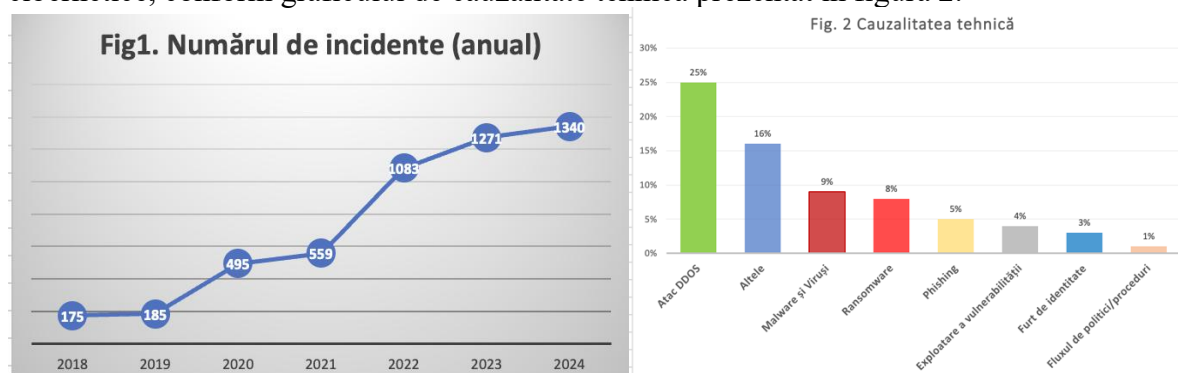


Nota de fundamentare
la proiectul hotărârii Guvernului cu privire la supravegherea și controlul de stat asupra
respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii
în sectoarele critice

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul hotărârii Guvernului este elaborat de către Ministerul Dezvoltării Economice și Digitalizării, în calitate de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ
Temeiul legal al elaborării și adoptării proiectului de act normativ îl constituie prevederile art. 18 alin. (3) și art. 19 alin. (5) din Legea nr. 48/2023 privind securitatea cibernetică (în continuare – Legea nr. 48/2023). Aceste norme stabilesc în competența Guvernului reglementarea: - măsurilor de supraveghere și a modului de aplicare a acestora, și - modului de efectuare a controlului de stat de către autoritatea competentă asupra respectării obligațiilor ce le revin acestora conform Legii nr. 48/2023 separat pentru furnizorii de servicii persoane juridice de drept privat și pentru furnizorii de servicii persoane juridice de drept public. Elaborarea proiectului de act normativ propus spre examinare este prevăzută și de următoarele documente strategice ale Republicii Moldova: • Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) - punctul 53, proiectul nr. 38 din Capitolul 10 „Societatea informațională și mass-media” al Clusterului 3 „Competitivitate și creștere incluzivă”; • Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) - măsura 2.3.11, indicatorul (v) „delimitarea clară și transparentă a competențelor instituțiilor de securitate cibernetică ale MD, cu ajustarea mandatelor instituțiilor relevante în urma unei note a unui expert.”; • Foaia de parcurs privind „Statul de drept” (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (Hotărârea Guvernului nr. 275/2025) – act. 4.1 și 4.3 din Rezultatul strategic nr. 4. „Consolidarea capacității de prevenire și combatere a criminalității cibernetice”; • Planul național de reglementări pentru anul 2025 (Hotărârea Guvernului nr. 841/2024) – acțiunea 18; • Strategia de transformare digitală a Republicii Moldova (Hotărârea Guvernului nr. 650/2023) - Obiectivul general nr. 5. „Crearea unui mediu digital accesibil, sigur și incluziv direcții prioritare”, direcția prioritară nr. 1) „Instituirea unei autorități competente în domeniul securității cibernetice la nivel național, cu funcții de punct unic de contact, echipă de răspuns la incidente de securitate cibernetică (CSIRT), dar și identificare, monitorizare și supraveghere, coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional.”.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative

Între 2018 și 2024, statele membre ale Uniunii Europene au raportat un total de 5108 de incidente cibernetice cu impact semnificativ¹, conform criteriilor stabilite de Directiva NIS², Codul³ european al comunicațiilor electronice și Regulamentul eIDAS⁴. Dintre acestea, 29 % au fost considerate acțiuni rău intenționate. Cel mai afectat sector a fost sectorul privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transporturi și energie.

Datele indică o tendință generală de creștere a numărului de incidente cu impact semnificativ (figura 1). Din cele 1402 de incidente rău intenționate raportate, majoritatea au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în figura 2.



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform raportului actualizat al IBM privind costul unei încălcări a securității datelor în 2024⁵, impactul financiar al încălcărilor securității datelor este și mai mare pentru entitățile critice. Raportul indică faptul că, în 2024, costul mediu global al unei încălcări a securității datelor a atins un nivel record de 4,88 milioane de dolari SUA, înregistrând o creștere de 10% față de 2023

Studiul global realizat de compania McAfee⁶, care a evaluat pierderile economice cauzate de criminalitatea informatică, intitulat "Pierderi nete: estimarea costului global al criminalității informatice", oferă o estimare a impactului economic al criminalității informatice pentru diferite țări, exprimat ca procent din PIB. Graficul prezentat în figura 3 evidențiază țările cele mai grav afectate în funcție de proporția daunelor monetizate în raport cu PIB-ul lor. În medie, pierderile cauzate de criminalitatea cibernetică reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că produsul intern brut al țării a fost de aproximativ 16,5 miliarde de dolari americani în 2023, se poate estima un prejudiciu anual potențial de aproximativ 49 de milioane de dolari, pe baza mediei de 0,3% din PIB.

¹ <https://ciras.enisa.europa.eu/ciras-consolidated-reporting>

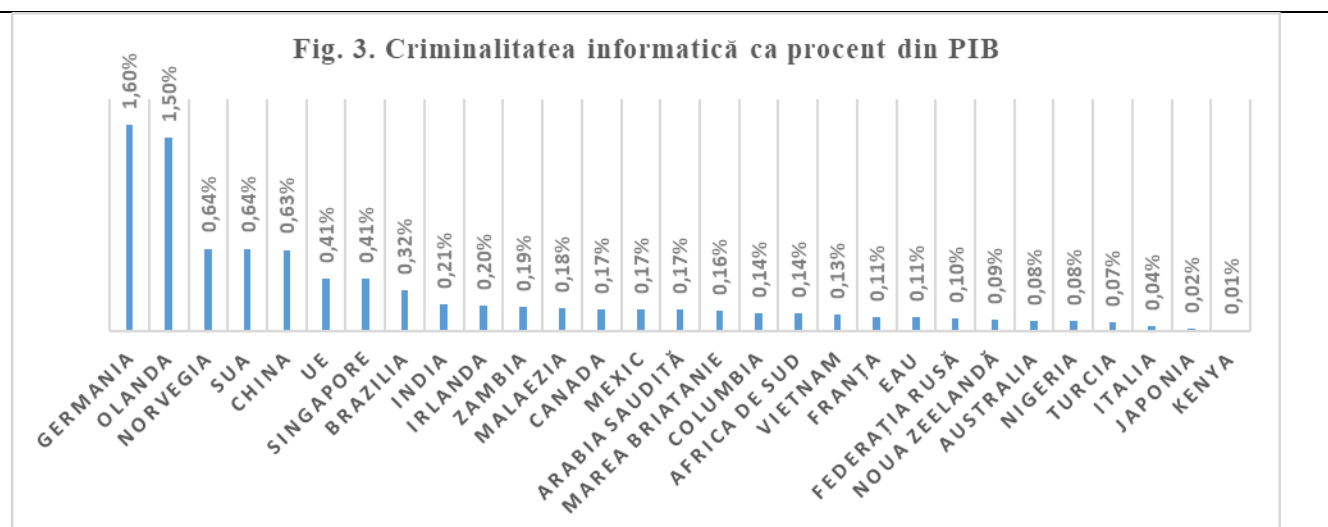
² Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016L1148>

³ Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02018L1972-20241018>

⁴ Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE: <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02014R0910-20241018>

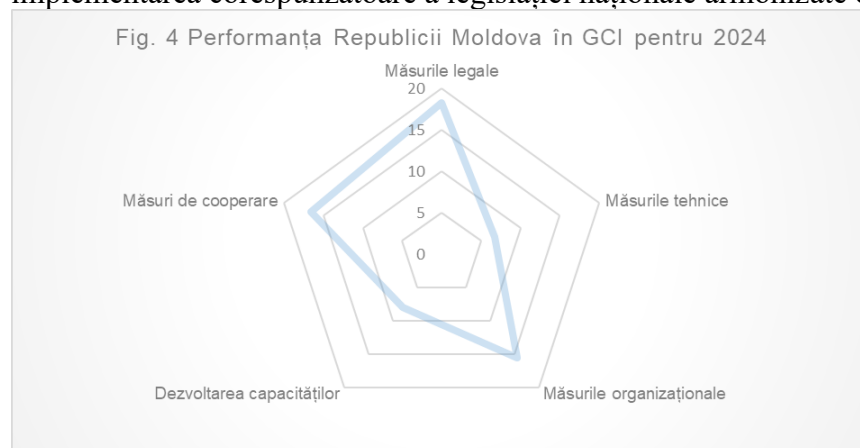
⁵ <https://www.ibm.com/reports/data-breach>

⁶ <https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciiis>



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

Conform Indicelui Global de Securitate Cibernetică (GCI) al UIT pentru 2024, Republica Moldova are un scor general de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 (nivelul 3 reprezintă țările care au obținut un scor general de cel puțin 55/100), demonstrând un angajament de bază în materie de securitate cibernetică, care include evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate, pe un număr moderat de piloni sau indicatori. Conform raportului UIT privind echipa națională de răspuns la incidente de securitate cibernetică, performanța Republicii Moldova pentru 2024, comparativ cu 2020, a înregistrat o creștere a măsurilor legale, organizaționale și de cooperare, însă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, dar acest lucru poate fi atribuit parțial ajustărilor metodologice și ponderilor GCI, precum și modificărilor aduse întrebărilor. Graficul de mai jos (Figura 4) evidențiază performanța Republicii Moldova în GCI pentru 2024, subliniind că măsurile tehnice și consolidarea capacităților sunt punctele slabe ale Republicii Moldova în acest domeniu. Cu toate acestea, acest indice poate fi îmbunătățit prin implementarea corespunzătoare a legislației naționale armonizate cu legislația UE.



Industria IT în Republica Moldova se dezvoltă rapid. În 2023, industria IT a atins o pondere de peste 5,3% din produsul intern brut, depășind 15 miliarde de lei în vânzări, ponderea sectorului TIC este de peste 8,3% din PIB, cu peste 25 de miliarde de lei în vânzări în 2023, realizate de aproximativ 3 200 de companii cu peste 35 000 de angajați. Creșterea în sectorul IT a fost generată de avantajele pe care Moldova le oferă ca destinație pentru externalizarea serviciilor IT, beneficiind de costuri competitive, amplasare geografică favorabilă și calificări ale forței de muncă, alături de un cadru fiscal și

administrativ facil pentru rezidenții Parcului IT Virtual Moldova. Rapoartele globale referitoare la digitalizare (cum ar fi Indicele UN DESA e-Guvernare, Indicele de Dezvoltare în Rețea NRI, Indicele Țării Digitale etc.), rapoartele emise de ANRCETI și sondajele anuale efectuate de Agenția de Guvernare Electronică (AGE) confirmă progresele semnificative ale Republicii Moldova în privința accesului la internet și utilizarea dispozitivelor IT, precum și dezvoltarea platformelor de e-guvernare. Cu toate acestea, avansul rapid al tehnologiei informației și comunicațiilor electronice și al proceselor de transformare digitală, deși aduce beneficii incontestabile în diverse domenii, este însoțit de o creștere semnificativă și continuă a amenințărilor la adresa securității cibernetice. Reieșind din acestea, securitatea cibernetică a fost declarată ca fiind o prioritate la nivel național, acest aspect fiind reflectat într-un set de documente de politici, cum ar fi:

- **Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru perioada 2025-2029**⁷ acordă prioritate punerii în aplicare a Legii 48/2023 privind securitatea cibernetică, în special identificării furnizorilor de servicii critice și punerii în aplicare a cerințelor de securitate pentru rețele și sisteme informatice, precum și operaționalizării complete a Agenției pentru Securitate Cibernetică. Hotărârea Guvernului nr. 562/2025 „Cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice”, care include în obiectul său de reglementare și cerințele de securitate pentru rețele și sisteme informatice, este în proces de promovare, urmând în timpul apropiat să fie supus examinării de către Guvern. Aceasta determină necesitatea consolidării capacităților furnizorilor de servicii din sectoarele critice, deoarece aceștia au nevoie de formare în ceea ce privește modul de punere în aplicare a cerințelor de securitate cibernetică și de respectare a cadrului normativ în domeniu.

- **Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030**⁸: unul dintre obiectivele acesteia este crearea unui mediu digital accesibil, sigur și incluziv, având ca scop asigurarea unei creșteri a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova. Aceste entități urmează fi gestionate mult mai eficient și transparent, iar incidentele cibernetice, precum și eventualele prejudicii materiale și reputaționale asociate acestora, vor fi evitate. În același timp, se urmărește implementarea unei abordări multidisciplinare, iar toate părțile interesate, inclusiv Guvernul, sectorul privat și societatea civilă, își vor asuma responsabilitatea și angajamentul comun pentru susținerea și cooperarea în asigurarea securității cibernetice.

- **Strategia securității naționale a Republicii Moldova**⁹, care evidențiază riscurile cibernetice la care este expusă Republica Moldova, subliniind în principal atacurile cinetice sau cibernetice lansate de actori statali externi asupra infrastructurii critice naționale și regionale, atacurile cibernetice lansate asupra instituțiilor publice sau private de către structuri specializate în criminalitatea cibernetică, precum și riscurile asociate evoluțiilor din domeniul tehnologiilor precum blockchain și criptomonede, inteligența artificială, învățarea automată, internetul obiectelor, tehnologia 5G, big data, tehnologiile cuantice, internetul ascuns.

La data de 16 martie 2023, Parlamentul a adoptat Legea nr. 48/2023 privind securitatea cibernetică, care a intrat în vigoare la data de 1 ianuarie 2025. Legea are ca obiectiv general să asigure legalitatea în spațiul cibernetic prin reglementarea principalelor elemente indispensabile implementării unui model de guvernare eficient la nivel național în vederea protecției și asigurării securității rețelilor și sistemelor informatice, utilizate de către persoanele juridice, publice sau private, în procesul de prestare a serviciilor considerate a fi esențiale pentru susținerea unor activități societale și economice critice. Un

⁷ https://www.legis.md/cautare/getResults?doc_id=148720&lang=ro

⁸ https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro

⁹ https://www.legis.md/cautare/getResults?doc_id=141253&lang=ro

instrument juridic esențial asumat în procesul reglementării acestui domeniu a constituit legislația Uniunii Europene, inclusiv în contextul obținerii de către Republica Moldova a statutului de țară candidat la aderarea la Uniunea Europeană, prin Legea respectivă asigurându-se, deși doar parțial, armonizarea cadrului normativ național la prevederile Directivei NIS¹⁰ și, implicit, a unor elemente esențiale ale Directivei NIS¹¹.

Astfel, Legea privind securitatea cibernetică cuprinde un set de reglementări care au ca scop în principal:

a) stabilirea cadrului general privind cooperarea și coordonarea strategică la nivel național și internațional, prin reglementarea expresă a constituirii unui consiliu coordonator cu rol consultativ al Guvernului, dedicat exclusiv domeniului securității cibernetice și stabilirea obligativității adoptării unei strategii naționale în acest domeniu;

b) desemnarea/instituirea de către Guvern a unei autorități competente în domeniul securității cibernetice la nivel național, care să includă în competența sa, de rând cu funcțiile de coordonare, cooperare internă, supraveghere și control de stat, și pe cele de echipă națională de răspuns la incidentele cibernetice și de punct unic de contact la nivel național;

c) reglementarea legală primară a procesului de coordonare și gestionare a crizelor în domeniul securității cibernetice și atribuirea competenței legale în această materie viitoarei autorități responsabile;

d) stabilirea cadrului legal primar în ce privește obligațiile de asigurare a securității cibernetice nu doar de către persoanele juridice de drept public, ci și de către cele de drept privat, în mod special în ceea ce privește obligațiile de implementare a măsurilor de securitate și în ceea ce privește obligațiile de notificare a incidentelor cibernetice semnificative, și împuternicirea autorității competente la nivel național în acest domeniu cu exercitarea funcțiilor de supraveghere și control de stat al modului în care persoanele vizate îndeplinesc aceste obligații;

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

Totuși, Legea nr. 48/2023 privind securitatea cibernetică stabilește doar cadrul normativ primar în domeniul securității cibernetice, pentru punerea în aplicare a acesteia fiind necesară aprobarea unor acte normative, în mod specific, la nivelul Guvernului. O parte importantă a chestiunilor abordate în lege, reglementarea cărora a fost dată în competența Guvernului, a fost deja soluționată prin aprobarea următoarelor acte normative:

- **Hotărârea Guvernului nr. 1028/2023** cu privire la constituirea, organizarea și funcționarea Agenției pentru Securitate Cibernetică;
- **Hotărârea Guvernului nr. 333/2024** cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice;
- **Hotărârea Guvernului nr. 860/2024** cu privire la identificarea furnizorilor de servicii;
- **Hotărârea Guvernului nr. 112/2025** pentru modificarea unor hotărâri ale Guvernului (*modificarea actelor normative subsidiare în conformitate cu Legea nr.48/2023 privind securitatea cibernetică și legile conexe*)
- **Hotărârea Guvernului nr. 562/2025** cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice.

¹⁰ **Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului** din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148;

¹¹ **Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului** din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune;

Proiectul de act normativ propus nu este generat ca urmare a identificării unei probleme noi, ci este o măsură care asigură implementarea prevederilor Legii nr. 48/2023 privind securitatea cibernetică și actele normative aprobate pentru punerea acesteia în aplicare. **Problema principală** care urmează a fi soluționată prin inițiativa propusă, astfel cum a fost identificată în analiza de impact aferentă proiectului de lege, ulterior aprobat prin Legea nr. 48/2023 privind securitatea cibernetică, constă în nivelul general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor ce vizează securitatea rețelelor și a sistemelor informatice. Această deficiență poate compromite buna funcționare a administrației publice centrale și locale, în special în ceea ce privește prestarea serviciilor publice, precum și activitatea economică a întreprinderilor din sectorul privat, afectând în consecință întreaga economie națională și, implicit, viața socială.

Categoria de subiecți interesați în intervenția propusă poate fi grupată în următoarele categorii:

1. **Guvernul și Ministerul Dezvoltării Economice și Digitalizării, în calitatea sa de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice** – din perspectiva, pe de o parte, a necesității instituirii unui mecanism instituțional și organizațional viabil de implementare a politicii de stat în domeniul securității cibernetice, în vederea asigurării rezilienței cibernetice a cercului de subiecți care cad sub incidența actului normativ, iar, pe de altă parte – necesitatea armonizării cadrului normativ național;
2. **Persoanele juridice de drept public, inclusiv autoritățile administrației publice locale** – categorie care prin efectul legii sunt identificate ca furnizori esențiali sau importanți de servicii;
3. **Persoanele juridice de drept privat, inclusiv întreprinderile de stat**, care cad sub incidența prevederilor proiectului de act normativ;
4. **Utilizatorii finali ai serviciilor** prestate de furnizorii de servicii, esențiali sau importanți, din perspectiva interesului pe care îl au în creșterea calității serviciilor de care beneficiază, în mod special din punctul de vedere al securității și protecției datelor cu caracter personal.

Problematica descrisă mai sus are la bază o serie de cauze:

1. măsuri de securitate a rețelelor și sistemelor informatice implementate fragmentar sau chiar lipsa acestora;
2. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică în ambele sectoare, public și privat. Vulnerabilitățile și incidentele cibernetice nu sunt raportate, în principal din cauza reticenței companiilor de a dezvălui aceste informații, din temerea prejudiciilor aduse reputației sau a posibilei răspunderi.
3. cadrul instituțional, procedural și normativ-juridic incomplet.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Prezentul proiect de hotărâre de Guvern va contribui la realizarea **obiectivului general al întregului cadru normativ în domeniul securității cibernetice** și anume de creștere a 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 de către aceștia a serviciilor esențiale.

Ca **obiective specifice** ale prezentului proiect de hotărâre de Guvern, care odată realizate vor contribui la atingerea obiectivului general enunțat mai sus, trebuie relevate următoarele:

- stabilirea unor mecanisme de evaluare a implementării cerințelor de securitate a rețelelor și sistemelor informatice pe care le dețin și le utilizează furnizorii de servicii din sectoarele critice;
- stabilirea procedurilor privind modul de exercitare de către Agenția pentru Securitate Cibernetică a funcțiilor de supraveghere și control de stat.

Proiectul de act normativ propus spre examinare are ca **obiect de reglementare** stabilirea cadrului juridic, organizatoric și procedural de exercitare de către Agenția pentru Securitate Cibernetică a

funcției de supraveghere și control de stat al modului în care furnizorii de servicii în sectoarele critice asigură conformarea cu prevederile cadrului normativ în domeniul securității cibernetice.

Domeniul de aplicare al proiectului propus spre examinare se extinde asupra tuturor furnizorilor de servicii, esențiali și importanți, care sunt sau urmează să fie identificați de Agenția pentru Securitate Cibernetică în conformitate cu prevederile Hotărârii Guvernului nr. 860/2024.

Din punct de vedere structural, proiectul include partea dispozitivă a hotărârii de Guvern și anexa.

Partea dispozitivă cuprinde decizia Guvernului de adoptare a regulamentului în speță și sarcina Ministerului Dezvoltării Economice și Digitalizării de elaborare, în comun cu Agenția pentru Securitate Cibernetică, a Metodologiei privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.

Anexa cuprinde Regulamentul cu privire la supravegherea și controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice. Acesta include patru capitole.

Capitolul I – Dispoziții generale – cuprinde prevederi care determină obiectul de reglementare al proiectului, actele legislative relevante care cuprind definițiile unor noțiuni utilizate în textul proiectului de act normativ, precum și categoria de subiecți care cad sub incidența prevederilor actului normativ. Totodată, capitolul enunță principiile specifice exercitării funcției de supraveghere și control de către Agenția pentru Securitate Cibernetică, dintre care se remarcă principiile proporționalității, eficacității și efectului de descurajare, principii expres prevăzute atât în Directiva NIS2, cât și în legislația națională în domeniul securității cibernetice.

Conform art. 25 alin. (2) lit. c) din Legea nr.98/2012 privind administrația publică centrală de specialitate, una din funcțiile de bază ale unui minister este **funcția de supraveghere și control de stat**. Această funcție este constituită din **două părți componente: supravegherea**, definită ca fiind totalitatea acțiunilor întreprinse prin analiza continuă sau periodică a unor informații ce țin de persoanele fizice și juridice, fără a interveni în activitatea acestora, și **controlul de stat**, definită ca verificarea respectării de către persoanele fizice și juridice a prevederilor legislației, realizate în limitele și în conformitate cu legea. Unul dintre principiile fundamentale de organizare și funcționare a administrației publice centrale de specialitate este **delimitarea funcțiilor de elaborare și de promovare a politicilor de funcțiile de implementare a acestora**, prevăzut la art. 4 pct. 1) lit. c) din nr.98/2012. În baza acestui principiu, pus în aplicare și prin prevederile art. 14 din Legea nr. 98/2012, funcția de supraveghere și control de stat a fost atribuită prin Legea nr. 48/2023 cu privire la securitatea cibernetică Agenției pentru Securitate Cibernetică. **Conceptul propus în proiect** urmează această abordare, delimitând reglementările care vizează supravegherea și controlul de stat în capitole separate. Aceasta este motivat de faptul că supravegherea este diferită de controlul de stat atât prin compoziția sa materială, cât și din punct de vedere a problematicii procedurale pe care o implică. De asemenea, supravegherea diferă de controlul de stat atât prin obiectivele pe care le urmărește și mijloacele pe care le folosește, cât și prin intensitatea și consistența intervenției autorității publice în exercitarea acestei subfuncții. Un alt aspect important al conceptului propus în proiect derivă din prevederile art. 19 alin. (5) din Legea nr. 48/2023, care delegă Guvernului reglementarea modului de efectuare a controlului de stat de către ASC, însă separat pentru persoanele juridice de drept public și, respectiv, pentru persoanele juridice de drept privat. Această separare este determinată de domeniul de aplicare a Legii nr. 131/2012 privind controlul de stat. Potrivit art. 1 controlul se extinde doar asupra controlului de stat al activității de întreprinzător. Acțiunea legii respective poate fi extinsă și asupra controlului persoanelor care nu practică activitatea de întreprinzător doar dacă legile speciale fac referință la Legea nr. 131/2012. Potrivit prevederilor art. 19 alin. (1) din Legea nr. 48/2023, Agenția pentru Securitate Cibernetică exercită controlul de stat asupra respectării legii de către furnizorii de servicii persoane juridice de drept privat, aplicând prevederile Legii nr.131/2012 privind controlul de stat.

Prevederea punctului 5 este determinată de necesitatea asigurării complementarității dintre cadrul strategic și operațional din domeniul securității cibernetice cu cel din domeniul protecției fizice a infrastructurii critice din perspectiva exercitării funcției de supraveghere și control de stat. Cadrul strategic și operațional în domeniul protecției fizice a infrastructurii critice este reglementat prin Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale. Legea nr. 48/2023 privind securitatea cibernetică și Legea nr. 223/2025 sunt acte ce asigură armonizarea cadrului normativ național la Directiva (UE) 2022/2555¹² și, respectiv, la Directiva (UE) 2022/2557¹³. Complementaritatea acestor două directive și, implicit, a legilor naționale menționate mai sus, constă în necesitatea asigurării unei cooperări și unui schimb de informații între autoritățile competente în temeiul acestor cadre legislative, „în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în legătură cu riscurile, amenințăările și incidentele de altă natură decât cibernetică ce afectează entitățile critice, inclusiv măsurile în materie de securitate cibernetică și măsurile fizice adoptate de entitățile critice precum și **rezultatele activităților de supraveghere desfășurate în legătură cu astfel de entități. În plus, pentru a raționaliza activitățile de supraveghere între autoritățile competente (n.n. – din ambele domenii de activitate) ... și pentru a reduce la minimum sarcina administrativă pentru entitățile în cauză, autoritățile competente ar trebui să depună eforturi pentru a armoniza modelele de notificare a incidentelor și procesele de supraveghere. După caz, autoritățile competente în temeiul Directivei (UE) 2022/2557 ar trebui să poată solicita autorităților competente în temeiul prezentei directive să își exercite competențele de supraveghere și de asigurare a respectării legii în legătură cu o entitate care este identificată drept o entitate critică în temeiul Directivei (UE) 2022/2557. Autoritățile competente în temeiul prezentei directive și cele competente în temeiul Directivei (UE) 2022/2557 ar trebui, atunci când este posibil în timp real, să coopereze și să facă schimb de informații în acest scop.**”¹⁴

În Capitolul II – Supravegherea respectării cadrului normativ în domeniul securității cibernetice de către furnizorii de servicii în sectoarele critice – sunt reglementate aspecte privind modul de supraveghere asupra respectării cadrului normativ în domeniul securității cibernetice de către toți furnizorii de servicii în sectoarele critice: atât de către cei care sunt persoane juridice de drept public, cât și de către cei care sunt persoane juridice de drept privat. În capitol sunt enumerate măsurile de supraveghere pe care ASC urmează să le realizeze în exercitarea acestei funcții și limitele și principalele caracteristici ale acestora. Conform proiectului, măsurile de supraveghere urmează a fi aplicate în baza rezultatelor evaluării riscurilor în domeniul securității cibernetice la nivel național, intersectorial, sectorial, subsectorial, precum și atunci când este relevant, în baza evaluărilor de riscuri în alte domenii, iar scopul acestora este să asigure facilitarea conformării, consolidarea capacităților și creșterea nivelului de reziliență cibernetică a furnizorilor de servicii.

Capitolul III - Controlul de stat asupra respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept privat, identificate ca furnizori de servicii în sectoarele critice – reglementează procedura controlului de stat în privința furnizorilor de servicii în sectoarele critice, care sunt persoane juridice de drept privat, principiile și procedura stabilită de prevederile Legii nr. 131/2012 privind controlul de stat fiind aplicate corespunzător.

¹² <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2555>

¹³ <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32022L2557>

¹⁴ Recitalul 33 din Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2).

În Capitolul IV - *Controlul de stat al respectării cadrului normativ în domeniul securității cibernetice de către persoanele juridice de drept public, identificate ca furnizori de servicii în sectoarele critice* – sunt reglementate aspecte privind activitatea desfășurată de către ASC în exercitarea funcției de control de stat asupra furnizorilor de servicii din sectorul public. Capitolul cuprinde prevederi privind planificarea controlului, pregătirea și realizarea controlului, etapa finalizării acestuia și monitorizarea măsurilor stabilite. Având în vedere faptul că prevederile Legii 131/2012 privind controlul de stat nu se răsfrâng asupra entităților din sectorul public, capitolul descrie o procedură separată pentru aceste entități și simplificată, într-o anumită măsură, din perspectiva faptului că entitățile din sectorul public, nepracticând activitate de întreprinzător nu pot beneficia de întregul spectru de garanții oferite de Legea respectivă mediului privat. Din contra aceste entități poartă o responsabilitate sporită dat fiind interesul public pe care îl protejează și în realizarea căruia își desfășoară activitatea administrativă. Cu toate acestea, procedura propusă păstrează garanții legate de continuitatea activității furnizorului de servicii, documentarea procesului, planificarea activității de control, etc.

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Opțiunile alternative nu au fost luate în considerare deoarece la nivel de lege este stabilită obligația Guvernului de a aproba cerințe privind măsurile de securitate a rețelelor și sistemelor informatice ale furnizorilor de servicii.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Proiectul de act normativ nu implică impacturi structurale și instituționale asupra sistemului administrației publice, inclusiv acțiuni de reformă structurală sau instituțională.

4.2. Impactul financiar și argumentarea costurilor estimative

Impactul financiar direct al proiectului asupra mediului de afaceri este reprezentat de costurile administrative ce urmează a fi suportate de către agenții economici. În vederea estimării costurilor administrative pe care agenții economici trebuie să le suporte pentru a se conforma obligațiilor informaționale impuse prin prezentul proiect de hotărâre de Guvern este utilizată Metodologia de estimare a costurilor administrative prin aplicarea Modelului Costului Standard aprobată prin Hotărârea Guvernului nr. 307/2016.

Astfel, în sensul Metodologiei menționate supra, obligația informațională generată pentru agenții economici de noile prevederi normative, în calitatea lor de furnizorii de servicii, este participarea la realizarea controlului de către Agenția pentru Securitate Cibernetică.

În continuare se prezintă potențialul cost administrativ care l-ar putea suporta un agent economic supus controlului, respectând formula dată de Metodologia de estimare a costurilor administrative prin aplicarea Modelului Costului Standard, aprobată prin Hotărârea Guvernului nr. 307/2016:

Acte normative	Autorități implicate	Descrierea obligației informaționale	Activități administrative	Timp, ore	Tarif, lei/oră	Preț, lei	Achiziții, lei	Preț total, lei	Numărul de agenți economici	Frecvența, număr pe an	Cantitate, număr pe an	Costuri administrative totale, lei
1	2	3	4	5	6	7=5x6	8	9=7+8	10	11		
Legea nr. 48/2023 privind securitatea cibernetică (art.4)	Agenția pentru Securitate Cibernetică	Participarea la realizarea controlului de către Agenția pentru Securitate Cibernetică	Familiarizarea cu obligația informațională	6,0	105,1	630,6	0,0	630,6			630,6	630,6
			Asistarea în procesul de efectuare a controlului	64,0	105,1	6726,4	0,0	6726,4			6726,4	6726,4
			Prezentarea informațiilor pe marginea	10,0	105,1	1051	0,0	1051			1051	1051

			procesului verbal de control									
TOTAL											8408,0	

Aceleași estimări urmează a fi aplicate și evaluării impactului financiar asupra sectorului public din perspectiva obligațiilor pe care furnizorii de servicii din acest sector urmează să le realizeze.

Totodată, evidențiem că activitatea ASC în exercitarea funcției de supraveghere și control de stat în domeniul securității cibernetice urmează a se efectua în limita mijloacelor financiare aprobate acestei autorități în bugetul de stat.

4.3. Impactul asupra sectorului privat

Sub aspectul impacturilor non-financiare asupra sectorului privat ținem să relevăm în mod special că proiectul de act normativ propus spre examinare va contribui la:

- Consolidarea rezilienței și securității cibernetice: Soluția propusă va contribui la consolidarea securității cibernetice prin detectarea și blocarea eficientă a atacurilor, protejând datele și informațiile sensibile și asigurând reacții rapide;
- Protecția informațiilor și a drepturilor utilizatorilor: Implementarea soluției va spori protecția informațiilor personale și a drepturilor utilizatorilor, prevenind accesul neautorizat și utilizarea abuzivă a datelor;
- Reducerea costurilor asociate incidentelor cibernetice: Soluția va reduce riscurile, impactul și costurile financiare legate de incidentele cibernetice, cum ar fi pierderile de date și daunele reputației sau perturbarea serviciilor, economisind astfel resursele necesare pentru recuperare și remediere;
- Siguranța infrastructurii critice: Soluția va proteja infrastructura critică, cum ar fi rețelele energetice, sistemul bancar și transportul, reducând riscul de întreruperi majore și asigurând continuitatea serviciilor vitale;
- Îmbunătățirea cooperării dintre autoritățile publice responsabile și furnizorii de servicii în sectorul privat în implementarea cerințelor de securitate a rețelilor și sistemelor informatice, aprobate prin Hotărârea Guvernului nr. 562/2025.

4.4. Impactul social

4.4.1. Impactul asupra datelor cu caracter personal

Din perspectiva datelor cu caracter personal, prevederile proiectului de act normativ vor avea un impact pozitiv, având în vedere că acesta are ca obiectiv ridicarea nivelului de securitate a rețelilor și sistemelor informatice ale furnizorilor de servicii esențiale.

4.4.2. Impactul asupra echității și egalității de gen

Nu este aplicabil.

4.5. Impactul asupra mediului

Nu este aplicabil.

4.6. Alte impacturi și informații relevante

Nu este aplicabil

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Nu este aplicabil.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

Nu este aplicabil.

6. Avizarea și consultarea publică a proiectului actului normativ

În conformitate cu prevederile art. 9 din Legea nr. 239/2008 privind transparența în procesul decizional, la data de 19.05.2025 a fost publicat anunțul referitor la inițierea procesului de elaborare a proiectului de act normativ pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe platforma de consultare particip.gov.md. (<https://particip.gov.md/ro/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-hotararii-de-guvern-cu-privire-la-supravegherea-si-controlul-de-stat-al-modului-in-care-furnizorii-de-servicii-respecta-prevederile-legii-nr-482023-privind-securitatea-cibernetica/14506>)

7. Concluziile expertizelor

Proiectul de act normativ urmează a fi supus expertizei anticorupție și expertizei juridice, conform procedurii stabilite de cadrul normativ.

8. Modul de încorporare a actului în cadrul normativ existent

Adoptarea și intrarea în vigoare a proiectului nu va necesita modificarea cadrului normativ existent. Totuși, după cum este reflectat și în partea dispozitivă a hotărârii Guvernului, pentru punerea în aplicare a acestei hotărâri, Ministerul Dezvoltării Economice și Digitalizării, în comun cu Agenția pentru Securitate Cibernetică, urmează să elaboreze și să prezinte Guvernului spre examinare Metodologia privind controlul de stat asupra activității de întreprinzător în baza analizei riscurilor aferent domeniilor de competență ale Agenției pentru Securitate Cibernetică.

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Instituția principală responsabilă de asigurarea implementării proiectului de act normativ este Agenția pentru Securitate Cibernetică. Pentru a asigura punerea în aplicare a prevederilor proiectului propus spre examinare, Agenția urmează:

- să finalizeze operaționalizarea în volum deplin a subdiviziunii responsabile de supraveghere și control;
- să aprobe ghiduri și orientări metodologice privind implementarea măsurilor de securitate a rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice;
- să efectueze evaluări ale riscurilor la nivel național, sectorial, subsectorial și în baza rezultatelor acestora să planifice activitățile de supraveghere și control de stat;
- să acorde suport consultativ furnizorilor de servicii, precum și să întreprindă alte acțiuni menite să faciliteze conformarea furnizorilor de servicii în sectoarele critice cu prevederile cadrului normativ în materie de securitate cibernetică, în mod special cu cerințele de securitate a rețelelor și sistemelor informatice ale acestora;
- să evalueze nivelul de conformare a furnizorilor de servicii în sectoarele critice cu cerințele cadrului normativ în domeniul securității cibernetice.

Viceprim-ministru,

Ministru al Dezvoltării Economice și Digitalizării

Eugen OSMOCHESCU