RAPORT DE EXPERTIZĂ

La proiectul Lege pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică)

Tipul actului vizat de proiect:

Înregistrat cu nr.

Domeniul:

din:

I. EVALUAREA GENERALĂ

1. Autor al actului normativ este Guvernul , autor nemijlocit - Ministerul Dezvoltării Economice și Digitalizării

2. Categoria actului normativ propus: Lege organică , ceea ce corespunde/nu corespunde art.72 din Constituţie şi Legii 100/2017 privind actele normative.

Proiectul de lege este promovat în calitate de lege organică, categorie de lege care corespunde exigențelor art. 72 alin. (3) lit.c) din Constituție şi Legii 100/2017 privind actele normative.

Expertul nu are obiecţii la categoria actului

3. Scopul promovării proiectului

Conform Notei informative, elaborarea proiectului de lege cu privire la modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică) are ca obiectiv general aducerea în concordanță a cadrului normativ conex/aferent cu Legea nr. 48/2023 privind securitatea cibernetică. Este de remarcat că, temeiul juridic este cuprins în dispozițiile cu caracter tranzitoriu cuprinse la alin. (2) al art. 23 din Legea nr. 48/2023.

Potrivit reglementărilor din Legea nr. 48/2023 privind securitatea cibernetică în vederea punerii în aplicarea a Legii sunt necesare intervenții în partea ce ține de:
- modul de aplicare a măsurilor de supraveghere de către autoritatea competentă;
- modul de realizarea a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 19 alin. (5));
- asigurarea interconexiunii dintre normele Legii nr. 48/2023 privind securitatea cibernetică și cele cuprinse în Legile sectoriale carea reglementează activitatea viitorilor furnizori de serviciii și eliminarea/revizuirea unor

prevederi care ar putea suscita interpretări echivoce sau contracdictorii în procesul aplicării Legii;
- finalizarea instituirii cadrului normativ primar necesar stabilirii modelului de guvernanță în domeniul securității cibernetice la nivel național.

Temeiul reglementării domeniului securitatea cibernetică, a constituit legislația Uniunii Europene inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană. Ținem să precizăm că Legea nr. 48/2023 armonizează parțial cadrul normativ la prevederile Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de Securitate cibernetică în Uniune, de modifiicare a Regulamentului UE nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148, și a unor elemente esențiale ale Directivei (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de Securitate arețelelor și a sistemelor informatice în Uniune.

4. Respectarea transparenței decizionale

Potrivit prevederilor art. 32 alin. (1) din Legea nr. 100/2017 cu privire la actele normative, proiectul actului normativ, însoţit de Nota informativă, se transmite spre avizare autorităţilor publice responsabile de implementarea prevederilor conţinute în proiect, instituţiilor interesate, precum şi reprezentanţilor societăţii civile, care întocmesc şi prezintă autorului proiectului de lege avizele la proiect în modul stabilit de Legea nr.239/2008 privind transparenţa în procesul decizional.

Art. 8 din Legea nr. 239/2008 privind transparența în procesul decizional, reglementează expres etapele de asigurare a transparenței în procesul decizional. Din analiza materialelor aferente proiectului de lege, se constată că anunțul cu privire la elaborarea proiectului de decizie a fost plasat pentru informare pe pagina web oficială a autorității publice: www.mded.gov.md , la data de 15 septembrie 2023, fiind indicat termenul limită pentru recepționarea recomandărilor la 26 septembrie 2023, precum și datele de contact ale persoanei responsabile de elaborarea și promovarea proiectului.

Proiectul și materialele aferente au fost plasate pentru consultarea publică pe pagina web oficială a autorității, cât și pe portalul guvernamental de consultări publice www.particip.gov.md , la data de 09 noiembrie 2023, cu stabilirea termenului limită de recepționare a recomandărilor pana la 22 noiembrie 2023, adică 10 zile lucrătoare, fapt ce corespunde prevederilor art.12 alin.(2) din Legea nr. 239/2008 privind transparența în procesul decizional.

Apreciind acțiunile autorului de asigurarea a accesului părților interesate la proiect, precum și stabilirea unui termen optim pentru recepționarea propunerilor de modificare/completare a proiectului de lege, se constată că prevederile de asigurare a transparenței decizionale statuate în Legea nr. 239/2008, au fost respectate de către autor.

Etapele transparenței procesului decizional nu au fost respectate

Termenele de plasare și consultare a proiectului au fost respectate

Sinteza recomandărilor pe pagina web a autorului a fost plasata

II. FUNDAMENTAREA PROIECTULUI

5. Structura notei informative

Nota informativă corespunde structurii

6. Suficienţa argumentării.

În conformitate cu art.30 al Legii nr.100/2017 cu privire la actele normative, proiectele de acte normative sunt însoțite de nota informativă care cuprinde:
a) denumirea sau numele autorului și, după caz, a participanților la elaborarea proiectului actului normativ;
b) condițiile ce au impus elaborarea proiectului actului normativ și finalitățile urmărite;
c) descrierea gradului de compatibilitate, pentru proiectele care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene;
d) principalele prevederi ale proiectului și evidențierea elementelor noi;
f) modul de încorporare a actului în cadrul normativ în vigoare”.

Argumentele invocate de autor în Nota informative, în mare parte justifică necesitatea elaborării proiectului, fiind întrunite astfel parțial cerințele art.30 al Legii nr.100/2017 cu privire la actele normative.

Urmare a examinării Notei informative și a prevederilor proiectului se constată insuficienta argumentării necesității de stabilire a sporului cu caracter specific pentru subdiviziunile de suport din cadrul Agentiei pentru Securitate Cibernetica. Potrivit normei de la art.XVII pct.l și 2 din proiect se stabileste sporul cu caracter specific de 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific, plus majorarea claselor de salarizare cu: 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”, și cu 25 de clase succesive – pentru funcțiile publice de execuție - apreciem ca fiind o acțiune excesivă și nejustificată, în raport cu alte categorii de personal din serviciul public.

Reieșind din faptul că autoritatea competentă a fost creată recent prin Hotărârea Guvernului nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică și aprobare a Regulamentului cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică, iar Legea nr. 48/2023 urmează să intre în vigoare la data de 1.01.2025, reținem asupra respectării principiului: nediscriminare, echitate şi coerență, în sensul asigurării tratamentului egal și a remunerării egale pentru muncă de valoare egală din Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar.

Fără desfășurarea de activitate propriu zisă a autorității competente și fără o evaluare a performanțelor profesionale individuale ale personalului în raport cu cerințele posturilor, așa precum sunt reglementate în Regulamentul cu privire la tipurile și modul de stabilire a sporurilor cu caracter specific (aprobat prin Hotărîrea Guvernului nr. 1231/2018), stabilirea unui spor cu caracter specific pentru subdiviziunile de suport din cadrul Agentiei pentru Securitate Cibernetică de 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific, se consideră excesivă în raport cu alte categorii de funcționari publici.

Suplimentar, majorarea claselor de salarizare cu: 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”, și cu 25 de clase succesive – pentru funcțiile publice de execuție fără ca să poată fi demonstart că raportul sarcinilor și obiectivelor stabilite este net superior și complexitatea competențelor solicitate, aportul intelectual necesar, gradul de angajare, responsabilitățile, precum și nivelul instituției în ierarhia autorităților statului poate crea un dezechilibru între puteri, iar la stabilirea nivelului de salarizare urmează să fie examinate condițiile economice și sociale ale statului.

Concludent, atribuirea clasei și a coeficientului de salarizare urmează a fi efectuată în baza unei evaluări ample a funcțiilor publice, conform chestionarului privind descrierea postului. Prevederile privind algoritmul aplicat la stabilirea salariilor angajaților entității noi create în domeniul securității cibernetice nu garantează în mod expres o obligație a existenței unui salariu într-o mărime determinată. Promovarea politicii salariale a

personalului bugetar este de competența exclusivă a statului, care are în vedere nivelul resurselor bugetului.

Acordarea de avantaje materiale funcţionarilor publici din cadrul autorităţilor unei puteri în detrimentul alteia poate submina puterea în discuție, plasând-o pe un plan secund pentru persoanele care vor să se angajeze într-o funcție publică (a se vedea §§ 83 și 84 din Hotărârea Curții Constituționale nr. 24 din 10 septembrie 2013). Având în vedere raționamentele din Hotărârea citate, Curtea a considerat că articolul 6 din Constituție este incident în prezenta cauză.
Anterior Curtea Constituțională a examinat chestiuni referitoare la salarizarea diferențiată a funcționarilor publici și a notat că asigurarea unui echilibru între puterile statului se reflectă şi în gradul de proporţionalitate al asigurării materiale a personalului administrativ (a se vedea HCC nr. 24 din 10 septembrie 2013, §§ 50-52).

Argumentarea nu e suficientă

7. Compatibilitatea cu legislaţia comunitară şi alte standarde internaţionale.

Potrivit notei informative, proiectul nu se încadrează în categoria legislației naționale ce urmează a fi armonizată cu legislația Uniunii Europene, totodată, având în vedere statutul de țară candidat pentru aderarea la Uniunea Europeană a Republicii Moldova, alinierea legislației naționale la legislația Uniunii Europene, prin transpunerea Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) - are un caracter de prioritate națională în domeniul securității cibernetice.

Nota informativă nu oferă o evaluare amplă a standardelor internaționale și a bunelor practici în domeniul stabilirii domeniilor sectoriale, care urmează a fi reglementate, remarcăm ca 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.

Nota / proiectul conţine referinţe la acquis-ul comunitar

Nota / proiectul nu conţine referinţe la alte standarde internaţionale relevante

8. Fundamentarea economico-financiară.

Art.30 lit. e) al Legii nr.100/2017 cu privire la actele normative, prevede expres că nota informativă trebuie să conțină „e) fundamentarea economico-financiară".

Potrivit Notei informative, implementarea prevederilor noului act normativ nu necesită alocarea de mijloace financiare. Analiza de impact la Legea nr. 48/2023 privind securitatea cibernetică cuprinde informații suficiente care acoperă și impactul financiar al prevederilor proiectului în speță. Totodată, reieșind din prevederile art. XVII din proiectul de lege, care prevede modificarea Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar, trebuie de relevat că acestea constau în costurile salariale pentru personalul Agenției pentru Securitate Cibernetică.

Stabilirea pentru personalul Agenției pentru Securitate Cibernetică a sporului cu caracter specific în mărime de 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific, plus majorarea claselor de salarizare cu: 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”, și cu 25 de clase succesive – pentru funcțiile publice de execuție, este semnificativă și urmează a fi corelate cu alocațiile bugetare adoptate prin Legea bugetului de stat pentru anul 2024 nr. 418/2023 și estimărilor pe anii 2025-2026. Astfel, in conformitate cu Legea bugetului de stat pentru anul 2024 nr. 418/2023, aprobat în ședinta plenară a parlamentului la data 22

decembrie 2023, la subprogramul 1504 „Tehnologii informationale” au fost aprobate cheltuieli în suma de 15 000,0 mii lei (pentru 45 unitati de personal/calculat pentru 9 luni).

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/furnizorilor de servicii), în special impactul asupra tarifelor acestora.

Implementarea proiectului nu presupune cheltuieli financiare

Nota informativă nu conține fundamentarea economico-financiară

9. Analiza impactului de reglementare.

Potrivit art. 19 alin. (2) lit. b) din Legea nr.235/2006 cu privire la principiile de baza de reglementare a activității de întreprinzător, pct. 29 subpct.2) și pct. 34 subpct.2) lit. b) ale Regulamentului Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, aprobat prin Hotărârea Guvemului nr. 1429/2008, Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, în cadrul ședinței din 10 ianuarie 2024 a examinat proiectul de lege supus expertizării și a susținut cu condiția luării în considerare a obiecțiilor și recomandărilor din analiza impactului de reglementare la proiectul de lege pentru modificarea unor acte normative (aducerea cadrului legal în concordanță cu Legea nr. 48/2023 privind securitatea cibemetică).
Asigurarea securității informaționale a constituit o provocare în legătură cu procesul de transformare digitală a țării. Această preocupare a fost reflectată de-a lungul anilor în documentele de politici publice, ca parte componentă a procesului de dezvoltare a societății informaționale în Republica Moldova, reflectată în documente de politici precum: Strategia Națională de edificare a societății informaționale – “Moldova electronică”, Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020”, Programul de modernizare tehnologică a Guvernării, inclusiv în Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030 (aprobată în septembrie 2023) etc.

O abordare oficială mai pronunțată față de domeniul securității cibernetice și problematicii acestuia a fost acordată odată cu adoptarea de către Parlament, în anul 2017 a Concepției securității informaționale a Republicii Moldova adoptată prin Legea nr. 299/2017 și, de către Guvern, a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobată prin Hotărîrea Guvernului nr. 811/2015, obiectivul de bază al căruia a constituit crearea unui sistem de management al securității cibernetice a Republicii Moldova prin securizarea serviciilor societății informaționale, contribuind astfel la dezvoltarea unei economii bazate pe cunoaștere, ceea ce, la rândul său, va stimula creșterea gradului de competitivitate economică și de coeziune socială, precum și va asigura crearea de noi locuri de muncă.

Totodată, cel mai important rezultat în acest domeniu, a fost adoptarea în martie 2023 a Legii nr. 48/2023 privind securitatea cibernetică care stabilește cadrul normativ primar în domeniul securității cibernetice și care urmează să intre în vigoare la data de 1 ianuarie 2025.

Articolul 23 din Legea nr. 48/2023 stabilește un set de sarcini Guvernului, orientate spre organizarea executării prevederilor acesteia. Una dintre aceste sarcini rezidă în: obligația Guvernului să elaboreze și să prezinte Parlamentului, în termen de 6 luni din data publicării legii propuneri privind aducerea legislației în conformitate cu Legea nr. 48/2023. Sarcina respectivă stabilită pentru Guvern rezidă din necesitatea asigurării unei sinergii atât la nivel normativ cât și la nivel terminologic dintre legea cadru în domeniul securității cibernetice și alte norme cu caracter primar la nivel sectorial.

Astfel, aceste intervenții au ca obiectiv asigurarea interconexiunii dintre normele Legiinr. 48/2023 privind

securitatea cibernetică și cele cuprinse în legile sectoriale care reglementează activitatea viitorilor furnizori de servicii și eliminarea/revizuirea unor prevederi care ar putea suscita interpretări echivoce sau contradictorii în procesul aplicării normei.

În temeiul art. 4 alin. (2) din Legea nr. 48/2023, Guvernul urmează să adopte lista sectoarelor, subsectoarelor, tipurilor și categoriilor de furnizori de servicii care vor cădea sub incidența prevederilor acestei legi și metodologia de identificare a persoanelor juridice ca fiind furnizori de servicii. Ca punct de pornire pentru determinarea conținutului listei menționate îl constituie anexele nr.1 și nr.2 la Directiva NIS2. Acestea cuprind sectoarele cu o importanță critică ridicată și, respectiv, alte sectoare de importanță critică.

Urmare a unei analize și cercetării preliminare comparative a cadrului legislativ european sectorial de referință, menționat în anexele menționate mai sus, și cel național, au fost determinate legile sectoriale în care sunt necesare și, în consecință, se propun în proiectul de lege, intervenții normative pentru a exclude eventuale ambiguități în interpretarea ulterioară a aplicabilității normelor juridice specifice anumitor sectoare în coroborare cu cele relevante din Legea privind securitatea cibernetică. Aceste intervenții vizează responsabilitatea viitorilor furnizori de servicii în ce privește îndeplinirea obligațiilor de asigurare a securității cibernetice și, corespunzător, competența de supraveghere și control a autorității naționale competente în materie de securitate cibernetică în ce privește modul în care aceste obligații sunt îndeplinite.

În ceea ce privește sectorul economic, vulnerabilitatea la incidente de securitate cibernetică poate afecta afacerile prin pierderi financiare. Aceste situații pot afecta în special afacerile mici și mijlocii, care pot fi mai puțin capabile să își permită să investească în securitatea cibernetică și pot fi mai vulnerabile la atacuri cibernetice.

În ceea ce privește sectorul securității naționale, vulnerabilitatea la incidente de securitate cibernetică poate afecta capacitățile de informații și infrastructurile critice ale țării. Atacurile cibernetice pot fi utilizate pentru spionaj, sabotaj sau chiar pentru a lansa atacuri împotriva infrastructurilor critice, cum ar fi rețelele de electricitate sau gaze. Aceste atacuri pot avea un impact semnificativ asupra securității și stabilității unei țări.

Proiectul a fost supus analizei impactului de reglementare, în conformitate cu prevederile Legii cu privire la principle de bază de reglementare a activitafii de întreprinzator nr.235/2006 și a Hotărârii Guvernului nr.23/2019.

Potrivit art. 13 al Legii nr.235/2006 cu privire la principle de bază de reglementare a activitații de întreprinzator:
„(1) Analiza impactului de reglementare reprezintă argumentarea, în baza evaluării costurilor și beneficiilor, necesității adoptarii actului normativ și analiza de impact al acestuia asupra activității de întreprinzător, inclusiv asigurarea respectării drepturilor și intereselor întreprinzătorilor și ale statului, precum și corespunderea actului scopurilor politicii de reglementare și principiilor prezentei legi.
(2) Actul de analiza a impactului de reglementare este parte integrantă a notei informative a proiectului de act normativ".

În conformitate cu art. 40 din Legea nr. 100/2017 cu privire la actele normative, proiectul de act normativ este prezentat Parlamentului spre examinare împreună cu dosarul de însoțire care conține:
”a) nota informativă;
b) după caz, raportul de analiză ex ante sau analiza impactului de reglementare;
c) avizele şi recomandările, în original, recepţionate în cadrul avizării şi consultărilor publice;
d) rapoartele de expertiză, în original;

e) sinteza obiecţiilor şi propunerilor autorităţilor publice și sinteza recomandărilor reprezentanţilor societăţii civile, dacă există, indicîndu-se acceptarea sau argumentarea respingerii propunerilor, obiecţiilor şi recomandărilor;
f) declaraţia de compatibilitate a Centrului de Armonizare a Legislaţiei, precum şi tabelul de concordanţă actualizat, pentru proiectele marcate cu sigla „UE”;
g) tabelul comparativ, în care să fie reflectate reglementările în vigoare și modificările propuse, pentru proiectele care conțin modificări la actele normative în vigoare;
h) alte materiale, după caz, în baza cărora a fost elaborat proiectul de act normativ.”

Reținem despre faptul că actul de analiza a impactului de reglemetare din dosarul de însoțire așa cum prevede art. 40 din Legea nr.100/2017 privind actele normative, însoțește în mod obligatoriu proiectele de acte normative pînă la aprobarea sau adoptarea finală de către autoritatea responsabilă.

În conformitate cu prevederile pct. 11 din Metodologia de analiză a impactului în procesul de fundamentare a proiectelor de acte normative, aprobată prin Hotărârea Guvernului nr. 23/2019, în cazul proiectelor de acte care conțin norme de reglementare a activității de întreprinzător, se expertizează de către Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, acesta fiind prezentat Parlamentului spre examinare în dosarul de însoțire al proiectului de lege.

Totodată contrar prevederilor sus menționate, chiar dacă actul de analiză a impactului de reglemetare a fost publicat pe pagina web oficială a autorității responsabile, acesta nu a fost prezentat în dosarul de însoțire a proiectului de lege, ci doar extrasul din procesul-verbal al ședinței Grupului de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător din 10 ianuarie 2024 și Opinia expertului Secretariatului Evaluării Impactului de Reglementare, dl. Nicolae Boțan.

Analiza impactului de reglementare a proiectului nu este necesară

Analiza impactului de reglementare a proiectului nu este suficient argumentată/documentată

10. Analiza ex-ante.

Analiza ex-ante a proiectului nu este necesară

Analiza ex-ante a proiectului nu este suficient argumentată/documentată

III. EVALUAREA DE FOND

11. Stabilirea şi promovarea unor interese / beneficii.

Proiectul promovează preponderant interesul angajatilor Agentiei pentru Securitate Cibernetica, prin armonizarea legislației sectoriale și crearea condițiilor pentru realizarea supravegherii și controlului asupra modului de asigurare a securității cibernetice de către furnizorii de servicii. Prin urmare, se constată că prevederile proiectului nu contravin interesului public.

Reieșind din prevederile propuse, și în funcție de finalitățile urmărite odată cu publicarea Legii nr. 48/2023 a început curgerea termenelor de implementare a acesteia stabilite de art. 23. Astfel, până la data de 1 ianuarie 2025, data intrării în vigoare a legii, Guvernul urmează să realizeze un complex de măsuri organizatorice, normative și tehnice orientate spre punerea în aplicare a normelor legale, în mod special:
- aducerea legilor actuale în concordanță cu prevederile Legii nr. 48/2023 privind securitatea cibernetică;

- adoptarea actelor normative subsidiare și aducerea în concordanță cu prevederile legii a cadrului normativ propriu;
- desemnarea/instituirea autorității competente, asigurarea acesteia cu resurse, inclusiv financiare etc.

Până la intrarea în vigoare a Legii nr. 48/2023 privind securitatea cibernetică, chestiunile privind asigurarea securității cibernetice sunt reglementate separat în diverse legi și acte normative ale Guvernului.

Proiectul de lege propune modificări la 21 de legi, iar în funcție de finalitățile urmărite acestea sunt divizate în două categorii:
- necesitatea finalizării constituirii cadrului juridico-normativ, în scopul asigurării funcționalității depline a modelului de guvernanță în domeniul securității cibernetice la nivel national.
- completarea legilor sectoriale care au ca obiect de reglementare activități din domenii și subdomenii corespondente sectoarelor sau subsectoarelor enumerate în anexele I și II ale Directivei NIS2, inclusive statutul persoanelor juridice ce urmează a fi identificate de către autoritatea competentă în domeniul securității cibernetice ca furnizori de servicii.

Obiectivul general al intervenției preconizate este creșterea nivelului de reziliență cibernetică a furnizorilor de servicii, privați sau publici, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale acestor furnizori utilizate în procesul de prestare a serviciilor lor.
Ca obiective specifice, care odată realizate vor asigura atingerea obiectivului general enunțat mai sus, ținem să evidențiem următoarele:

-elaborarea și implementarea unui cadru normativ complet și coerent pentru autoritatea competentă în securitatea cibernetică, având ca obiectiv uniformizarea practicilor europene în gestionarea incidentelor cibernetice și coordonarea operațională a situațiilor de criză;

-elaborarea și implementarea unui cadru normativ complet și coerent pentru echipa națională de răspuns la incidentele de securitate cibernetică, cu accent pe monitorizarea și analiza amenințărilor, precum și coordonarea procesului de divulgare a vulnerabilităților;

-implementarea măsurilor de securitate de către furnizorii de servicii pentru atingerea unui nivel minim comun, având ca rezultat creșterea nivelului general de pregătire și de răspuns la incidentele cibernetice;

-elaborarea și implementarea unui cadru normativ complet și coerent pentru cooperarea eficientă la nivel național și internațional în domeniul securității cibernetice, inclusiv diseminarea informațiilor relevante și adoptarea celor mai bune practici internaționale;

-stabilirea și implementarea unei politici salariale echitabile și competitive pentru angajații Agenției pentru Securitate Cibernetică, asigurând astfel atracția și retenția profesioniștilor în domeniul securității cibernetice și contribuind la eficacitatea organizațională.

În același context, este necesar de evidențiat că un obiectiv convergent al contextului expus îl constituie necesitatea, având în vedere statutul de țară candidat pentru aderarea la Uniunea Europeană a Republicii Moldova, alinierii legislației naționale la legislația Uniunii Europene, transpunerea Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) este caracterul de prioritate națională în domeniul securității cibernetice.

Toate aceste obiective sunt trasate în analiza de impact la Legea nr. 48/2023 privind securitatea cibernetică. Rezultatele prezentului proiect de lege depinde direct de rezultatele Legii nr. 48/2023, această neputând funcționa separat.

Proiectul promovează interese, beneficii

Promovarea intereselor/beneficiilor se face cu respectarea interesului public

12. Prejudicii aduse prin aplicarea actului.

În proiectul de lege sunt propuse modificări la 21 de legi, care pot fi divizate, în funcție de factorii ce le determină, finalitățile pe care le urmăresc și efectele pe care le vor produce, în următoarele categorii:

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

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

Consolidarea securității cibernetice aduce beneficii extinse, protejând datele și informațiile sensibile, ceea ce ar conduce la o mai bună încredere în sectorul privat și public. Reducerea costurilor asociate cu incidentele cibernetice este un alt aspect esențial, economisind sume semnificative de bani și protejând infrastructura critică. Mai mult decât atât, o securitate cibernetică consolidată ar stimula inovația și cercetarea, aducând noi tehnologii și soluții în domeniul securității cibernetice. Aceasta ar putea genera oportunități economice și consolidarea poziției Republicii Moldova în această sferă.

Pe de altă parte, costurile sunt un element important de luat în considerare, însă sunt direct corelate cu așteptările societății și statului față de domeniul securității cibernetice. În același timp, opțiunea recomandată, potrivit Notei de fundamentare nu presupune costuri de implementare suplimentare față de cele deja prezentate în analiza de impact la Legea nr. 48/2023 privind securitatea cibernetică. O situație diferită se atestă la sarcinile administrative ale furnizorilor de servicii identificați în temeiul Legii nr. 48/2023

privind securitatea cibernetică, care sînt suplimentare față de cele analizate la Legea nr. 48/2023.

La aplicare, proiectul va aduce prejudicii

Prejudicierea intereselor/beneficiilor se face cu respectarea interesului public

13. Vulnerabilitatea proiectului din perspectiva drepturilor omului

Potrivit Notei Informative prevederile proiectului de lege nu aduce atingere drepturilor fundamentale ale omului consacrate de Constituţia Republicii Moldova, Declaraţia Universală a Drepturilor Omului şi Convenţia Europeană a Drepturilor Omului.

Totodată, este important de subliniat constările Parlamentului European din Raportul referitor la drepturile omului și democrația în lume și politica UE în această privință (raport annual pe anul 2021) la rubrica Tehnologiile digitale.

Astfel, în Propunerile de rezoluție a Parlamentului European, se subliniază că tehnologiile trebuie dezvoltate, implementate și utilizate sub o supraveghere umană semnificativă, în deplină transparență și asigurând responsabilitatea și nediscriminarea, în special pentru a evita atât prejudecățile în deciziile automatizate, cât și încălcările protecției datelor.

Se subliniază suplimentar că tehnologiile digitale au jucat rolul important, în special în timpul pandemiei de COVID-19; și aceste tehnologii vor continua să fie puse în aplicare în întreaga lume în perioada post-pandemie și ar trebui să fie reglementate în mod corespunzător pentru a se profita de punctele lor forte, evitând, în același timp, orice consecințe negative asupra drepturilor omului; în mod deosebit, importanța unor garanții eficace pentru dreptul la viață privată și la protecția datelor în sistemele de supraveghere în masă legate de sănătate, precum și a utilizării proporționale a acestora, care ar trebui, de asemenea, să fie limitată în timp; riscurile evidente ale utilizării necorespunzătoare a tehnicilor de supraveghere împotriva apărătorilor drepturilor omului, a membrilor opoziției, a jurnaliștilor, a societății civile și a altor persoane în special, în primul rând deoarece reprezintă un obstacol serios în calea apărării drepturilor omului, un risc pentru viața privată și libertatea de exprimare, precum și o amenințare gravă la adresa instituțiilor democratice.

Supravegherea și controlul de stat în domeniul securității cibernetice pot ridica numeroase probleme legate de respectarea drepturilor omului și a vieții private a cetățenilor. Pe de o parte, este important să existe măsuri eficiente de supraveghere și control pentru a proteja infrastructurile și datele critice împotriva atacurilor cibernetice și a activităților ilegale online. Pe de altă parte, aceste măsuri trebuie să fie echilibrate pentru a evita abuzurile și încălcările drepturilor individuale.

Adițional, Propunerea de rezoluție a Parlamentului European referitoare la situația drepturilor fundamentale în Uniunea Europeană (raport anual 2022 și 2023), expune îngrijorare întrucât organismele guvernamentale din unele state membre și țări terțe au folosit programul ”Pegasus” și alte programe de spionaj împotriva jurnaliștilor, politicienilor, reprezentanților autorităților de aplicare a legii, diplomaților, avocaților, oamenilor de afaceri, actorilor societății civile și altor actori în scopuri politice și chiar infracționale; iar astfel de practici sunt extrem de îngrijorătoare și demonstrează riscul ca tehnologiile de supraveghere să fie folosite în mod abuziv pentru a submina drepturile fundamentale ale omului, democrația și procesele electorale, subliniază că digitalizarea este un proces transversal care afectează accesul la toate serviciile, în special la asistența medicală, și exercitarea drepturilor fundamentale și reamintește, în ceea ce privește digitalizarea, că trebuie să se acorde o atenție deosebită prejudecăților discriminatorii ce sunt introduse în noile tehnologii și să se oblige dezvoltatorii și operatorii să pună la dispoziție informații accesibile publicului cu privire la modul în

care sunt pregătite aceste sisteme, în special în ceea ce privește dezvoltarea noilor tehnologii, îndeosebi în funcțiile decizionale.

Proiectul respectă drepturile/libertăţile

14. Compatibilitatea proiectului cu prevederile cadrului normativ național

Prin prisma compatibilității proiectului de lege cu cadrul normativ national expunem că pentru implementarea eficientă a Legii nr. 48/2023 privind securitatea cibernetică, prevederile prezentului proiect de lege se propune a se implementa începînd cu 1 ianuarie 2025, cu excepția prevederilor art. XVII din proiect care presupune modificarea Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar, în scopul asigurării funcționalității autorității competente în domeniul securității cibernetice. În realizarea obiectivului propus Guvernul a aprobat Hotărîrea nr. 1028/2023 cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică și Regulamentul cu privire la organizarea și funcționarea Agenției pentru Securitate Cibernetică.

În esență, proiectul de lege vizat are drept scop modificarea a unui șir de acte normative care cuprind în esență sectoarele și subsectoarelor identificate ca critice (stabilite în Anexa 1 “Sectoarele cu o importanță critică ridicată” și în Anexa II „Alte sectoare de importanță critică”), precum si tipul entitatilor aferente acestor sectoare , așa precum reiese și din clauza de armonizare din Legea nr.48/2023.

Potrivit Notei informative la proiectul de lege prenotat acestea sunt identificate în diferite sectoare, cum ar fi-sănătate, transport maritim, comunicații electronice, financiar-bancar, comunicații poștale, securitate, rețele de infrastructură, etc., (Legea nr. 1456/1993 cu privire la activitatea farmaceutică, Legea ocrotirii sănătatii nr. 411/1995, Codul navigației maritime comerciale nr. 599/1999, Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Legea comunicațiilor electronice nr. 241/2007, Legea nr. 131/2012 privind controlul de stat asupra activității de întreprinzător, Legea nr. 171/2012 privind piața de capital, Legea nr. 176/2013 privind transportul naval intern al Republicii Moldova, Legea nr. 303/2013 privind serviciul public de alimentare cu apa și de canalizare, Legea comunicațiilor poștale nr. 36/2016, Legea nr. 209/2016 privind deșeurile, Legea nr. 102/2017 cu privire la dispozitivele medicale, Legea nr. 120/2017 cu privire la prevenirea si combaterea terorismului, Legea 174/2017 cu privire la energetică, etc. in vederea aducerii acestora in concordanta cu Legea nr. 48/2023 privind securitatea cibemetică.

Cerințele în materie de securitate cibernetică impuse entităților care furnizează servicii sau desfășoară activități care sunt semnificative din punct de vedere economic variază considerabil de la un stat membru la altul î,n ceea ce privește tipul de cerință, nivelul lor de detaliere și metoda de supraveghere. Pentru a realiza acest lucru, entitățile identificate drept entități critice în temeiul Directivei (UE) 2022/2557 ar trebui să fie considerate a fi entități esențiale în temeiul prezentei directive.

Totuși, în procesul de identificare a fumizorilor de servicii, autoritatea competenta în domeniul securității cibernetice urmează să aplice principiile de aplicare a Legii nr. 48/2023 prevazute de alineatele (5) si (6) ale art. 3:

”(5) În cazul în care legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele critice, stabilite de către Guvern, prevăd implementarea unor măsuri de securitate sau îndeplinirea obligațiilor de notificare a incidentelor cibernetice cu impact semnificativ, ale căror efecte sunt cel puțin echivalente cu efectele obligațiilor stabilite de prezenta lege, se consideră că prevederile legilor respective au caracter special în raport cu prevederile prezentei legi.

(6) În cazul în care obligațiile, prevăzute la alin. (5), stabilite de legile care reglementează activitatea furnizorilor de servicii, sectoarele și subsectoarele critice, stabilite de către Guvern, sunt aplicabile unui număr mai restrâns de persoane juridice decât cel prevăzut de prezenta lege și de actele normative de punere în aplicare a acesteia, prevederile prezentei legi se aplică persoanelor juridice care nu cad sub incidența obligațiilor impuse de legile respective.”

Reieșind din considerentele actului European transpus, și din prevederile normei de la art. 4 alin. (2) din Legea nr. 48/2023 care stabilește expres că: ” 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.”

Constatăm neconcordanață cu prevederile în vigoare, iar determinarea, în baza unei analize comparative formal-juridice, a tipologiei corespondente în legislatia națională prin identificarea termenilor care înglobează tipurile de entități enumerate în anexele Directivei NIS2, nu respectă rigorile de calitate ale actului normativ.

Proiectul nu este compatibil cadrului normativ naţional

15. Analiza detaliată a prevederilor

Nr. obiecției	Art.	Text	Obiecții	Elemente de coruptibilitate/vulnerabilitate	Recomandări

1	Pe tot cuprinsul proiectului de lege	Revizuirea formulelor de trimitere utilizate pe tot cuprinsul proiectului de lege, întru evitarea interpretărilor eronate a normelor proiectului, mai ales, în partea ce ține de stabilirea obligațiilor ce necesită a fi îndeplinite de către furnizorii de servicii identificați în temeiul Legii nr. 48/2023 privind securitatea cibernetică. Următoarele formule utilizate în proiectul de lege:” în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi” (art. XIV pct. 1 din proiect);” actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice” (art. I pct. l, art. II, art. III, art. IV, art. V pct. 1, art. VII pct. 1, art. VIII, art. IX pct. 3, art. XI pct. 1, art. XII, art. XIV pct.2, art. XVII pct. 2, art. XIX pct. 1, art. XX pct. 2, art. XXI pct. 2 și art. XXII din proiect)	Pentru a fi în corespundere cu prevederile art. 55 alin. (5) al Legii nr. 100/2017 și ale Metodologiei de tehnică legislativa aplicată la redactarea proiectelor de acte normative, aprobată prin Hotărârea Biroului permanent nr. 3/2022, care stipulează expres că, dacă trimiterile la alte acte normative sunt necesare acestea trebuie să desemneze actul normativ sau dispoziția concretă la care se face referire.	Array	În vederea respectării trăsăturilor calitative ale proiectului: precizia; claritatea; caracterul practic, propunem excluderea formulelor utilizate. Rațiunea excluderii rezidă din prevederile Legii nr. 48/2023 și reiese însăși din obiectul de reglementare al acesteia, care la art. 1 stipulează expres că: ”Prezenta lege reglementează cadrul normativ, organizaţional şi de cooperare în domeniul securităţii cibernetice, stabileşte competenţa autorităţilor şi instituţiilor publice în materie de securitate cibernetică, determină cadrul naţional general de gestionare a crizelor în domeniul securităţii cibernetice, instituie cerinţe, măsuri şi mecanisme în scopul asigurării securităţii reţelelor şi sistemelor informatice, care sunt esenţiale pentru funcţionarea societăţii, şi al gestionării incidentelor cibernetice.” Totodată, prevederile art. 11 alin. (4) lit. b) din Legea nr. 48/2023 stabilește că aceste cerințe specifice de securitate se aprobă de Guvern la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securităţii cibernetice.

2	Pe tot cuprinsul proiectului de lege	Clarificarea și precizarea asupra terminologiei. Proiectul de lege, utilizează două formulări:” autoritatea competentă în domeniul securității cibernetice” și” autoritatea competentă la nivel național în domeniul securității cibernetice” .	Pentru un spor de rigoare juridică și claritate normativă, recomandăm precizarea și uniformizarea noțiunii utilizate în proiect.	Array	Uniformizarea noțiunii utilizate.
3	Art. V pct.1 și Art. XXII alin. (3)	formula –” în temeiul acestei legi”.	Redacția alin. (3) a art. 21 din Legea comunicațiilor electronice nr. 241/2007, se atestă o formă repetitivă a normelor de trimitere. Utilizarea dublei trimiteri induce în eroare furnizorii și comport un risc de coruptibilitate, mai ales că norma conține prevederi referitoare la încălcările depistate și eventualele sancțiunile aplicate.	Array	Se recomandă de exclus repetiția.
4	Art. XVII	Stabilirea pentru personalul Agenției pentru Securitate Cibernetică a sporului cu caracter specific în mărime de 120% din suma anuală a salariilor de bază pentru personalul cu drept de a beneficia de spor cu caracter specific. -Majorarea claselor de salarizare cu: 15 clase succesive - pentru funcțiile publice de conducere de „șef de direcție” și „șef adjunct de direcție”, și cu 25 de clase succesive – pentru funcțiile publice de execuție	Mecanismul de stabilire a salariilor și a altor drepturi de natură salarială face parte din categoria informațiilor de interes public, iar Nota informativă nu demonstrează că raportul sarcinilor și obiectivelor entității în raport cu alte autorități publice, este substanțial mai superior. Consecvent, norma propusă deviază de la conceptul initial al proiectului de lege- aducerea în concordanță a cadrului normativ conex cu Legea nr. 48/2023.	Array	Excluderea din proiect a prevederilor propuse întru respectarea echilibrului și respectarea principiului transparenței

5	Pe tot cuprinsul proiectului de lege	Sectoarele și subsectoarele critice	Potrivit art. 4 alin. (2) din Legea nr. 48/2023, Guvernul aprobă lista sectoarelor și subsectoarelor critice și, corespunzător, a tipurilor și categoriilor de personae 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 ftind furnizori de servicii, precum și modul de întocmire, ținere si actualizare a listei furnizorilor de servicii. Prin urmare, în conformitate cu Legea cadru, Guvernul trebuie să aprobe lista sectoarelor si subsectoarelor, dar și tipurile și categoriile de persoane juridice care urmează să cadă sub incidența prevederilor Legii privind securitatea cibernetică, precum si cadrul metodologic de identificare a acestora	Array	Reevaluarea sectoarelor și subsectoarelor critice cu evaluarea riscurilor și costurilor.Or, stabilirea în dispozițiile finale și tranzitorii ale proiectului a unei implementări graduale.

IV. CONCLUZII

În urma analizei proiectului de lege pentru modificarea unor acte normative, din perspectiva alegerii domeniilor prioritare în care să fie instituite cerințe de securitate cibemetică si, corespunzător, care să fie supravegheate/monitorizate și supuse controlului de stat de noua Agentie pentru Securitate Cibernetică, sunt necesare optiuni alternative și argumentare corespunzatoare, mult mai fundamentală, decat simpla trimitere la cadrul normativ European.

In situația în care domeniile critice evidente (autoritățile publice, segmentul bancar și financiar, utilitătile publice etc.) reprezintă marea majoritate a punctelor critice de risc, atunci asumarea cu noi cerinte dar și risipirea neeficientă a resurselor Agentiei pentru domenii care nu sunt demonstrate a fi critice în realitate în Republica Moldova nu este rațională în prima perioadă, de organizare a activității autorității.

Observăm că intervențiile vizează responsabilitatea viitorilor furnizori de servicii în ce privește îndeplinirea obligațiilor de asigurare a securității cibernetice și, corespunzător, competența de supraveghere și control a autorității naționale competente în materie de securitate cibernetică în ce privește modul în care aceste obligații sunt îndeplinite.

Din analiza efectuată, constatăm că în context, examinînd proiectul național prin prisma actului UE menționat, remarcăm că, proiectul national nu are ca scop transpunerea directă a unor prevederi din Directiva (UE) 2022/2555, precum și nu instituie careva prevederi noi care contravin actului UE, inserând obligații generale aferente securității cibernetice pentru furnizorii de servicii în actele normative sectoriale.

Considerăm important de a reglementa diferențierea categoriilor de entități pentru a asigura un echilibru

corect între cerințele și obligațiile bazate pe riscuri, pe de o parte, și sarcina administrativă care decurge din supravegherea conformității, pe de altă parte.

O altă problemă conceptuală a proiectului, ține de modul de organizare a activității de monitorizare și supraveghre a furnizorlor de servicii în sensul Legii privind securitatea cibernetică. În acest context, abordăm problema ce ține de conceptul formulelor de trimitere utilizate pe tot cuprinsul proiectului de lege, mai ales, în partea ce ține de stabilirea obligațiilor ce necesită a fi îndeplinite de către furnizorii de servicii identificați în temeiul Legii nr. 48/2023 privind securitatea cibernetică, întru evitarea interpretărilor eronate a normelor proiectului.

Astfel, pentru a fi în corespundere cu prevederile art. 55 alin. (5) al Legii nr. 100/2017 și ale Metodologiei de tehnică legislativa aplicată la redactarea proiectelor de acte normative, aprobată prin Hotărârea Biroului permanent nr. 3/2022, care stipulează expres că, dacă trimiterile la alte acte normative sunt necesare acestea trebuie să desemneze actul normativ sau dispoziția concretă la care se face referire, considerăm necesar revizuirea acestora.

Prin urmare, evidențiem următoarele formule utilizate în proiectul de lege:” în conformitate cu prezenta lege, cu legile sectoriale, precum și în temeiul altor legi” (identificate la art. XIV pct. 1 din proiect);” actele normative de punere a acesteia în aplicare și de alte acte normative care stabilesc cerințe specifice de asigurare a securității cibernetice” (identificate la art. I pct. I, art. II, art. III, art. IV, art. V pct. 1, art. VII pct. 1, art. VIII, art. IX pct3, art. XI pct. 1, art. XII, art. XIV pct.2, art. XVII pct. 2, art. XIX pct. 1, art. XX pct. 2, art. XXI pct. 2 și art. XXII din proiect).

Rațiunea subliniată mai sus, rezidă din prevederile Legii nr. 48/2023 și reiese însăși din obiectul de reglementare al acesteia, care la art. 1 stipulează expres că: ”Prezenta lege reglementează cadrul normativ, organizaţional şi de cooperare în domeniul securităţii cibernetice, stabileşte competenţa autorităţilor şi instituţiilor publice în materie de securitate cibernetică, determină cadrul naţional general de gestionare a crizelor în domeniul securităţii cibernetice, instituie cerinţe, măsuri şi mecanisme în scopul asigurării securităţii reţelelor şi sistemelor informatice, care sunt esenţiale pentru funcţionarea societăţii, şi al gestionării incidentelor cibernetice.” Totodată, prevederile art. 11 alin. (4) lit. b) din Legea nr. 48/2023 stabilește că aceste cerințe specifice de securitate se aprobă de Guvern la propunerea autorităţii administraţiei publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securităţii cibernetice. Concept care în viziunea noastră, se exclude reciproc și nu asigură respectarea rigorilor cadrului legal și al respectării principiilor clarității și previzibilității. Recomandăm organizarea activității de supraveghere și monitorizare să fie exercitate doar în limitele Legii nr. 48/2023 fapt care va oferi posibilitatea subiecților implicați în acest raport juridic sa-și organizeze activitatea mai eficient.

În ceea ce privește predictibilitatea menționăm că proiectul urmează a fi consultat obligatoriu cu persoanele juridice de drept privat care se califică drept întreprinderi mijlocii, potrivit clasificării prevăzute de legislația cu privire la întreprinderile mici și mijlocii, și persoanelor juridice de drept privat ce depășesc criteriile pentru întreprinderile mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele critice, stabilite de către Guvern, și care sunt identificate ca furnizori de servicii de către autoritatea competentă desemnată.

În aceste condiții, mediul de afaceri și alte părți interesate vor avea suficient timp să se implice în dezbateri și să ofere feedback, consolidând astfel democrația participativă.

Proiectul de act normativ pentru modificarea unor acte normative (modificarea cadrului legal în conformitate cu Legea nr. 48/2023 privind securitatea cibernetică) a fost înregistrat în Parlament cu nr. 41 din 14 februarie

2024, aprobat în prima lectură în ședința plenară din 29.02. 2024.

În urma analizei efectuate, concluzionăm că proiectul de lege oferă o nouă reglementare a mai multor entități identificate ca furnizori de servicii în temeiul Legii nr. 48/2023, și are menirea să asigure o funcționalitate mai bună și un cadrul legal de reglementare optim pentru Agenția pentru Securitate Cibernetică avînd ca obiectiv scăderea riscului de incidente cibernetice. Elaborarea acestuia, a fost dictată de adoptarea Legii nr. 48/2023 cu privire la securitatea cibernetică și se datorează, în mare parte, transpunerii cadrului normativ national și alinierii legislației naționale la legislația Uniunii Europene (transpunerea Directivei (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2).

Temeiul instituționalizării domeniului securitate cibernetică, a constituit legislația Uniunii Europene inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană.

Totodată, proiectul evidențiază o serie de deficiențe și probleme conceptuale privind organizarea procedurii de supraveghere și monitorizare precum și povara administrativă pentru notificari și alte proceduri de raportare. Printre principalele aspecte semnalate se numără reglementarea incompletă a normelor juridice în ceea ce privește functiile de control si supraveghere ale Agentiei pentru Securitate Cibernetică, de asemenea este important să se clarifice și să se reglementeze impactul potențial al controlului în raport cu alte solutii mai putin invasive dar și asigurarea transparenței în activitatea noii Agenții.

Nu în ultimul rînd, se propune abordarea exhaustivă a măsurilor restrictive și sanctiunile pe care le va putea aplica Agenția, spectrul de raportări care urmează a fi prezentate de către entitățile vizate în proiectul de lege.

Materialele aferente proiectului de lege nu aduce în discuție aspecte legate de consultările publice în procesul de elaborare a proiectului de lege, fapt care face imposibilă reflectarea pozitiei persoanelor afectate, în special a agenților economici.

În concluzie, evidențiem nevoia de îmbunătățire a proiectului de lege din punct de vedere redacțional, precum și în ceea ce privește detaliile reglementărilor menționate (în partea ce ține de controlul, monitorizarea și supravegherea) și abordarea principiilor democratice și a dialogului între diversele părți implicate. Relevăm, importanța respectării procedurii legiferării în scopul analizei situației reale din Republica Moldova în acest domeniu, precum și identificarea domeniilor de infrastructură critică în concordanță cu standardele europene.