SINTEZA

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

AVIZARE

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

REAVIZARE

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

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

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

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

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

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

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

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

[5] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

			de control şi supraveghere noi ale Agenţiei, este important să se clarifice impactul potenţial al controlului în raport cu alte soluţii mai puţin invazive.	nivel naţional, pentru toţi furnizorii de servicii identificaţi. Este important de subliniat că aceste estimări sunt realizate în baza datelor europene disponibile şi că, pentru o imagine mai precisă, este necesară colectarea şi analiza datelor specifice Republicii Moldova în ceea ce priveşte incidentele semnificative. Toate aceste date vor fi disponibile odată cu operaţionalizarea activităţii Agenţiei pentru Securitate Cibernetică, după o perioadă anumită de timp de implementare a prevederilor legale, inclusiv în contextul exercitării de către această entitate a funcţiei de cercetare şi dezvoltare. Cât priveşte precizările normative efectuate în Legea nr. 131/2012 privind controlul de stat asupra activităţii de întreprinzător, care cuprinde lista organelor de control şi domeniile aferente acestora cu o poziţie nouă dedicată Agenţiei pentru Securitate Cibernetică, urmează de subliniat că aceasta nu poate fi interpretată ca o opţiune, ci ca o obligaţie. Acest aspect devine evident având în vedere prevederile art. 7 alin. (3) lit. e) din Legea nr. 48/2023 privind securitatea cibernetică, care stabileşte că autoritatea competentă în domeniul securităţii cibernetice este însărcinată să exercite funcţiile de supraveghere şi control de stat asupra modului în care furnizorii de servicii respectă obligaţiile impuse de legea menţionată.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Ședința interinstituțională

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

			că, obiecții de ordin conceptual nu avem de formulat. Totodată, aferent rigorilor de tehnică legislativă, este recomandabil, ca în cazul completării articolelor cu noi elemente structurale (în cazul dat, alineate), acestora să li se atribuie numere în ordine consecutivă, dar nu numere cu indice, or, numerotarea elementelor structurale cu indicii respectivi se efectuează doar în cazul completării în interior a unui șir numeric (pct. 1-3 din Art. I; Art. II; pct. 1 și 2 din Art. VII; pct. 1 și 2 din Art. IX; pct. 1 și 2 din Art. XI; Art. XII; Art. XV; Art. XVII; pct. 2 din Art. XIX).	
2	**CNPF** **Ministerul Finanțelor**		Propune o nouă redacție a art. VII: **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, care prestează activitatea stabilită la art. 33 alin. (1) lit. h), 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 respectivei legi, actelor normative de punere a acesteia în aplicare, precum și pentru respectarea cerințelor specifice de asigurare a securității cibernetice stabilite de prezenta lege și de actele normative ale Comisiei Naționale.	**Se acceptă parțial.** S-a acceptat doar propunerea de a diviza în alineate distincte reglementările privind responsabilitatea pentru realizarea obligațiilor de asigurare a securității cibernetice, pe de o parte, și, pe de altă parte, a competenței de exercitare a funcției de supraveghere și control de către autoritatea competentă la nivel național. În rest propunerile nu au fost acceptate din următoarele considerente, după cum urmează: **a. referitor la redacția alin. (9) al art. 41** ***propunerea de completare cu cuvintele „care prestează activitatea stabilită la art. 33 alin. (1) lit. h)”*** implică riscuri pentru implementarea ulterioară corespunzătoare a prevederilor legale, în mod special a celor de identificare a furnizorilor de servicii conform Legii nr. 48/2023 privind securitatea cibernetică. Redacția actuală a acestui alineat, propus de MDED în

			(10) Supravegherea şi controlul modului în care sunt îndeplinite obligaţiile stipulate la alin. (9) se realizează de către autoritatea competentă la nivel naţional în domeniul securităţii cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Comisia Naţională, în conformitate cu actele normative ale Comisiei Naţionale şi actele normative de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică.". 2. Articolul 62 se completează cu alineatele (4) şi (5) cu următorul cuprins: „(4) Operatorii de piaţă, identificaţi în calitate de furnizori de servicii în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică, sunt responsabili pentru îndeplinirea obligaţiilor care le revin conform respectivei legi, conform actelor normative de punere a acesteia în aplicare, precum şi pentru respectarea cerinţelor specifice de asigurare a securităţii cibernetice stabilite de prezenta lege şi de actele normative ale Comisiei Naţionale. (5) Supravegherea şi controlul de stat al modului în care operatorii de piaţă îndeplinesc obligaţiile stabilite la alin. (4) se realizează de către autoritatea competentă la nivel naţional în domeniul securităţii cibernetice, desemnată în temeiul Legii nr. 48/2023 privind securitatea cibernetică, în cooperare cu Comisia Naţională, în conformitate cu actele normative ale Comisiei Naţionale şi actele normative de	proiectul de lege, are ca obiectiv interconexiunea acestei legi cu Legea nr. 48/2023 şi excluderea eventualelor interpretări deficitare în ce priveşte obligaţiile şi competenţa. Totuşi, norma este formulată generic, determinând doar categoria entităţilor (societăţi pe acţiuni), fără activităţile/serviciile pe care le prestează. Această marjă discreţionară este necesară, deoarece cadrul metodologic de identificare şi tipologia specifică a furnizorilor de servicii urmează a fi încă aprobată de Guvern. Ulterior, în baza acestui cadru normativ Agenţia pentru Securitate Cibernetică va determina care societăţi de investiţii sunt furnizori de servicii în sensul Legii nr. 48/2023. Prin urmare, considerăm îngustarea marjei de acţiune a autorităţii competente destul de riscantă în contextul în care nu putem anticipa care va fi abordarea metodologică în identificarea acestui tip de entităţi. b) **referitor la redacţiile alin. (9) al art. 41 şi alin. (4) al art. 62** ***propunerea de completare cu textul „precum şi pentru respectarea cerinţelor specifice de asigurare a securităţii cibernetice stabilite de prezenta lege şi de actele normative ale Comisiei Naţionale",*** în contextul în care normele de completare propuse la Legea nr. 174/2012 au ca scop conexiunea cu Legea nr.48/2023 şi excluderea ambiguităţilor în interpretare, pe de o parte dublează prevederile însăşi a legii care se propune a fi completată – Legea nr. 174/2012: completarea acestei legi cu norme de trimitere la Legea nr. 48/2023, nu

			punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică.	anulează obligativitatea executarea prevederilor legii sectoriale în speță de către categoriile respective de entități; pe de altă parte, această completare aria de acte normative și reglementări acre ar putea conține reglementări și cerințe specifice de securitate cibernetică și a informației. Din aceste considerente, redacția actuală a proiectului corespunde atât din punctul de vedere al efectelor pe care le produce și a obiectivelor normelor juridice, dar și din perspectiva normelor de tehnică legislativă. **c) referitor la redacțiile alin. (10) al art. 41 și alin. (5) al art. 62** ***propunerea de completare cu textul în cooperare cu Comisia Națională, în conformitate cu actele normative ale Comisiei Naționale și actele normative de punere în aplicare a Legii nr. 48/2023 privind securitatea cibernetică,*** este în primul rând în contradicție cu prevederile Legii nr. 48/2023, Agenția pentru Securitate Cibernetică va avea competență exclusivă de supraveghere și control al modului cum sunt respectate prevederile Legii nr. 48/2023, și nu Comisia Națională a Pieței Financiare. În al doilea rând, funcția de supraveghere și control, Agenția o va exercita exclusiv și în mod primordial în temeiul Legii 48/2023 și nu doar a cadrului normativ de punere în aplicare a acesteia. Or, acesta din urmă a priori se prezumă că este conform limitelor legale stabilite.

Secretar de stat

Digitally signed by Lupaşcu Mihai
Date: 2024.02.08 17:20:18 EET
Reason: MoldSign Signature
Location: Moldova

Mihai LUPAȘCU