supravegherea modului în care BNM asigură implementarea adecvată a măsurilor de securitate a rețelelor și sistemelor informatice pe care le utilizează la prestarea serviciilor sau desfășurarea activităților care sunt esențiale pentru susținerea unor activități societale și economice critice și perturbarea cărora ar putea afecta semnificativ nu doar valorile menționate mai sus, ci și securitatea națională.
8.	Banca Națională a Moldovei (scr.nr.31-002/13/878)	Cu referire la conținutul proiectului de lege, având în vedere finalitatea urmărită de acest proiect, și anume asigurarea interconexiunii dintre normele Legii nr. 48/2023 și cele cuprinse în legile care reglementează activitatea viitorilor furnizori de servicii și eliminarea/revizuirea unor prevederi care ar putea suscita interpretări echivoce sau contradictorii în procesul aplicării legii, observăm că rămâne incert, în procesul de supraveghere a asigurării securității cibernetice, modul în care vor fi delimitate competențele de supraveghere și control ale autorității competente la nivel național în domeniul securității cibernetice, de cele ale autorităților care reglementează și supraveghează propriu-zis un anumit sector/subsector critic. Observăm, că riscul potențialelor conflicte negative sau pozitive de competențe dintre BNM și autoritatea competentă la nivel național în domeniul securității cibernetice au fost semnalate și de autorii proiectului, care la pct. 16 subpct. 23) din sinteza propunerilor/recomandărilor și obiecțiilor au	Cu titlu de precizare menționăm că în principiu, opinia BNM pe marginea proiectului de lege prezentat spre avizare și, implicit, asupra unor prevederi ale Legii nr. 48/2023 privind securitatea cibernetică sunt pertinente problematicii finalizării constituirii în Republica Moldova a unui model de guvernare în domeniul securității cibernetice care să corespundă principiilor eficienței și eficacității, principii care în ultimă instanță trebuie să asigure o astfel de funcționalitate a entităților responsabile care să aibă ca efect, pe

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		<p>remarcat că: „[...] Agenția de Securitate Cibernetică ... urmează, în comun cu Banca Națională a Moldovei să fie identificate mecanisme fiabile de coordonare a eforturilor în procesul de asigurare a respectării prevederilor acestei legi. Mecanismele respective bineînțeles urmează să asigure evitarea suprapunerii de competențe dintre BNM și ANSC și, cu atât mai mult intrusiunile reciproce nejustificate”. Înțelegem că un astfel de mecanism urmează a fi identificat nu doar pentru sectorul bancar, dar și pentru toate sectoarele supravegheate de către autoritatea competentă la nivel național în domeniul securității cibernetice în vederea asigurării respectării prevederilor Legii nr. 48/2023. Propunem în acest sens, identificarea unui mecanism unic reglementat prin lege și manifestăm disponibilitate pentru conlucrare în vederea atingerii acestui obiectiv.</p>	<p>termen mediu și lung, creșterea continuă a rezilienței cibernetice în țara noastră.</p> <p>Reiterăm că din perspectiva exercițiului de către Agenția de Securitate Cibernetică a funcției de supraveghere și control, pentru punerea în aplicare a prevederilor Legii nr. 48/2023 prin reglementarea modului de supraveghere și control al respectării acestei legi, urmează, în comun cu Banca Națională a Moldovei să fie identificate mecanisme fiabile de coordonare a eforturilor în procesul de asigurare a respectării prevederilor acestei legi. Mecanismele respective bineînțeles urmează să asigure evitarea suprapunerii de competențe dintre BNM și ASC și, cu atât mai mult intrusiunile reciproce nejustificate.</p>
9.	<p>Banca Națională a Moldovei (scr.nr.31-002/13/878)</p>	<p>Suplimentar, cu privire la excluderea din proiectul de lege a modificărilor propuse la Legea nr. 202/2017 privind activitatea băncilor (Legea nr. 202/2017), observăm că autorul în sinteza propunerilor/recomandărilor și obiecțiilor la proiectul de lege, menționează că: „în consecință prevederile Legii 48/2023 vor trebui aplicate în măsura în care anumite situații juridice nu sunt reglementate, inclusiv prin prisma principiilor enunțate la art. 3 alin. (5) din Legea nr. 48/2023, de legislația sectorială cu caracter special”. Menționăm în acest context că, actualmente Legea nr. 202/2017 conține unele prevederi generale cu privire la asigurarea securității cibernetice de către bănci (a se vedea, spre exemplu, art. 38, care stabilește cerințele față de cadrul de administrare al unei bănci din</p>	<p>Cu titlu de precizare menționăm că în situația în care legile sectoriale în domeniul financiar bancar vor stabili cerințe de securitate și obligații de notificare cel puțin echivalente cu cele prevăzute de Legea nr. 48/2023 și actele de punere a acestora în aplicare, atunci legile sectoriale bineînțeles vor fi cele care vor reglementa raporturile juridice respective.</p> <p>Din considerentele expuse mai sus este eronat să considerăm că Directiva</p>

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		<p>perspectiva desfășurării activității acesteia în condiții de asigurare a unei gestiuni efective și prudente a tuturor riscurilor inclusiv, dar fără a se limita la riscul tehnologiilor informaționale și de comunicare). Menționăm că, prevederi detaliate privind gestionarea riscului tehnologiilor informaționale și de comunicare se regăsesc în reglementările secundare ale BNM, spre exemplu, Regulamentul nr. 47/2018 privind cerințele minime pentru sistemele informaționale și de comunicare ale băncilor. Totodată, având în vedere că art. 3 alin. (5) din Legea nr.48/2023 condiționează aplicarea directă a prevederilor derogatorii ce țin de asigurarea securității cibernetice - de reglementarea acestora prin lege (și nu prin act subordonat legii), înțelegem că modul și măsura în care acest regulament va fi aplicabil băncilor, odată cu intrarea în vigoare a Legii nr. 48/2023, rămân a fi interpretabile.</p> <p>În această ordine de idei, supunem atenției Dvs. faptul, că BNM este în proces de promovare a proiectului de lege nr. 988/MF/BNM/2023, prin care se completează Legea nr. 202/2017 cu un articol care instituie reglementări detaliate privind administrarea riscurilor aferente tehnologiilor informaționale și de comunicare, de securitate a informației și continuitatea activității, cu următorul cuprins: "Articolul 38². Administrarea riscurilor aferente tehnologiilor informaționale și de comunicare, de securitate a informației și continuitatea activității (1) Fiecare bancă trebuie să dispună de personal, sisteme și servicii eficiente aferente tehnologiilor informaționale și de comunicare (TIC) ce asigură, de o manieră proporțională cu natura, amploarea și complexitatea riscurilor inerente activităților și modelului de afaceri, desfășurarea activităților băncii. În acest scop, banca va stabili roluri și responsabilități, va aproba și pune în aplicare o strategie TIC și de securitate a informației și planuri de acțiuni în vederea atingerii obiectivelor acesteia.</p> <p>(2) Banca trebuie să stabilească un cadru de administrare a continuității activității capabil să asigure capacitatea de a funcționa în</p>	<p>NIS2 exceptează expres entitățile financiare din domeniul său de aplicare. Din contra, aceste entități urmează a fi identificate ca atare nu doar în baza Directivei NIS2, ci și a Directivei privind reziliența entităților critice (așa-numita Directiva CER). Astfel, nici art. 4 alin. 1 din Directiva NIS, nici recitalul (28) din preambulul la această Directivă nu exclud entitățile financiare din sfera de aplicare a Directivei NIS2. Aceste prevederi doar stabilesc principiile de aplicare a legislației, în mod special raportul dintre legea specială și cea generală. În același context, este important de remarcat faptul că în procesul de identificare a furnizorilor de servicii și exercitare a supravegherii modului cum aceștia implementează legea, autoritatea competentă în temeiul Legii nr. 48/2023 urmează să determine echivalența și implicit aplicabilitatea reglementărilor sectoriale în raport cu cele ale Legii nr. 48/2023 și să acționeze în consecință.</p> <p>Totodată, în cadrul examinării proiectului în ședința din 21.03.2024, Comisia a acceptat propunerea parvenită din partea autorilor proiectului și anume de a exclude din</p>

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		<p>mod continuu cu asigurarea protejării tuturor informațiilor critice, inclusiv, în vederea limitării pierderilor în cazul unei întreruperi severe a activității. În acest scop, banca va identifica riscurile de continuitate la care este expusă și va aproba și pune în aplicare planuri de asigurare a continuității activității.</p> <p>(3) Banca trebuie să dispună de un cadru de administrare a riscurilor aferente TIC și de securitate a informației care să conțină procese și proceduri pentru a asigura identificarea, analiza, evaluarea, diminuarea, monitorizarea, raportarea și menținerea riscurilor în limitele apetitului la risc al băncii.</p> <p>(4) Banca trebuie să dispună de un cadru de administrare a securității informației care trebuie să definească principiile, normele și modalitățile de protejare a confidențialității, integrității și disponibilității datelor și informației băncii și ale clienților acesteia, instituind în baza acestuia măsuri pentru diminuarea nivelurilor riscurilor TIC și de securitate a informației la care este expusă.</p> <p>(5) Banca trebuie să stabilească procese de revizuire a riscurilor, de testare a securității informației și continuității activității care să valideze eficacitatea măsurilor de control și aplicabilitatea planurilor de asigurare a continuității activității.</p> <p>(6) Cerințe specifice privind punerea în aplicare a alin.(1)-(5) sunt stabilite în actele normative ale Băncii Naționale.”</p> <p>Propunem includerea acestor prevederi în proiect, pentru a soluționa, parțial, problematica aplicabilității reglementărilor speciale în materie de securitate cibernetică în domeniul bancar și a competențelor corelative ale BNM de a urmări respectarea acestora.</p>	<p>Art.XV ce completează Legea nr. 202/2017 privind activitatea băncilor cu articol nou 38² a alin.(7) și (8). Astfel, textul următor se exclude din proiect:</p> <p>”(7) În măsura în care gestionarea riscurilor TIC, de securitate a informației și de continuitate a activității nu este reglementată de dispozițiile prezentei legi și cerințele specifice menționate la alineatul (6), acestea se completează cu prevederile Legii nr. 48/2023 privind securitatea cibernetică și de actele normative de punere a acesteia în aplicare.</p> <p>(8) Supravegherea și controlul modului în care băncile realizează obligațiile stabilite de prezentul articol se exercită de către autoritatea competentă la nivel național în domeniul securității cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Banca Națională a Moldovei, în conformitate cu prevederile prezentei legi și ale Legii nr. 48/2023 privind securitatea cibernetică.”</p>
10.	Banca Națională a Moldovei (scr.nr.31-002/13/878)	Suplimentar, cu referire la completarea Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat cu art. 77 (păstrarea informațiilor din cadrul sistemelor și resurselor informaționale de stat în afara teritoriului Republicii Moldova), propunem a se preciza aplicabilitatea acestui articol în raport cu	Cu titlu de precizare menționăm faptul că în redacția finală completare cu art. 77 a fost exclusă, dar a fost introdusă completare a atribuțiilor Guvernului cu litera e) la art.22,

Nr. crt.	Autorul amendamentului	Conținutul amendamentului, propunerii, obiecției	Decizia Comisiei sesizate în fond
I.	II.	III.	IV.
		<p>autoritățile publice autonome care gestionează în mod independent sistemele și resursele informaționale deținute. În acest sens, menționăm că BNM, în procesul de gestionare independentă a sistemelor sale informaționale, utilizează serviciile Cloud pentru realizarea copiilor de rezervă criptate ale sistemelor informaționale și pentru stocarea acestora în Cloud, asigurând astfel capacitatea de restabilire rapidă în caz de incident major. De asemenea, BNM utilizează aplicații bazate pe Cloud, precum M365, ZOOM Meetings, Microsoft Teams (ș.a.), precum și tehnologii emergente cloud-enabled, inclusiv soluții pilot AI/ML/LLM, care sunt esențiale pentru progresul și inovația în activitatea BNM. Ținem să evidențiem că utilizarea serviciilor Cloud de către BNM se bazează pe o înțelegere profundă și o evaluare riguroasă a tuturor riscurilor implicate (riscurile operaționale, riscurile legate de continuitatea afacerii, riscurile de securitate a informației, riscurile aferente protecției datelor cu caracter personal) și se desfășoară conform celor mai bune practici și standarde internaționale, pentru a asigura ca orice utilizare a tehnologiei Cloud să fie securizată și aliniată obiectivelor strategice de securitate cibernetică și de continuitate operațională.</p> <p>Adițional, observăm că potrivit art. 77 din Legea nr. 467/2003, păstrarea informațiilor din cadrul sistemelor și resurselor informaționale de stat în afara teritoriului Republicii Moldova se realizează în baza unui acord interguvernamental. În acest context, având în vedere, pe de o parte, durata procedurilor de încheiere a acordurilor interguvernamentale, dar și necesitatea asigurării disponibilității serviciilor Cloud în termeni proximi, solicităm respectuos informații privind acordurile în vigoare, care corespund prevederilor art. 77 din Legea nr. 467/2003, precum și informații privind termenele estimative propuse pentru încheierea acestor categorii de acorduri.</p>	<p>agreată cu SIS, în următoare redacție: „e) aprobă regulile și modul de găzduire a sistemelor și resurselor informaționale de stat în cadrul centrelor de date amplasate în Republica Moldova sau pe teritoriul statelor membre ale Uniunii Europene”.</p>

Lilian CARP
Președintele Comisiei

